MOORE GEOMETRIES AND RANK 3 GROUPS HAVING $\mu = 1$†

By WILLIAM M. KANTOR

[Received 13 November 1975; in revised form 24 September 1976]

1. Introduction

HIGMAN [**9, 10**] and Aschbacher [**2**] have determined all rank 3 permutation groups having $\mu = 1$ and $\lambda = 0$ (in the notation of [**9**]). In this note we will complete the classification of rank 3 groups with $\mu = 1$:

THEOREM 1.1. *No rank* 3 *groups exist having* $\mu = 1$ *and* $\lambda > 0$.

In view of the standard correspondence between transitive groups and certain graphs, this result can be rephrased in the following manner. Let Γ be a graph which is connected and not complete. Assume that $G \leqslant \mathrm{Aut}\,\Gamma$ is transitive both on ordered adjacent and non-adjacent pairs of points, and that two non-adjacent points are adjacent to exactly one point. Then Γ has no triangles, and G and Γ are as on p. 151 of [**9**].

The proof is primarily geometric and combinatorial, groups entering only after extremely strong information has been obtained concerning involutions.

The underlying geometric objects associated with such groups are defined and generalized in § 3. When all lines have just two points, these are precisely Moore graphs [**12**]; this suggests calling them Moore geometries in the general case. They fall into two classes, one of which has been studied in [**3**] using elementary arithmetic and standard eigenvalue conditions (cf. (3.3)).

Elementary properties of Moore geometries are proved in § 3. In particular, it is shown in (3.6) that from any finite affine plane one can obtain in a natural manner a Moore geometry having special numerical properties; thus, in some sense Moore geometries may be regarded as generalizations of affine planes. By combining G. Higman's character theoretic result (2.1) with intricate counting arguments, in § 4 we obtain severe restrictions on involutions of Moore geometries. These are used in §§ 5 and 6 to prove (1.1); some aspects of the proof are reminiscent of arguments used for projective planes (especially (4.8)).

I am grateful to G. Higman for pointing out (2.1) (in a slightly different form); this produced a considerable simplification of my original proof of (1.1). The reader strictly interested in (1.1) need only examine (2.1), (3.1)–(3.3), (4.1)–(4.8), (5.1)–(5.3), and §6. On the other hand, Moore

† This research was supported in part by NSF Grant GP 37982X.

geometries seem sufficiently interesting in their own right to warrant the inclusion of many of their properties; this is done in the remainder of this paper.

I am indebted to Noboru Ito and the referee, Peter Cameron, for their many helpful comments.

If G is a group acting on a set X, and $Y \subseteq X$, then $G(Y)$ and G_Y will denote the pointwise and global stabilizers of Y.

2. Strongly regular graphs

Let Γ be a graph. For points x, y of Γ, we write $x \sim y$ if x and y are joined, and $x \not\sim y$ if x and y are distinct and not joined. $x^\perp$ denotes $\{x\} \cup \{y \mid y \sim x\}$.

Let Γ be a strongly regular graph with parameters n, k, l, λ, μ, and adjacency matrix A satisfying

$$A^2 - (\lambda - \mu)A - (k - \mu)I = \mu J$$

$$AJ = kJ,$$

(where I and J are the identity and all one $n \times n$ matrices (see, e.g., Higman [9], [11]). Set $\Delta^2 = (\lambda - \mu)^2 + 4(k - \mu)$, where $\Delta > 0$. Then, by a straightforward calculation,

$$\varepsilon = -\frac{\lambda - \mu - \Delta}{2\Delta} I + \frac{1}{\Delta} A - \frac{2k - (\lambda - \mu) + \Delta}{2n\Delta} J$$

is an idempotent matrix. For each $g \in \operatorname{Aut}\Gamma$, let $M(g)$ denote the corresponding $n \times n$ permutation matrix. Then $\varepsilon M(g) = M(g)\varepsilon$. It follows that the function $\theta(g) = \operatorname{trace}(\varepsilon M(g))$ is a character of $\operatorname{Aut}\Gamma$.

$\theta(g)$ can be calculated as follows. Let $\chi(g)$ denote the number of fixed points of g, and $\alpha(g)$ the number of points x with $x \sim x^g$. Then a simple calculation yields

THEOREM 2.1.

$$\theta(g) = -\frac{\lambda - \mu - \Delta}{2\Delta} \chi(g) + \frac{1}{\Delta} \alpha(g) - \frac{2k - (\lambda - \mu) + \Delta}{2\Delta}$$

defines a character of $\operatorname{Aut}\Gamma$. *In particular,* $\theta(g)$ *is an algebraic integer, and hence even an integer if* Δ *is.*

Note that Δ is usually an integer. Moreover, the degree $\theta(1)$ of θ is the multiplicity of one of the eigenvalues of A (cf. Higman [9], [11]).

Theorem 2.1 is due to G. Higman, in a slightly different form. When $\operatorname{Aut}\Gamma$ has rank 3 on points, (2.1) is a special case of results of Scott [13].

The remainder of this section is devoted to some easy examples of (2.1), designed to indicate how it may help restrict the parameters of Γ in some situations; further examples will appear in § 4. Each case is designed to make the determination of $\alpha(g)$ easy.

DEFINITION. If $S \subseteq \operatorname{Aut}\Gamma$, $F(S)$ denotes its set of fixed points.

Example 1. Assume $F(g) = z^{\perp}$, and that hyperbolic lines ([**9**], [**11**]) contain no joined pairs of points. (This occurs if, for example, $\mu > \lambda + 1$ [**9**].) Then $\alpha(g) = 0$. For suppose $x \notin z^{\perp}$; then g fixes each point joined to both x and z, and hence fixes xz, so $x \neq x^g$ by hypothesis. Thus, in this situation 2Δ divides $-(\lambda-\mu-\Delta)(k+1)-2k+(\lambda-\mu)-\Delta = -k(\lambda-\mu-\Delta+2)$.

Example 2. If Γ corresponds to a generalized quadrangle of order (s, t), then (2.1) implies that $s+t$ divides $(t+1)\chi(g)+\alpha(g)-(s+1)(t+1)$ for every $g \in \operatorname{Aut}\Gamma$. There is also a corresponding result for the dual quadrangle.

If $F(g) = z^{\perp}$ for some z, we obtain $s+t \mid (t+1)st$.

Suppose next that g is an involution, and that $F(g)$ is a subquadrangle of order (s', t'). Then

$$\alpha(g) = (1+t')(1+s't')(s-s') \quad \text{and} \quad \chi(g) = (1+s')(1+s't'),$$

but the divisibility condition is unwieldy. If, however, $s = s'$ here then (2.1) yields $s+t \mid (s+1)(t+1)st'$.

Example 3. Assume $\lambda = 0$ and $|g| = 3$. Since Γ then contains no triangles, $\alpha(g) = 0$. Thus, (2.1) implies that 2Δ divides $(\mu+\Delta)\chi(g) - 2k - \mu - \Delta$.

In particular, if $\mu = 2$ here then $\sqrt{(k-1)}$ is an integer dividing $\chi(g)-2$. (The parameters $\lambda = 0$, $\mu = 2$ correspond to a biplane having a null polarity; cf. Cameron [**5**].)

For the case $\mu = 1$, see the remark following (4.7).

Example 4. Let $\mathfrak{D}$ be a design such that pairs of distinct blocks have exactly two different intersection sizes σ, τ. Let M be the incidence matrix of $\mathfrak{D}$, I_v and J_v the $v \times v$ identity and all-one matrices, and I_b and J_b the analogous $b \times b$ matrices. Then the set of blocks forms a strongly regular graph, whose adjacency matrix A satisfies

$$MM^t = (r-\lambda)I_v + \lambda J_v$$

$$M^tM = kI_b + \sigma A + \tau(J_b - I_b - A).$$

Let χ, α, and θ be as before (with different interpretations for k and λ). Set $G = \operatorname{Aut}\mathfrak{D}$. Then M induces a G-isomorphism between the eigenspaces (of dimension $v-1$) of MM^t and M^tM with eigenvalue $r-\lambda$.

Hence, either $1+\theta$ or $b-\theta$ (depending on whether $\theta(1)=v-1$ or $b-v$) is the permutation character χ_p of G on the points of $\mathcal{D}$.

Now (2.1) provides an intriguing relationship between χ_p, χ, and α. This does not seem to yield any useful information in the case of designs with $\lambda=1$. Consider, however, the 3-designs studied by Cameron [4], with parameters $v=(s+1)(s^2+5s+5)=r+1$, $b=(s^2+5s+5)(s^2+4s+2)$, $k=s^2+3s+2=\lambda+1$, and which are locally symmetric. (Here, $\sigma=0$ and $\tau=s+1$.) By (2.1), $\chi_p(g)(s+3)=\chi(g)-\alpha(g)/(s+1)+s^2+5s+5$. In particular, if $|g|=3$ then $\chi_p(g)(s+3)=\chi(g)+s^2+5s+5$.

