GENERALIZED QUADRANGLES HAVING A PRIME PARAMETER†

BY

WILLIAM M. KANTOR

ABSTRACT

Generalized quadrangles $\mathcal{Q}$ are studied in which $s$ or $t$ is prime and $\text{Aut}(\mathcal{Q})$ has rank 3 on points.

1. Introduction

A generalized quadrangle $\mathcal{Q}$ of order $(s, t)$ consists of a set of points and lines, with each line on $s+1$ points and each point on $t+1$ lines, such that two points are on at most one line and a point not on a line is collinear with exactly one point of the line. We will study the case where $s$ or $t$ is prime and $\text{Aut}(\mathcal{Q})$ has rank 3 on points.

**Theorem 1.1.** Let $\mathcal{Q}$ be a generalized quadrangle of order $(p, t)$ with $p$ prime and $t > 1$. Suppose $G = \text{Aut}(\mathcal{Q})$ has rank 3 on points. Then either $t = p^2 - p - 1$ and $p^3 \mid |G|$, or $G = \text{PSp}(4, p)$ or $P_1 U(4, p)$ and $\mathcal{Q}$ is one of the usual quadrangles associated with these groups, or $p = 2$, $G = A_6$ and $\mathcal{Q}$ is one of the usual quadrangles associated with $PS_6(4, 2)$.

A group $G$ having a $BN$-pair whose Weyl group is $D_8$ naturally acts as an automorphism group of a generalized quadrangle of order $(s, t)$ with $s > 1$ and $t > 1$. Moreover, $(1 + s)(1 + t)(1 + st)s^2t^2$ divides $|G|$. Thus, as an immediate consequence of (1.1) we have:

**Corollary 1.2.** Let $G$ be a finite group having $BN$-pair and Weyl group $D_8$. Suppose that $|P : B| = 1$ is a prime $p$ for some maximal parabolic subgroup $P$. Then $G$ has a normal subgroup $H$ isomorphic to $\text{PSp}(4, p)$ or $\text{PSU}(4, p)$, with the usual $BN$-pair induced on $H$.

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

Received November 14, 1974

Vol. 23, 1976

GENERALIZED QUADRANGLES HAVING A PRIME PARAMETER

**Corollary 1.3.** Let $G$ be a rank one, prime, $p \nmid \gamma$, $(\gamma, \delta) = 1$, $r$ a power of $\delta = 1$. Then $G$ can be regarded as an orthogonal geometry over $GF(p)$.

**Corollary 1.3** is a consequence of the preceding sort also followed by other methods. The proof of (1.1) requires for both reason, and later considerations in Section 4.

The basic idea is to take a Sylow $p$-subgroup of the center and various point-and line methods yield the following results:

**Theorem 1.4.** Let $\mathcal{Q}$ be a generalized quadrangle of order $(p, t)$ with $p$ prime and $s > 1$. Suppose $G = \text{Aut}(\mathcal{Q})$, $s \neq p^2 - p - 1$ or $p^3 \mid |G|$. Then $G$ is the usual quadrangles associated with $\text{PSp}(4, p)$ or $P_1 U(4, p)$.

We remark that there is a well-known result on the size of $3^2 | \text{Aut}(\mathcal{Q}) |$ (see, e.g., Higman [2], p. 391 on lines).

Finally, we note that the methods employed in this paper, such as rank 4 automorphism group, are proved to be $p$ prime.

2. Preliminary results

Let $\mathcal{Q}$ be a generalized quadrangle of order $(p, t)$.

**Lemma 2.1.** Let $\mathcal{Q}$ be a generalized quadrangle having $\mathcal{Q}$ the set of points $y$ such that a line is not a complement of $x^2$. We call $x$ and $y$ lines $L$ and $M$ are adjacent if $L \cap M$.

Let $H(x)$ denote the set of elements $H(L)$ is the pointwise stabilizer of $L$.