3. Moore geometries

Let Γ be a graph satisfying the following properties. There is more than one point; no point is joined to all others; and two non-adjacent points x, y are both joined to exactly one point, called $x\circ y$.

If L is a maximal clique in Γ (i.e., maximal set of pairwise adjacent points), Π (L) will denote the complement of $\bigcup\{x^\perp \mid x\in L\}$, and L will be called a *line*.

LEMMA 3.1.

(*i*) *Lines exist, and each has at least two points.*

(*ii*) *Two points are on at most one line.*

(*iii*) *No point is collinear with all others.*

(*iv*) *Two non-collinear points x, y are both collinear with exactly one point $x\circ y$.*

(*v*) *A point not in a line is collinear with at most one point of the line.*

(*vi*) *No triangles or quadrangles of lines exist.*

Proof. Two points are collinear if and only if they are joined. Suppose $w, y, z\in x^\perp-\{x\}$ with $w\sim y\sim z$ and $w\neq z$. Then w and z are joined to x and z, so by hypothesis they must be joined. Thus, $x^\perp-\{x\}$ is partitioned into cliques, and (ii) holds. The remaining assertions are obvious.

DEFINITION. A system of points and lines satisfying (i)–(vi) is called a *Moore geometry.*

THEOREM 3.2. *Let $\mathcal{G}$ be a Moore geometry. Then exactly one of the following holds.*

(I) *The underlying graph is strongly regular; all lines have the same number $s+1$ of points; and all points are on the same number $t+1$ of lines.*

(II) *There are integers a, b, l satisfying the following conditions.*

(α) *Each point is in $A=\{x \mid |x^\perp|=a\}$ or $B=\{x \mid |x^\perp|=b\}$.*

(β) *$A\neq\emptyset$ and $B\neq\emptyset$.*

(γ) *Each line has 2 or l points, and both sizes occur.*

(δ) *Each 2-point line meets A and B, while each l-point line is contained in A.*

(ε) $a-b=l-2>0$, *and* $|A\cup B|=1+(a-1)(b-1)$.

Proof. Let $L=xx'$. Then by (iv), each $z\in\prod(L)$ can be written $z=(x\circ z)\circ(x'\circ z)$, while $y\circ y'\in\prod(L)$ whenever $y\in x^{\perp}-L$ and $y'\in x'^{\perp}-L$. Thus, $|\prod(L)|=|x^{\perp}-L|\circ|x'^{\perp}-L|$.

By (iii) and (iv), each point is on at least two lines. Suppose $p=x\circ y$. Then each $z\in x^{\perp}-px$ determines a unique $z\circ y\in y^{\perp}-py$. Thus, $|x^{\perp}-px|=|y^{\perp}-py|>0$. In particular, $|x^{\perp}|=|y^{\perp}|$ if and only if $|px|=|py|$.

Suppose L is a line with $|L|>2$. Then $|x^{\perp}|$ is independent of $x\in L$. (For, let $\{p,x'\}\subseteq L-\{x\}$, $p\neq x'$, and $y\in p^{\perp}-L$; then $|x^{\perp}-L|=|y^{\perp}-py|=|x'^{\perp}-L|$.) Thus, $|\prod(L)|=|x^{\perp}-L|^2$, so the total number of points of $\mathcal{G}$ is

$$n=|L|+|L|\cdot|x^{\perp}-L|+|x^{\perp}-L|^2=|L|-|L|\cdot|x^{\perp}|+|x^{\perp}|^2. \qquad (\#)$$

If all lines have 2 points, then $|x^{\perp}|=|y^{\perp}|$ for all x, y, and (I) holds with $s=1$ and $t=|x^{\perp}|-2$. Suppose all lines have more than 2 points. Then once again, $|x^{\perp}|=d$ is independent of x. By ($\#$), so is $|L|$, and there are $(d-1)/(|L|-1)$ lines per point. Thus, (I) also holds in this case.

We may thus assume that some line has more than two points, while some line has just two points u and u'. In the latter case, $n=2+(|u^{\perp}|-2)+(|u'^{\perp}|-2)+(|u^{\perp}|-2)(|u'^{\perp}|-2)$.

By ($\#$), for a given x there are just two sizes of lines through x. Moreover, if $y\sim x$ then either $|xy|>2$ and $|x^{\perp}|=|y^{\perp}|$, or $|xy|=2$ and $|y^{\perp}|=1+(n-1)/(|x^{\perp}|-1)$.

The connectedness of $\mathcal{G}$ implies that some point p is on both an l-point line px and a 2-point line py, where $l>2$. Set $a=|p^{\perp}|=|x^{\perp}|$ and $b=|y^{\perp}|$. Then $a-l=b-2$, $n=1+(a-1)(b-1)$, and (ε) holds. Clearly (β) holds. If $z\in x^{\perp}-px$, then $|z^{\perp}|-|zx|=|p^{\perp}|-|px|=a-l=b-2$, so $|x^{\perp}|=b$ if and only if $|zx|=2$. Thus, the points of $x^{\perp}-\{x\}$ fall into the sets A and B defined in (α), according to the size of zx. Each line on p or x has 2 or l points.

We can now prove (α). Let $w\notin p^{\perp}$, and set $q=p\circ w$. If $|pq|>2$ then $|pq|=l$ and $|q^{\perp}|=a$, so $|w^{\perp}|=a$ or $1+(n-1)/(|q^{\perp}|-1)=b$. Suppose $|pq|=2$, so $|q^{\perp}|=1+(n-1)/(|p^{\perp}|-1)=b$ and $|w^{\perp}|-|qw|=|p^{\perp}|-2$. If $|qw|=2$ then $|w^{\perp}|=|p^{\perp}|$, while if $|qw|>2$ we know $|q^{\perp}|=|w^{\perp}|$. This proves (α).

From py, we see that $n=1+(a-1)(b-1)$. For any 2-point line uu', $n=1+(|u^{\perp}|-1)(|u'^{\perp}|-1)$. Since $|u^{\perp}|$ and $|u'^{\perp}|$ are a or b, while $a-b=l-2\neq 0$, it follows that uu' meets both A and B.

Finally, consider a line M with $|M|=m>2$. If $M\subseteq A$ then $|M|=l$ by ($\#$) (since $n=l-al+a^2$ already). It remains to eliminate the case $M\cap B\neq\varnothing$. But here, we know $M\subseteq B$. Let $v\in M$ and $w\in v^{\perp}-M$. Then

$|w^\perp|-|wv|=b-|m|$. If $|wv|=2$ then $wv\cap A\neq\emptyset$, so $w\in A$ and $2-m=a-b=l-2>0$. Thus, each line meeting M must have m points, and hence lies in B. Thus, the connected component of $\mathcal{G}$ containing M lies entirely in B. Since $A\neq\emptyset$ and $\mathcal{G}$ is connected, this is a contradiction. This completes the proof (γ), (δ), and hence of (3.2).

DEFINITIONS. 1. A Moore geometry has *type* (s, t) or (a, b, l) according to whether (3.2 I) or (3.2 II) holds.

2. A Moore geometry of type $(a, 3, l)$ is called *trivial*. It consists of an l-point line $L=\{x_1, \ldots, x_l\}$, and $l+1$ other points $z, y_1, \ldots, y_l$, with lines L, $\{x_i, y_i\}$, and $\{z, y_i\}$. Here, $A=L\cup\{z\}$ and $B=\{y_1, \ldots, y_l\}$. A Moore geometry of type $(1, 1)$ is also called *trivial*.

3. In a Moore geometry of type (a, b, l), an *i-line* ($i=2$ or l) is a line having exactly i points.

4. A *subgeometry* of a Moore geometry $\mathcal{G}$ is a subset F of points which is a Moore geometry under the induced adjacency. Thus, $x, y\in F$ and $x\neq y$ in $\mathcal{G}$ imply $x\circ y\in F$. Clearly, if $S\subseteq \mathrm{Aut}\,\Gamma$ then the set $F(S)$ of fixed points of S is either a subgeometry or satisfies $F(S)\subseteq x^\perp$ for some x.

Remarks. No relationship is known in type (a, b, l) between $|A|$, $|B|$ and a, b, l (except for $|A|>|B|$; cf. (3.8)). Examples of non-trivial Moore geometries of type (a, b, l) will be given in (3.5) and (3.7). No Moore geometries of type (s, t) are known with $s>1$; the following result provides a few restrictions on the parameters s and t.

LEMMA 3.3. *The following hold for a Moore geometry of type* $(s, t)\neq(1, 1)$.

(i) $\Delta=\sqrt{\{s(s+4t)\}}$ *is an integer.*

(ii) Δ *divides* $s^2(t+1)\{(s-2)t+1\}$.

(iii) *There are* $\{1+s(t+1)(st+1)\}(t+1)/(s+1)$ *lines.*

(iv) *An incidence matrix* $\mathcal{G}$ *has rank equal to the number of points.*

(v) $t>s$.

(vi) $s=1$ *implies that* $t=2$, 6, *or* 56.

(vii) $s\neq 2$.