**Lemma 2.1.** Let $\mathcal{Q}$ be a generalized quadrangle having $\mathcal{Q}$ the set of points $p$.

(i) Suppose a subgroup $H$ of $\text{Aut}(\mathcal{Q})$ is

(a) $\mathcal{Q}$

(b) $\mathcal{Q}$

(c) $\mathcal{Q}$

(d) $\mathcal{Q}$

(e) $\mathcal{Q}$

(f) $\mathcal{Q}$

(g) $\mathcal{Q}$

(h) $\mathcal{Q}$

(i) $\mathcal{Q}$

(j) $\mathcal{Q}$

(k) $\mathcal{Q}$

(l) $\mathcal{Q}$

(m) $\mathcal{Q}$

(n) $\mathcal{Q}$

(o) $\mathcal{Q}$

(p) $\mathcal{Q}$

(q) $\mathcal{Q}$

(r) $\mathcal{Q}$

(s) $\mathcal{Q}$

(t) $\mathcal{Q}$

(u) $\mathcal{Q}$

(v) $\mathcal{Q}$

(w) $\mathcal{Q}$

(x) $\mathcal{Q}$

(y) $\mathcal{Q}$

(z) $\mathcal{Q}$

[Note: The above text is a sample of plain text representation of the document content. For a comprehensive understanding, please refer to the original document.]
Corollary 1.3. Let $G$ be a rank $3$ group having subdegrees $1$, $p$, $p^2$ with $p$ a prime, $p^t = \gamma \delta$, $(\gamma, \delta) = 1$, $t$ a power of $p$, $r > 1$ and either $(1 + \delta)r \equiv \gamma \pmod{p}$ or $p = 2$ and $\delta = 1$. Then $G$ can be regarded as acting on the singular points of a symplectic or orthogonal geometry over $GF(p)$, or on the singular lines of a $4$-dimensional symplectic or unitary geometry over $GF(p)$.

Corollary 1.3 is a consequence of (1.1) and Kantor [4]. Further consequences of the preceding sort also follow from the latter paper. The present work originated in an attempt to push the rather elementary methods of [4] somewhat further. The proof of (1.1) requires little more than elementary group theory, combined with results of Higman [1], [2], [3]. The case $t = p$ is especially simple; for both this reason, and later convenience, it has been presented separately in Section 4.

The basic idea is to take a Sylow $p$-subgroup $P$ of $G$, and then see how both its center and various point- and line-stabilizers in $P$ must behave. The same methods yield the following result; the details are left to the reader.

Theorem 1.4. Let $\mathcal{Q}$ be a generalized quadrangle of order $(s, t)$ with $s > 1$ and $t$ prime and $s > 1$. Suppose $G = \text{Aut} \mathcal{Q}$ has rank $3$ on points, $p^t \mid G$, and either $s \not= p^2 - p - 1$ or $p^t \mid G$. Then $G \equiv \text{PSP}(4, p) \text{ or } \text{PGL}(4, p)$, and $\mathcal{Q}$ is one of the usual quadrangles associated with these groups.

We remark that there is a well-known quadrangle of order $(3, 5)$ for which $3^t \mid |\text{Aut} \mathcal{Q}|$ (see, e.g., Higman [2], p. 287); $\text{Aut} \mathcal{Q}$ has rank $3$ on points and rank $5$ on lines.

Finally, we note that the methods presented here apply to other situations, such as rank $4$ automorphism groups of generalized hexagons of order $(p, p)$ with $p$ prime.

2. Preliminary results

Let $\mathcal{Q}$ be a generalized quadrangle of order $(s, t)$. If $x$ is a point, $\Gamma(x)$ denotes the set of points $y$ such that a line $xy$ exists, $x^{+} = \{x\} \cup \Gamma(x)$, and $\Delta(x)$ is the complement of $x^{+}$. We call $x$ and $y$ joined or adjacent if $xy$ exists; and dually lines $L$ and $M$ are adjacent if $L \cap M$ is a point.

$H(x)$ will denote the set of elements of $H \cong \text{Aut} \mathcal{Q}$ fixing each line on $x$, while $H(L)$ is the pointwise stabilizer of $L$.

Lemma 2.1. Let $\mathcal{Q}$ be a generalized quadrangle of order $(s, t)$.