Proof. (i) and (ii) follow from standard eigenvalue considerations: in (2.1), $\Delta=\sqrt{(s^2+4st)}$, and $\theta(1)$ is an integer.

(iii) Count flags.

(iv) Some incidence matrix D satisfies $DD^t=(t+1)I+A$. By (2.1), $-(t+1)$ is not an eigenvalue of A.

(v) This follows from (iv). (Alternatively, let $w\in\prod(L)$. Then w is collinear with exactly $s+1$ points not in $\prod(L)$, one in each $x^\perp-L$, $x\in L$. Thus, $t+1\geq s+1$. By (i), $t\neq s$.)

(vi) This is well-known ([**9**], [**12**]).

(vii) Suppose $s=2$. Then $\Delta^2=4(1+2t)$. By (ii), $\sqrt{(1+2t)}$ divides $t+1$, whereas $(1+2t, t+1)=1$.

Remarks. Note that when $s=4$, (i) and (ii) state merely that $\sqrt{(t+1)}$ is an integer. Thus, $s=4$ is the most likely candidate for s if a Moore geometry of type (s, t) is to exist with $s>1$. On the other hand, (ii) implies that, for $s\neq 4$, t is bounded by a function of s.

Both (v) and (vii) are well-known results: (v) asserts the non-existence of finite generalized pentagons with more than 5 points; and (vii) is the Friendship Theorem.

One can also study $D'D$ and the adjacency matrix of the dual of $\mathcal{G}$. However, these do not seem to provide any additional information.

DEFINITION. Let $\mathcal{G}$ have type (a, b, l), with A and B as in (3.2). Define (B, A) to be the incidence structure have B as set of points, A as set of blocks, and incidence relation $\sim$. Then any two points are on a unique block, and each point is on exactly $b-1$ blocks. Note, however, that some blocks may be on no points!

LEMMA 3.4. *If (B, A) is a design, with k points on each block, then* $k^2-(l-1)k-(b-2)=0$, $k^2-k\equiv 0 \pmod{l-1}$, *and* $(a+1)(a-k)(a-k-1)\equiv 0 \pmod{l}$.

Proof. Suppose each block is on k points. Then $|B|=1+(b-1)(k-1)$ and $|A|=\{1+(b-1)(k-1)\}(b-1)/k$. Since $|A|+|B|=1+(a-1)(b-1)$, it follows that $a-1=k-1+\{1+(b-1)(k-1)\}/k$. As $a-b=l-2$, this proves the first assertion.

If $x\in A$, then $|x^{\perp}\cap B|=k$ and $|x^{\perp}\cap A|=a-k$. Here, $x^{\perp}\cap A$ is a union of l-lines. The number of such lines is $(a-k-1)/(l-1)$; then $b-2\equiv k \pmod{l-1}$ implies the second assertion. Finally, there are exactly $|A|(a-k-1)(l-1)^{-1}/l$ l-lines. Since $|A|=(b-1)(a-k)\equiv(a+1)(a-k) \pmod{l}$, this proves the lemma.

That the hypotheses of (3.4) can actually be satisfied is seen from the following example.

Example 1. Let a be an affine plane of order l. Denote by A its set of lines and B its set of points. Join two members of A if they are disjoint, and members of A and B if they are incident. The result is a Moore geometry of type $(2l, l+2, l)$, called an *affine Moore geometry.*

Example 2. Starting with an affine Moore geometry as above, adjoin a new point to each l-line, and a new line containing all new points. The resulting Moore geometry of type $(2l+1, l+2, l+1)$ will be called *projective.*

Example 3. Let θ be a polarity of a finite projective plane of order n. Let A and B be the sets of nonabsolute resp. absolute points. Join two points x and y if $x\neq y\in x^{\theta}$. The resulting Moore geometry of type $(n+2, n+1, 3)$ will be called *polar.* (There is a unique example $\mathcal{G}_{13}$ when

$n = 3$, and two examples when $n = 4$, one of which is also affine; the other is denoted $\mathcal{G}_{21}$.)

PROPOSITION 3.5 (W. Bridges). *A Moore geometry of type (a, b, l) is polar if and only if $l = 3$.*

Proof. Suppose $l = 3$, and regard the points of $\mathcal{G}$ as both the points and lines of an incidence structure. Call x and y incident if either $x \sim y$ or $x = y \in B$. It is then straightforward to verify that the result is a projective plane of order $b - 1$. Moreover, there is an obvious polarity, and hence $\mathcal{G}$ is polar.

LEMMA 3.6. *Every Moore geometry of type $(2l, l+2, l)$ is affine or $\mathcal{G}_{21}$.*

Proof. Let $|L| = l$ and $x \in L$. Note that $|x^\perp - L| = a - l = l$.

If $w \in \prod(L) \cap B$, then $|w^\perp \cap (x^\perp - L)| = 1$; these intersections account for l of the $b = l+2$ points of $w^\perp$. Thus, w is joined to a unique point of $\prod(L)$, which must be in A by (3.2 δ).

We claim that $\prod(L)$ contains two joined points of A. For suppose not. If $z \in A \cap \prod(L)$ then $|z^\perp \cap \prod(L)| = a - l = l$, so z is joined to $l - 1$ points of $\prod(L)$, all in B. It follows that $\prod(L)$ splits up into $(a-l)^2/l = l$ sets S of size l, each consisting of a point of A joined to $l - 1$ points of B. Let $z \in S$. Then each of the $l - 1$ points of $S - \{z\}$ is joined to a point of $x^\perp - L$, and each such point must be in A (by (3.2 δ)). Thus, $x^\perp - L$ consists of an l-line L_x and a point $b_x \in B$. Since each point of $S - \{z\}$ is joined to a point of L_x, necessarily $z \sim b_x$. Since $x \in L$ was arbitrary, we see that $z^\perp - \{z\} \subseteq B$. However, there is a point $w \in \prod(L) \cap B$ not joined to z. Then $z \circ w \in B$, which is not the case.

Thus, there is an l-line M with $|M \cap \prod(L)| \geq 2$.

CASE 1. $M \not\subseteq \prod(L)$. Suppose that $M \cap x^\perp = \{u\}$. Then $xu \subset A$ and $|x^\perp - (l \cup xu| = a - (2l-1) = 1$. Thus, $x^\perp = L \cup xu \cup \{p\}$ with $p \in B$. Let $z \in M - \{u\}$. Then $|z^\perp \cap \prod(L)| = a - l = l$ implies that $z^\perp \cap \prod(L)$ contains a unique $q \notin M$. Consider $q \circ x$. Since $q \sim z \sim u$, we cannot have $q \circ x \in ux$. Thus, $q \circ x = p$, so $q \in A$. But qz contains at least $l - 1$ points of $\prod(L)$. Thus, $l - 1 = 2$ and $\mathcal{G}$ has type $(6, 5, 3)$. Now (3.5) applies.

CASE 2. $M \subset \prod(L)$. Each point of M is joined to a different point of $x^\perp - L$, and no two of the latter points can be collinear. Consequently, $x^\perp - L \subset B$. As $x \in L$ was arbitrary, it follows that $B = \bigcup \{x^\perp - L \mid x \in L\}$ and $A = L \cup \prod(L)$. If $z \in \prod(L)$ then $|z^\perp \cap \prod(L)| = a - l = l$, so $z^\perp \cap \prod(L)$ is a line. Thus, $\prod(L)$ is partitioned into l lines of size l.

Each point of B is joined to $l + 1$ points of A. Each point of A is joined to l points of B. Two points of B are joined to a unique point of A. Hence, (B, A) is an affine plane, and the lemma follows easily.

THEOREM 3.7. *If $\mathcal{G}$ is a non-trivial Moore geometry of type (a, b, l), then $a \geq 2l+1$, unless $\mathcal{G}$ is affine, projective, $\mathcal{G}_{13}$ or $\mathcal{G}_{21}$.*

Proof. Suppose $a < 2l$. Then $b = a-l+2 \leq l+1$. Let $|L| = l$. If $p \in B \cap \prod(L)$ then $p^\perp$ contains the $l+1$ points p and $x \circ p$, $x \in L$. Thus, $p^\perp \cap \prod(L) = \{p\}$. Moreover, $x \circ p \in A$ implies that $|x(x \circ p)| = l$, so $|x^\perp| \geq 2l-1$ and hence $x^\perp$ is the union of two l-lines.

Similarly, if $z \in A \cap \prod(L)$ then $z^\perp \cap \prod(L) \cap B = \varnothing$ and $|z^\perp \cap \prod(L)| = a-l < l$. Thus, $z^\perp \cap \prod(L) = L' - \{x \circ z\}$ for an l-line L' and a point $x \in L$. Once again, $x^\perp$ is the union of two l-lines.

Thus, in any case we may assume $x^\perp = L \cup M$ for some x and l-lines L, M. Each point of $\mathcal{G}$ is collinear with some point of L or M.

Let $p \in B$ be joined to $w \in L$, say. Let $u \in M - \{x\}$. Then $y = p \circ u \in A$. Thus, $|uy| = l$ and $u^\perp = M \cup uy$.

It follows that, if M and all its points are deleted from $\mathcal{G}$, the result is still a Moore geometry, of type $(a-1, b, l-1) = (2l-2, b, l-1)$ where $b = 2+(a-1)-(l-1) = l+1$, unless $l-1 = 2$ and the result is a Moore geometry of type (1, 2). In the former case, $\mathcal{G}$ is found to be projective by (3.6), while in the latter case $\mathcal{G}$ is $\mathcal{G}_{13}$ by (3.5).

One other indication of the significance of the incidence structure (B, A) is afforded by the following straightforward

LEMMA 3.8. *For any Moore geometry of type (a, b, l), an incidence matrix of (B, A) has rank $|B|$; moreover, $|B| < |A|$.*

Proof. By [6], p. 20, the indicated rank is $|B|$, and $|B| \leq |A|$ with $|B| = |A|$ if and only if (B, A) is a projective plane. However, the latter case cannot occur, since A contains two (joined) points which are not joined to a point of B.

Consequently, if Aut $\mathcal{G}$ is transitive on A, then it is also transitive on B.

A point in a Moore geometry of type (a, b, l) will be called *isolated* if it is in A and is on no l-line.

PROPOSITION 3.9. *Let $\mathcal{G}$ be a non-trivial Moore geometry of type (a, b, l). Let A and B be as usual.*

(i) *Assume that q is isolated. Then q is unique, $|B| = a-1$, and each point of $A-\{q\}$ is joined to exactly one point of B. If N denotes an adjacency matrix of the graph induced on $A-\{q\}$, then $(N+I) \times (N^2-(l-3)N-(a-2)I) = (a-2)J = NJ$ (where I and J are the identity and all-one matrices).*

(ii) *If no two l-lines meet, then $\mathcal{G}$ is affine.*

(iii) *If some l-line meets all others, then $\mathcal{G}$ is projective or $\mathcal{G}_{13}$.*

Proof. (i) First of all, q is collinear with each point of B (since $q \not\sim p \in B$ would imply $q \sim q \circ p \sim p$ with $q \circ p \in A$ and $|q(q \circ p)| = l$). Thus, $a-1 = |B|$.

If $x \in A-\{q\}$ then $q \circ x$ must be the only point of B joined to x. In particular, q is the only isolated point.

Let N_2 and N_3 be the characteristic functions of the relations $\{(x, y) \mid x, y \in A-\{q\}, x \not\sim y, x \circ y \in A\}$ and $\{(x, y) \mid x, y \in A-\{q\}, x \not\sim y, x \circ y \in B\}$. Then $N^2=(a-2)I+(l-2)N+N_2$, $NN_3=N_2$, $NJ=(a-2)J$, and $I+N+N_2+N_3=J$.

This implies (i). (Note also that $N_3^2=(a-l)N_3+(a-l-1)I$.)

(ii) Suppose first that there is an isolated point q. Let $x \in A-\{q\}$. Then (i) and our hypothesis imply that $|x^\perp|=2+(l-1)$, so $a=l+1$, whereas $\mathcal{G}$ is non-trivial.

Thus, the l-lines partition A. It follows easily that (B, A) is an affine plane, as required.

(iii) Let M be an l-line meeting every l-line. Then each non-isolated point of $A-M$ is on a unique l-line, and hence is joined to $a-l$ points of B. Since $a-l>1$, no isolated points exist by (i). Let $p \in B$. If $p \sim x \in M$, then x is the only point in $x^\perp$ joined to p. If $p \sim x \notin M$, let y be the point of M on the unique l-line through x; then x is the unique point of $y^\perp$ joined to p. Consequently, $b-1 \leqslant l$, so $a-l+1 \leqslant l$ and (3.7) applies.

COROLLARY 3.10. *In* (3.7), $a \neq 2l+1$ *if* $l>3$.

Proof. Assume $a=2l+1$. By (3.9 ii), there is a point q on exactly two l-lines L, M. Let $q' \in q^\perp \cap B$ and $p \in B-(q^\perp \cap B)$. Then $q \sim q \circ p \in A$, so we may assume $q \circ p \in L$. Then $x \in M-\{q\}$ implies that $x \not\sim p$ and $x \circ p \in A$. Thus, each point of M is on two l-lines.

Label the points of M as $q_1, \ldots, q_l$. Let M and L_i be the two l-lines on q_i. If $x_i \in L_i-\{q_i\}$ for each i, then either $x_1 \circ x_2$ is one of the points of $x_1^\perp \cap B$, or x_2 is on an l-line $\neq L_1$ through x_1. It follows that we can choose x_1, x_2, x_3 with $x_1 \circ x_i \in A$. But then either $x_1 \circ x_2 = x_1 \circ x_3$ or $x_1 \circ x_2 \neq x_1 \circ x_3$ implies that some point ($x_1 \circ x_2$ or x_1) of A is on at least three l-lines.

4. Involutions

Let $\mathcal{G}$ be a non-trivial Moore geometry with n points, σ an involutory automorphism, and $F=F(\sigma)$. Severe restrictions on F will follow from the next lemma.

LEMMA 4.1.

(i) *If* $x^\sigma \sim x$ *for some* x, *and* $L=xx^\sigma$, *then* $|F \cap \prod(L)|=|x^\perp-L|$.

(ii) *If* $z \notin F$, *then there is either exactly one line on* z *meeting* F *or exactly one fixed line on* z. *In any case there is at most one line on* z *meeting* F.

(iii) F *contains two collinear points.*

Proof. (i) If $y \in x^\perp-L$, then $y^\sigma \in (x^\sigma)^\perp-L$, so $y \not\sim y^\sigma$ and $y \circ y^\sigma \in F \cap \prod(L)$. Conversely, if $w \in F \cap \prod(L)$ then $w=(x \circ w) \circ (x \circ w)^\sigma$.

(ii) If $z^\sigma \not\sim z$ then $z \circ z^\sigma \in F$. If $z^\sigma \sim z$ then zz^σ is the only fixed line on z.

It remains to show that $z \sim x$, $y \in F$ and $x \neq y$ imply $y \in xz$. But if $y \notin xz$, then x, z, y, z^σ is a quadrangle.

(iii) If $x^\sigma \sim x$ for some x, this follows from (i) and the non-triviality of $\mathfrak{G}$. If $x^\sigma \not\sim x$ for all x, but $F = \{u\}$, then $x^\sigma \circ x = u$ for all $x \neq u$, and this is absurd.

THEOREM 4.2. *If $\mathfrak{G}$ has type $(s, t) \neq (1, 1)$, then one of the following holds for $F(\sigma)$.*

(i) *$s > 1$ and $F = x^\perp$ for some x; also, $\alpha(\sigma) = 0$ if s is odd.*

(ii) *$s > 1$ and F is a subgeometry of type (s, t'), where $t = st'(t'+1)$; also $2t'+1 \mid s^2 - 2s - 4$ and $\alpha(\sigma) = 0$ if s is odd.*

(iii) *$(s, t) = (1, 2)$ or $(1, 6)$, and either $|x^\perp - F| = 0$ or 2 for some x, or F is a subgeometry of type $(1, 2)$.*

(iv) *(G. Higman.) $(s, t) = (1, 56)$ and $|x^\perp - F| = 2$ for some x, $\chi(\sigma) = 56$, $\alpha(\sigma) = 112$, and σ is an odd permutation of the points of $\mathfrak{G}$.*

Remark. Here $\chi(\sigma)$ and $\alpha(\sigma)$ are as in (2.1).

Proof. The cases $(s, t) = (1, 2)$ and $(1, 6)$ are left to the reader.

LEMMA 4.3. *If F is a subgeometry of type (s, t'), then* (4.2 ii) *holds.*

Proof. Suppose first that $\alpha(\sigma) > 0$ and s is odd. Necessarily $L \cap F = \varnothing$ for some fixed line L. Then (4.1 i) yields $|F| = st$, whereas $|F| = 1 + s(t'+1)(st'+1)$. Thus, $s = 1$ and $t = 1 + (t'+1)^2$. Since $t = 56$ and $t' = 1, 2$, or 6 by (3.3 vi), this is absurd.

Thus, $\alpha(\sigma) = 0$ or s is even. By (4.1 ii), the number of pairs (x, z) with $z \notin F$ and $x \in F \cap z^\perp$ is

$$|F|\{s(t+1) - s(t'+1)\} = n - |F|.$$

Thus, $t = st'(t'+1)$.

In (2.1) and (3.3), $\Delta = s(2t'+1)$. By (2.1), if $\alpha(\sigma) = 0$ then Δ divides $(s-2)\cdot[1 + s(t'+1)(st'+1)] + 2st + s + 2 = s(s^2t'^2 + s^2t' + st' - 2t' + s)$. Thus, $s^2 - 2s - 4 \equiv 0 \pmod{2t'+1}$. In particular, if $s = 1$ then $t = 6$. (Note the similarity of this case to Baer involutions of projective planes.)

LEMMA 4.4. *F cannot be a subgeometry of type (s', t') with $s > s'$.*

Proof. Suppose F has type (s', t'), with n' points and $b' = n'(t'+1)/(s'+1)$ lines, where $s > s'$. Then the union of the lines in F contains $b'(s - s')$ points not in F. If w is one of these, then $w^\sigma \sim w$; if $L = ww^\sigma$ then $st = |\prod(L) \cap F| = (s't')^2$ by (4.1 i).

Let $z \notin F$. We claim that $z^\sigma \sim z$ implies that $|zz^\sigma \cap F| = s' + 1$. For, if not set $M = zz^\sigma$ and note that $|\prod(M) \cap F| = st = (s't')^2$. Since $|M \cap F| \leq 1$, it follows that $M \cap F$ is a point x and $F \subset x^\perp \cup \prod(M)$. Thus, $|F| \leq 1 + s'(t'+1) + (s't')^2$, which is not the case. This proves the claim.

Next, suppose $z^\sigma \not\sim z$. Then $z \circ z^\sigma \in F$, and by (4.1 ii) this is the unique point of F joined to z.

Now count in two ways the number of pairs (x, z) with $z \notin F$ and $x \in F \cap z^\perp$:

$$n'[s(t+1)-s'(t'+1)] = b'(s-s') \cdot (s'+1) + [n-n'-b'(s-s')] \cdot 1.$$

Plugging in $st = s'^2 t'^2$ and simplifying yields

$$s'^2(1+2t'+s't') = s(1+2s'+s't').$$

Since $(s', 1+2s'+s't') = 1$, necessarily $s'^2 \mid s$. If $s'^2 = s$, then $2t' = 2s'$, which contradicts (3.3 v). Thus, $s \geqslant 2s'^2$, so $1+2t'+s't' \geqslant 2+4s'+2s't'$, and hence $2t' > 1+s't'$. Now $s' = 1$, so $1+2t'+t' = s(1+2+t')$. Consequently, $s = (3t'+1)/(t'+3)$. Then $1 < s < 3$ contradicts (3.3 vii).

LEMMA 4.5. *If $F \subseteq x^\perp$, then either* (4.2 i) *or* (4.2 iii) *holds.*

Proof. If $x \in L = L^\sigma$, then (4.1 i) implies $L \subseteq F$. Thus, F is a union of lines on x. In particular, $|F| \equiv 1 \pmod{s}$.

Suppose $\alpha(\sigma) = 0$, and let $y \not\sim x$. Then $y^\sigma \not\sim y$, so $y \circ y^\sigma \in F$. Since y was arbitrary, $y \circ y^\sigma = x \circ y$ can be any point of $x^\perp - L$. Thus, we obtain $F = x^\perp$. By (2.1), $\sqrt{\{s(s+4t)\}}$ divides $(s-2)\{1+s(t+1)\}+2st+s+2 = s^2(t+1)$. Thus, $s \neq 1$, so (4.2 i) holds in this case.

Now assume $\alpha(\sigma) > 0$, and let $x \notin M = M^\sigma$. Suppose s is odd. Then $M \cap F = \varnothing$, so $|F| = st$ by (4.1 i). Since $|F| \equiv 1 \pmod{s}$, necessarily $s = 1$ and $|F| = 56$. There is a point $y \in x^\perp$ moved by σ. If $u \in y^\perp - \{x, y\}$, then $u^\sigma \sim u$ (as otherwise, $u \circ u^\sigma \in x^\perp$, whereas $y = u \circ x$). Thus, $\alpha(\sigma) = 2 \cdot 56$ and (4.2 iii) holds.

Consider next the case s even. Here, each fixed line meets F. Let $y \in x^\perp$ and $z \in y^\perp - xy$. If $z^\sigma \not\sim z$ then $z^\sigma \circ z \in F \subset x^\perp$, so $y = x \circ z = z^\sigma \circ z$. If $z^\sigma \sim z$ then zz^σ meets F, and $y = x \circ z \in zz^\sigma \cap F$. Thus, $F = x^\perp$ here.

LEMMA 4.6. *F cannot be a subgeometry of type (a, b, l).*

Proof. Assume it is. Let L and L' be lines with $|L \cap F| = 2$ and $|L' \cap F| = l$. Recall that $l > 2$ by definition, so $s+1 > 2$ here. Also $2 \equiv s+1 \equiv l \pmod{2}$.

By (4.1 i), $|F \cap \prod(L)| = st$, while by (3.2), $|F \cap \prod(L)| = (a-2)(b-2)$. We claim that $l = s+1$. For if not, then (4.1 i) implies that $|F \cap \prod(L')| = (a-l)^2 \equiv st$, so $(a-l)^2 = (a-2)(b-2) = (a-2)(a-l)$, whereas $l > 2$.

Now $l = s+1$ and $st = (a-2)(b-2) = (a-2)(a-s-1)$, so $a^2-(s+3)a+2s+2-st = 0$. Hence, if $\Sigma > 0$ and $\Sigma^2 = (s+3)^2-8s-8+4st = (s-1)^2+4st$, then Σ is an integer. By (3.3 i), $\Delta = \sqrt{(s^2+4st)}$ is an integer. Clearly, $\Delta > \Sigma$, so $2s-1 = \Delta^2-\Sigma^2 \geqslant \Delta+\Sigma > s+s$. This contradiction proves (4.6).

Finally, (4.2) follows from (3.2) and (4.3)–(4.6).

COROLLARY 4.7. (*G. Higman.*) *Every involution of a Moore geometry* $\mathcal{G}$ *of type* $(1, 56)$ *is an odd permutation.* $\mathrm{Aut}\,\mathcal{G}$ *is not transitive on points.*

Proof. Set $G = \mathrm{Aut}\,\mathcal{G}$. If $|G| \equiv 2 \pmod 4$ and $|G_x|$ is even for some x, G cannot be transitive on $1+57^2$ points.

Remark. For $\mathcal{G}$ as in (4.7), $3 \nmid |\mathrm{Aut}\,\mathcal{G}|$. To see this, assume $g \in \mathrm{Aut}\,\mathcal{G}$ has order 3. Then $\alpha(g) = 0$ in (2.1), so we obtain $-\chi(g)+115 \equiv 0 \pmod{15}$. Consequently, $\chi(g) > 5$ and $F(g) \subseteq x^\perp$ for some x. Let $y \in F(g) - \{x\}$. Then g acts on $y^\perp - \{x, y\}$, a set of size 56. Since g fixes no point of $y^\perp - \{x, y\}$, this is impossible.

Elementary considerations involving fixed point sets and transfer now imply that $G = \mathrm{Aut}\,\mathcal{G}$ has order dividing $2 \cdot 5^6 \cdot 7^2 \cdot 11 \cdot 13 \cdot 19$, and that $O^{2'}(G)/O_{\{5,11\}}(G)$ is cyclic of order dividing $7^2 \cdot 13 \cdot 19$. Moreover, G has a normal Sylow 11-subgroup.

COROLLARY 4.8. *Let* $\mathcal{G}$ *be a Moore geometry of type* (s, t), $s > 1$, *and suppose* $G \leqslant \mathrm{Aut}\,\mathcal{G}$ *fixes the line* xy. *If* $|G(x^\perp)|$ *and* $|G(y^\perp)|$ *are even, then* $\{\sigma \in G \mid \sigma^2 = 1$ *and* $F(\sigma) \supseteq z^\perp$ *for some* $z \in xy\}$ *is an elementary abelian 2-group.*

Proof. $[G(x^\perp), G(y^\perp)] \leqslant G(x^\perp) \cap G(y^\perp)$. If an element g in the latter group moves some point u, then $\{x \circ u, u, y \circ u, u^g\}$ contains a triangle or quadrangle. Thus, $[G(x^\perp), G(y^\perp)] = 1$. Let $\sigma \in G(x^\perp)$ and $\tau \in G(y^\perp)$ be involutions. Then $\sigma\tau$ is the identity on only one line through x or y. By (4.2), $F(\sigma\tau) = z^\perp$ for some z, and clearly $z \in xy$.

Let σ' be another involution in $G(x^\perp)$. Then $\sigma'\tau = \tau\sigma'$. Also, by the last paragraph, $\sigma' \cdot \sigma\tau = \sigma\tau \cdot \sigma'$ since clearly $z \neq x$. Thus, $\sigma\sigma' = \sigma'\sigma$. Hence, $\sigma\sigma'$ is 1 or an involution in $G(x^\perp)$. This proves the corollary. (Note the similarity between this proof and a standard argument concerning projective planes; cf. Artin [**1**], p. 57.)

COROLLARY 4.9. *Let* S *be a 2-group acting on a Moore geometry of type* (s, t) *with* s *odd. If* $F(S)$ *is a subgeometry, then it has type* (s, t') *with* $t = st'(t'+1)$.

Proof. Deny! By (4.2), there are 2-groups S and T with $S > T$, $|S : T| = 2$, $F(T)$ a subgeometry of type (s, t') with $t = st'(t'+1)$, and $F(S)$ a subgeometry of type (s, t'') with $t' = st''(t''+1)$. But then $t' > s^3$ by (3.3). Since $2t'+1 \mid s^2-2s-4$ by (4.2), this is impossible.

Remark. Suppose $\mathcal{G}$ has type (s, t) with $s > 1$ odd, and $g \in \mathrm{Aut}\,\mathcal{G}$ has order 4. If $F(g^2)$ is a subgeometry of type (s', t'), then $F(g^2) = F(g)$. For otherwise, $\chi(g) = 1 + s(t'+1)$ by (4.2, 9). Since $\mathcal{G}$ contains no quadrangles, while s is odd, $\alpha(g) = 0$ by (4.2 i, ii). Thus, (2.1) implies that $\Delta = s(2t'+1)$ divides $(s-2)[1+s(t'+1)] + 2s(t+1) - (s-2)$. This leads to the contradiction $2 \equiv 0 \pmod{2t'+1}$.

THEOREM 4.10. *Suppose σ is an involutory automorphism of a non-trivial Moore geometry of type (a, b, l). Set $F = F(\sigma)$, and let A and B be as in* (3.2). *Then one of the following holds.*

(i) $F = x^\perp$ *for some* x.

(ii) $F \subset x^\perp$, $x \in A$, $x^\perp - F \subseteq B$, F *is a union of lines through* x, $|F| = a - l > 2$, *and some fixed line is disjoint from* F *and contained in* A; *moreover,* x *is unique unless* $a - l = l$ *and* F *is a line.*

(iii) F *is a subgeometry of type* $(l-1, t)$ *for some* t, *and* $F \subseteq A$.

(iv) F *is a subgeometry of type* $(1, t)$ *for some* $t > 1$, $F \not\subseteq A$, $F \not\subseteq B$, *and each fixed line meets* F. *Moreover,* $|A \cap F|(a - t - 2) + |B \cap F|(b - t - 2) = n - |F| + j(l-2)$, *where* j *is the number of* l*-lines meeting* F *exactly twice.*

(v) F *is a subgeometry of type* (a', b', l) *for some* a', b'.

(vi) F *is a subgeometry of type* (a', b', l') *with* $l > l'$ *and* $a - l = (a' - l')^2$. *Each 2-line of* F *is contained in a 2-line of* $\mathfrak{G}$. *Every fixed line meets* F.

Remarks. Note that no analogue of (2.1) is available here. Also, $|A|$ and $|B|$ are not known, and in (v) and (vi) the relationships between A, B, A' and B' are not clear. Hence, one cannot expect results quite as precise as (4.2).

Proof. By (3.2 δ) and (4.1 i), if $L = L^\sigma \not\subseteq F$, then $|L| = l$, $L \subseteq A$, and $|F \cap \prod(L)| = a - l = b - 2$. Let n be the number of points of $\mathfrak{G}$.

Suppose $F \subset x^\perp$. By (4.1 i), F is a union of lines through x. As in the proof of (4.5), some fixed line M is not on x. By (3.2 δ), $M \subseteq A$. If now $F \cap M = \varnothing$ then $|F| = a - l$ by (4.1 i). Here $\{z \circ x \mid z \in M\}$ is a set of l points of $x^\perp - F$. Hence, $|x^\perp| \geq (a-l) + l = a = b - l + 2 > b$, so $x \in A$. Then also $\{z \circ x \mid z \in M\} = x^\perp - F$ consists of pairwise non-collinear points, and hence each corresponding line $x(z \circ x)$ has just 2 points. Thus, $x^\perp - F \subseteq B$ by (3.2 δ). Moreover, now $|F| > 2$. For if $F = \{x, y\}$ then $|xy| = 2$, $y \in B$, and $F \subset y^\perp$, which we have seen cannot occur.

Consider the case $F \cap M = \{u\}$, so l is odd. By (4.1 i), $|F| \geq |xu| + (a - l)$. As $|M| > 2$, $u \in A$. If $|xu| = 2$ then $x \in B$, so $b = |x^\perp| > |F| \geq 2 + a - l = b$. If $|xu| = l$ then $x \in A$, so $a = |x^\perp| > |F| = l + a - l$.

Thus, $F \subseteq x^\perp$ implies that (i) or (ii) holds. From now on, we may assume F is a subgeometry.

Suppose first that F has type (s, t) with $F \subseteq A$ (which certainly holds if $s > 1$). Assume $s + 1 < l$. Then $s^2 t^2 = a - l$ by (4.1 i). Then also by (4.1 i), no fixed line can miss F. By using (4.1 ii), the number of pairs (x, z) with $z \notin F$ and $x \in z^\perp \cap F$ is found to be

$$|F|(a - 1 - s(t+1)) = |F|(t+1)(s+1)^{-1}(l - s - 1) \cdot (s+1) + [n - |F| - |F|(t+1)(s+1)^{-1}(l - s - 1)] \cdot 1,$$

where $|F|(t+1)(s+1)^{-1}(l-s-1)$ is the number of points not in F lying on lines of F. Since $s^2 t^2 = a - l = b - 2$ and $n = 1 + (a-1)(b-1)$, it follows

(after simplifying and dividing by s^2t^2) that $(a-1)(1+2s+st)=s^2(t+1)$. Here, $(1+2s+st, s^2(st+1))=(1+2s+st, -2s)=(1+2s+st, 2)$. It follows that $st+2s+1$ divides $2(s+1)^2$. By (3.3 v), $st+2s+1>(s+1)^2$. Thus, $st+2s+1=2(s^2+2s+1)$. Now $1\equiv 2 \pmod{s}$, so $s=1$ and $t=5$, which contradicts (3.3 i).

Thus, if F has type (s, t) with $F\subseteq A$, then (iii) holds. Suppose F has type $(1, t)$ and $F\not\subseteq A$. Since F contains a pentagon, by (3.2 δ) there is an l-line L with $|L\cap F|=2$. Thus, l is even. By (4.1 i), $|F\cap\prod(L)|=a-l=b-2$, where $|F\cap\prod(L)|=t^2$. Since $\mathcal{G}$ is non-trivial, it follows that $t>1$. By (4.1 i), every fixed line meets F twice. By (4.1 ii), the number of pairs (x, z) with $z\notin F$ and $x\in z^\perp\cap F$ is

$$|A\cap F|(a-t-2)+|B\cup F|(b-t-2)=j(l-2)\cdot 2+[n-|F|-j(l-2)]\cdot 1,$$

where $j(l-2)$ is the number of points not in F on some line of F. This proves (iv).

Finally, suppose F has type (a', b', l'). Here $l'>2$. Let $|F\cap L|=l'$, so $|L|=l$. If (v) does not hold, then $l>l'$. By (4.1 i), $|F\cap\prod(L)|=a-l=(a'-l')^2$. Let $|F\cap M|=2$. If $|M|=l$, then $|F\cap\prod(M)|=a-l=(a'-2)(b'-2)$ by (4.1 i); since $b'-2=a'-l'\neq a'-2$, this is a contradiction. Moreover, if some fixed line met F in at most one point, then (4.1 i) would yield $|F|=a-l$ or $(a-l)+a'$, whereas $|F|\geq|F\cap\prod(L)|+a'l'$. This completes the proof of (4.10).

COROLLARY 4.11. *In* (4.10), *if l is even, $\mathcal{G}$ is neither projective nor $\mathcal{G}_{13}$ and F is a trivial Moore geometry of type $(a', 3, l')$, then $l'=l$, $a=3l+1$, $b=2l+3$, and there is a fixed line M with $M\cap F=\varnothing$.*

Proof. Let $|F\cap L|=l'$. By definition, $l'>2$, so $|L|=l$. Also, $|F\cap\prod(L)|=1$. Since $\mathcal{G}$ is non-trivial, $a-l>1$, and hence by (4.10 vi), $l'=l$ and $|F|=2l+1$.

Let L_0 be a line with $|L_0\cap F|=2$, and suppose $|L_0|=l$. Then by (4.1 i), $a-l=|F\cap\prod(L_0)|=l-1$, so $a=2l-1$. This contradicts (3.7).

Consequently, L is the only l-point line meeting F. Since $L\subset A$, it follows from (3.2 δ) that $F\cap\prod(L)=\{u\}\subset A$ and $(u^\perp-\{u\})\cap F\subseteq B$. Thus, $|F\cap A|=l+1$ and $|F\cap B|=l$.

Suppose next that each fixed line meets F. By (4.1 ii), the number of pairs (x, z) with $z\notin F$ and $x\in z^\perp\cap F$ is

$$1+(a-1)(b-1)-(2l+1)=(l+1)(a-a')+l(b-b').$$

Since $b=a-l+2$, $b'=3$, and $a'=l+1$, this yields $(a-2l)(a-l-1)=0$. Then $a=2l\not\equiv a' \pmod{2}$, which is impossible.

Thus, some fixed line M misses F. By (4.1 i), $2l+1=a-l=b-2$, as required.

The cases of affine or projective Moore geometries, which appear as exceptions in (4.10 ii) and (4.11), can actually occur. We leave it to the reader to translate properties of involutions of affine or projective planes ([6], p. 172) into the language of Moore geometries. The example of Baer involutions of affine planes has the following partial characterization.

PROPOSITION 4.12. *Let $\mathcal{G}$ be a Moore geometry, and σ an involution such that $F = F(\sigma)$ is an affine subgeometry of type $(2l', l'+2, l')$. Then one of the following holds.*

(i) *$\mathcal{G}$ is affine of type $(2l'^2, l'^2+2, l'^2)$.*

(ii) *$\mathcal{G}$ has type $(2l'^2+2l', 2l'^2+l'+2, l')$; $A \cap F$, $B \cap F$ is the natural partition of F; and some fixed line misses F.*

(iii) *$\mathcal{G}$ has type $(2l'^2, 2l'^2-l'+2, l')$; $A \cap F$, $B \cap F$ is the natural partition of F; and each fixed line meets F.*

(iv) *$\mathcal{G}$ has type $(28, 26, 4)$, $l'=4$, $|A \cap F|=30$, $|B \cap F|=6$, some 4-line meets F just twice, and each fixed line meets F.*

Proof. By (4.2), $\mathcal{G}$ must have type (a, b, l), say. Let A and B be as usual for $\mathcal{G}$, and let A' and B' be as usual for $F = F(\sigma)$. We will have to relate A' and B' to A and B, using properties of F. Each point of A' is on an l'-line of F, so $A' \subseteq A$.

Consider (4.10 vi). Here, each point of B' is on a 2-line of F, and hence is in B by (3.2 δ). Thus, $A' = A \cap F$ and $B' = B \cap F$. Each fixed line meets F, and there are exactly $l'+1$ such lines of size l. Thus, we can use (4.1 ii) to count the number of pairs (x, z) with $z \notin F$ and $x \in z^\perp \cap F$:

$$|A'|(a-a')+|B'|(b-b') = [n-|F|-(l'+1)(l-l')] \cdot 1 + (l'+1)(l-l') \cdot l'.$$

Here, $|A'| = l'^2+l'$, $|B'| = l'^2$, and $b-2 = a-l = (a'-l')^2 = l'^2$. It follows that $l = l'^2$ and $a = 2l'^2$, as desired.

Now consider the case (4.10 v), where $l = l'$. Suppose first that some fixed line M misses F. Then $a-l = |F| = 2l^2+l$ by (4.1 i). Again by (4.1 i), no l-line can meet F just twice. Thus, no point of B' can be in A, so $A' = A \cap F$ and $B' = B \cap F$. This is the conclusion of (ii).

It remains to consider the possibility where each fixed line meets F. Set $i = |A \cap B'|$. By (4.1 ii), the number of pairs (x, z) with $z \notin F$ and $x \in z^\perp \cap F$ is

$$|A'|(a-a')+i(a-b')+(|B'|-i)(b-b') = [n-|F|-i(b'-1)(l-2)] \times 1 + i(b'-1)(l-2) \cdot 2,$$

where $i(b'-1)(l-2)$ is the number of points not in F lying on lines of F. Here, $|A'| = l^2+l$, $|B'| = l^2$, $a' = 2l$, and $b' = l+2$.

Suppose $i=0$. Then

$$(l^2+l)(a-2l)+l^2(b-l-2)=1+(a-1)(b-1)-(2l^2+l).$$

Since $b-2=a-l$, this yields (iii).

Finally, suppose $i\neq 0$. Then some l-line L satisfies $|F\cap L|=2$, so l is even. By (4.1 i), $a-l=|F\cap\prod(L)|=(a'-2)(b'-2)=(2l-2)l$. It follows that $l(2l-3)=i(l-2)$, and hence that (iv) holds.

A similar result holds when $F(\sigma)$ is projective or polar.

5. Geometries having many involutions

Throughout this section, we will consider the following situation. Let $\mathcal{G}$ be a Moore geometry of type (s, t), $s>1$, such that for some $G\leqslant \mathrm{Aut}\,\mathcal{G}$, $|G(x^\perp)|$ is even for every point x. We may assume that G is generated by its involutions.

By (4.8), $E(L)=\{\sigma\in G \mid \sigma^2=1 \text{ and } \sigma\in G(x^\perp) \text{ for some } x\in L\}$ is an elementary abelian 2-group for each line L. Clearly $E(L)\trianglelefteq G_L$. Write $E(x)=E(L)\cap G(x^\perp)$.

LEMMA 5.1. *Let z be a point such that $E(L)_M=E(z)$ whenever $L\cap M=\{z\}$. Then the following hold.*

(i) *t is even.*

(ii) *G_z is transitive on the set of lines through z.*

(iii) *If $z\in L$ then G_{zL} is transitive on $(E(L)/E(z))^\#$.*

Proof. $E(L)$ is semiregular on the lines $\neq L$ through z. This proves (i) and (ii). Let bars denote images in $G_z/E(z)$. Suppose $L\cap M=\{z\}$, $\sigma\in E(L)-E(z)$, and $\tau\in E(M)-E(z)$ are such that $\bar\sigma$ and $\bar\tau$ are not G_z-conjugate. Then $\langle\bar\sigma\bar\tau\rangle$ contains an involution g, and $\bar\sigma g$ is conjugate to $\bar\sigma$ or $\bar\tau$ in $\langle\bar\sigma,\bar\tau\rangle$. Then $\bar\sigma g\in\overline{E(N)}$ for some N on z, and $\bar\sigma$ fixes N. Thus, $N=L$, so $g=\bar\sigma\bar\sigma g\in\overline{E(L)}$ and $\bar\tau$ fixes L. This contradiction proves that all involutions in $E(L)/E(z)$ are conjugate in G_z, and hence in G_{zL}.

LEMMA 5.2. *There exist lines L and M such that $L\cap M=\{x\}$ is a point and $E(L)_M>E(x)$.*

Proof. Deny! Then G is transitive on lines by (5.1 ii), and hence on points by (3.3 iv) and [6], p. 21. In particular, $|E(x)|=e$ is independent of x, and $|E(L)|=1+(s+1)(e-1)$ for each L. Since e divides $|E(L)|$, $e\mid s$. Now s and t are even.

Let $S\in Sy1_2G$. Then S fixes some x and some line L on x. By hypothesis, $E(L)$ is strongly closed in S with respect to G. Since G is flag-transitive on $\mathcal{G}$ by (5.1 ii), G_L is transitive on the subgroups $E(y)$, $y\in L$, and hence acts irreducibly on $E(L)$. Consequently, by Goldschmidt

[7], $G/O(G)$ is isomorphic to $PSL(2, q)$, $Sz(q)$ or $PSU(3, q)$ (where $q = |E(L)|$), $PSL(2, q)$ (q odd), or a group of Ree type.

Clearly, $E(L) \cap E(M) = E(x)$ whenever $L \cap M = \{x\}$. By (3.3 vii), $|E(L)| = 1 + (s+1)(e-1) \neq 4$, so $|S| \neq 4$. If $G/O(G)$ is of Ree type, then $E(L) = S$ and two conjugates of S exist whose intersection has order 4, whereas $|E(L)| = 8$ and $e = 4$ cannot both hold. Thus, $G/O(G)$ is $PSL(2, q)$, $PSU(3, q)$ or $Sz(q)$, where $q = |E(L)|$.

If $L \cap M = \{x\}$, then $E(L)O(G) = E(M)O(G)$. The connectedness of $\mathcal{G}$ now implies that $E(L)O(G)$ is independent of L. Then $G = E(L)O(G)$, which is ridiculous.

LEMMA 5.3. *If $L \cap M = \{x\}$ and $E(L)_M > E(x)$, then*
(i) $|E(M)| \leq |E(x)|^2$,
(ii) *$E(L)$ and $E(M)$ normalize one another, and*
(iii) *$E(L)E(M)$ fixes exactly one point of $\mathcal{G}$.*

Proof. Let $\tau \in E(L)_M - E(x)$, so $\tau \in E(u)$ with $u \in L - \{x\}$. Then $C_{E(M)}(\tau) = E(x)$. Regard τ as a linear transformation of the $GF(2)$-space $E(M)$. Then $\mathrm{Im}(\tau - 1) \leq \mathrm{Ker}(\tau - 1) = E(x)$. This proves (i).

Let $\sigma \in E(M)$. Then $\sigma^\tau \sigma^{-1} \in \mathrm{Im}(\tau - 1) \leq E(x)$, so $\tau\tau^\sigma \in E(x) \leq E(L)$, and hence $\tau^\sigma \in E(L)$. Then $\tau^\sigma \in E(u^\sigma) \cap E(L)$ implies that $u^\sigma \in L$. Thus, $L = xu = (xu)^\sigma$, so $E(M)$ fixes L. Interchanging L and M proves (ii), while (iii) is obvious.

LEMMA 5.4. *For each point x and line L, $|E(x)| = s$ and $|E(L)| = s^2$.*

Proof. By (5.3 iii), there is a unique orbit x^G which contains points fixed by Sylow 2-subgroups of G. Set $|E(x)| = e$.

Suppose G is point-transitive. Then $|E(L)| = 1 + (s+1)(e-1)$ for each line L. Since e divides $|E(L)|$, $e \mid s$. By (5.3 i), some L exists with $|E(L)| \leq e^2$, so $s \leq e$. Thus, $e = s$ and the result holds in this case.

We may thus assume that G is not transitive. Let $z \notin x^G$. By (5.3), we can apply (5.1) to z. In particular, t is even and G_z is transitive on the lines through z. Choose z so that, if $z \in N$, then $|E(N)|$ is minimal.

Let $S \in Syl_2 G$. Then S fixes some point x and some line M on x. We may assume $E(N) \leq S$. Then $E(M)$ normalizes $E(N)$ by (5.3 ii). If $M \neq N$, set $L = M$; if $M = N$, let L be as in (5.3). In either case, we obtain $E(L)$ normalizing $E(N)$ with $L \neq N$. By (5.3), $L \cap N = \{x\}$ and $|E(N)| \leq |E(x)|^2$.

Let $E(L)$ move z to $z' \neq x, z$, and choose $\tau \in E(z')^\#$. Then $\tau^{G_N} \subseteq E(N) - E(x)$. On the other hand, $|\tau^{E(L)}| = |E(L)/E(x)|$, while $|\tau^{G_{xN}}|$ is divisible by $|E(N)/E(z)| - 1$ by (5.1 iii). Thus,

$$|\tau^{G_N}| \geq |E(L)/E(x)|\,(|E(N)/E(z)| - 1) \geq |E(L)/E(x)|\,(|E(x)| - 1)$$

since $E(x) \cap E(z) = 1$.

We claim that $|E(L)| \geq |E(N)|$. For suppose, $|E(L)| < |E(N)|$. Then $v \in L - \{x\}$ implies that $|E(x)|\,|E(v)| \leq |E(L)| < |E(N)| \leq |E(x)|^2$. Thus, $v \notin x^G$. Our choice of z now contradicts $|E(L)| < |E(N)|$.

Thus, $|\tau^{G_N}| \geq |E(N)| - |E(x)|$. Since $\tau^{G_N} \subseteq E(N) - E(x)$, equality must hold: $|E(L)| = |E(N)|$, $E(N) = E(x)E(z)$, and G_N is transitive on $N - \{x\}$. Set $|E(z)| = f$, so $f \leq e$ by (5.3 i). Now $ef = |E(N)| = e + (f-1)s$ implies that $e = s$.

It remains to prove that $f = s$, so suppose $f < s$. Then $|E(L)| = sf$ implies that $x^G \cap L = \{x\}$. As before, G_L is transitive on $L - \{x\}$, and $|E(v)| = f$ for $v \in L - \{x\}$.

Recall that S fixes $M = L$ or N. Let L' be any line on x; we claim that $x^G \cap L' = \{x\}$, $G_{L'}$ is transitive on $L' - \{x\}$, and $|E(L')| = sf$. For, we may assume $E(L') \leq S$. Then $E(L')$ normalizes $E(M)$. Proceeding as before (with M, L' replacing N, L) we find that $G_{L'}$ is transitive on $L' - \{x\}$, $x^G \cap L' = \{x\}$, and $|E(L')| = |E(M)| = sf$, as asserted.

Thus, every line of $\mathcal{G}$ meets x^G exactly once. $z^\perp$ contains exactly $t+1$ points of x^G, while each remaining point of x^G is joined to a unique point of $z^\perp - \{z\}$ not in x^G. Thus, $|x^G| = (t+1) + [s(t+1) - (t+1)]t$. Counting in two ways the pairs (x', L') with $x' \in x^G \cap L'$, we find that $|x^G|\,(t+1)$ is the number of lines of $\mathcal{G}$. By (3.2 iii), $(t+1)^2[1 + (s-1)t] = [1 + s(t+1)(st+1)](t+1)/(s+1)$. This is impossible, and hence the lemma holds.

Remark. By [6], pp. 126, 130–132, for each L the subgroups $E(x)$, $x \in L$, determine a desarguesian affine plane.

LEMMA 5.5. *If t is even, then $s \mid t$.*

Proof. $E(L)E(M)$ must fix a line $N \neq L, M$ on x. By (5.4), $E(L)E(M)/E(x)$ acts on $N - \{x\}$ as a transitive elementary abelian group. Hence, $W = (E(L)E(M)) \cap G(N)$ has order at least s^3/s by (5.4). All involutions in W are clearly in $E(x)$. Let $u \in N - \{x\}$ and $u \in L' \neq N$. Then $W_{L'}$ is semiregular on $L' - \{u\}$, so $|W_L| \leq s$. Thus, $|L'^W| \geq s$ for each $L' \neq N$ on u. This proves the lemma.

6. Proof of Theorem 1.1

Let G be a minimal counterexample to (1.1). By (3.2), G is acting on a Moore geometry $\mathcal{G}$ of type (s, t), where $s > 1$.

Since G_x is transitive on the set of points $z \notin x^\perp$, it is transitive on the pairs (y, z) with $y = x \circ z$. Thus, G_x is 2-transitive on the set of lines through y.

Let P be a 2-group maximal with respect to having $D = F(P)$ a subgeometry.

We claim that $P \neq 1$. For suppose $P = 1$. Then § 5 applies. In particular, by (5.2) and (5.3), lines L and M exist with $L \cap M = \{x\}$ and $E(L)$ normalizing $E(M)$. The 2-transitivity of G_x implies that $E(L_1)$ normalizes $E(M_1)$ whenever $L_1 \cap M_1 \neq \emptyset$. Let $y \neq x$, and consider $\langle E(x), E(y)\rangle$. This group is clearly abelian if $y \in x^\perp$. If $y \notin x^\perp$ and $u = x \circ y$, then the group is contained in the 2-group $\langle E(xu), E(yu)\rangle$. Thus, by a well-known result of Baer ([8], p. 105), $\langle E(x)^{O}\rangle \leq O_2(G)$. But $\mathcal{G}$ has an odd number of points by (5.4), so this is absurd. Thus, $P \neq 1$.

If P is Sylow in G_{xz} for some non-collinear $x, z \in D$, then $N_O(P)^D$ has rank 3, and this contradicts the minimality of G. Thus, $N_O(P)^D_{xz}$ contains an involution σ for each such pair x, z. By (4.2), σ fixes $D \cap (x \circ z)^\perp$ pointwise. Clearly, $x \circ z$ can be any point of D.

Consequently, § 5 applies to $N_O(P)^D$. In particular, s is even.

Let $S \in S_y l_2 G_x$. Then each orbit of S of points not collinear with x has length $\geq (s^2t)_2$. Let $\sigma \in Z(S)$ be an involution. Again using (5.2, 3), we find by (4.2) that $F(\sigma)$ must have type (s, t') with $t = st'(t'+1)$. Then S acts on a subset of $F(\sigma)$ of size $s^2t'(t'+1) = st$ with orbits of length $\geq (s^2t)_2$, so $(st)_2 \geq (s^2t)_2$, which is ridiculous.

This completes the proof of (1.1).

REFERENCES

1. E. Artin, *Geometric algebra*, Interscience, New York 1957.
2. M. Aschbacher, 'The non-existence of rank three permutation groups of degree 3250 and subdegree 57,' *J. Alg.* 19 (1971), 538–540.
3. R. C. Bose and T. A. Dowling, 'A generalization of Moore graphs of diameter two,' *J. Comb. Theory* 11 (1971), 213–226.
4. P. J. Cameron, 'Permutation groups with multiply transitive suborbits,' *Proc. LMS* 25 (1972), 427–440.
5. P. J. Cameron, 'Biplanes,' *Math. Z.* 131 (1973), 85–101.
6. P. Dembowski, '*Finite geometries*,' Springer, Berlin-Heidelberg-New York, 1968.
7. D. Goldschmidt, '2-Fusion in finite groups,' *Annals of Math.* 99 (1974), 70–117.
8. D. Gorenstein, *Finite groups*, Harper and Row, New York, 1968.
9. D. G. Higman, 'Finite permutation groups of rank 3,' *Math. Z.* 86 (1964), 145–156.
10. D. G. Higman, 'Primitive rank 3 groups with a prime subdegree,' *Math. Z.*, 91 (1966), 70–86.
11. D. G. Higman, 'Partial geometries, generalized quadrangles and strongly regular graphs,' pp. 263–293 *in Atti Conv. geom. combinat.*, Perugia, 1971.
12. A. J. Hoffman and R. R. Singleton, 'On Moore graphs with diameters 2 and 3,' *IBM J. Res. Dev.* 4 (1960), 497–504.
13. L. L. Scott, 'Uniprimitive groups of degree kp.' Ph.D. thesis, Yale U. 1968.

University of Oregon
Eugene, Oregon 97403
U.S.A.