(i) Suppose a subgroup $H$ of $\text{Aut} \mathcal{Q}$ fixes at least three points of some line and
at least three lines through some point. If no fixed point $H$ is joined to all others, and no fixed line meets all others, then the set of fixed points and lines of $H$ form a sub-quadrangle of order $(s', t')$ for some $s' \leq s$ and $t' \leq t$.

(ii) If $\mathcal{D}$ has a proper subquadrangle of order $(s, t)$, then $t \geq st'$.

(iii) $t' \geq s$ and $s' \geq t$ if $s > 1$ and $t > 1$.

**Proof.** (i) is straightforward. To prove (ii) (which is due to Payne [6] and Thas [7]), take $x$ outside of the subquadrangle $\mathcal{D}$. Then each of the $t + 1$ lines through $x$ meets $\mathcal{D}$; at most once. Counting in two ways the pairs $(y, L)$ with $y \in L$, $x$ and $y$ collinear, and $y, L \in \mathcal{D}$, we find that $(t + 1)(t' + 1) \geq 1 + (s + 1)t' + st'^2$ (the latter being the number of lines of $\mathcal{D}$). This implies that $t \geq st'$.

Finally, (iii) is Higman's inequality [2].

The second part of the following transitivity-boosting lemma is probably well-known; the proof of the first part has the same flavor as the one in Kantor [4].

**Lemma 2.2.** Suppose $G \leq \text{Aut} \mathcal{D}$ has rank 3 on points. Then

(i) $G$ is 2-transitive on the lines through $x$; and

(ii) If $(s, t + 1) = 1$ and $y \in \Gamma(x)$, then $G_{xy}$ is transitive on $y^t - xy$.

**Proof.** (i) Let $x \in L$. Then $G_L$ contains a Sylow $p$-subgroup $P$ of $G$, for each prime $p | t$. It suffices to show that for each $P$ and $P$, each orbit $L^P$ of lines $\not\in L$ on $x$ has length divisible by $t_p$ (the $p$-part of $t$).

Suppose $|L^P| < t_p$ for some such orbit. There exist points $y \in L - \{x\}$ and $y' \in L' - \{x\}$ whose $P_L = P_{L'}$ orbits have lengths $\equiv s_p$. Thus, $|P_L_{xy'}| \geq |P_L|/s_p^2 > |P|/s_p^2 t_p$, so $|P^*: P_{xy'} < s_p^2 t_p \leq |\Delta(y)|_{t_p}$ for a Sylow $p$-subgroup $P^* \leq P_{xy'}$ of $G_{xy'}$. Since $y' \in \Delta(y)$ and $G_{xy'}$ is transitive on $\Delta(y)$, this is impossible.

(ii) Since $(\Gamma(x), |\Delta(x)|) = (s(t + 1), s't^2) = s$, each $G_{xy}$-orbit on $\Delta(x)$ has length divisible by $s't^2/s = |y^t - xy|$.

**Remark.** Note that the hypotheses of (2.2) guarantee that $G_L$ is 2-transitive on $L$. What (2.2) says is that a second 2-transitive group is also always available.

**Lemma 2.3.** The pointwise stabilizer $G(x^t)$ of $x^t$ is semiregular on $\Delta(x)$, and $|G(x^t)| = t$.

**Proof.** The first statement is (6.17) of Higman [2], and follows immediately from (2.1 i). To prove the second one, let $M$ be a line not on $x$, and set $y = x^t \cap M$. Then each $u \in x^t - xy$ is joined to some $w \in M - \{y\}$, and hence $G(x^t)_u \cong G(x^t)_w = 1$.

**Theorem 2.4.** (Higman [1]) If $s = t = |G(x^t)|$. Then $\mathcal{D}$ is isomorphic to $G \cong \text{PSp}(4, s)$.

**Theorem 2.5.** (Higman [3]) If $s = t^2$ and $|G(x^t)| = t$. Then $G \cong \text{PSU}(4, t)$, and $G \cong \text{PSU}(4, t)$.

**Lemma 2.6.** (Higman [2])

**Corollary 2.7.** Suppose $s 

(i) If $s | t + 1$ then $t = s$

(ii) If $s | t - 3$ and $3 | s - 1$

(iii) If $s | t - 2$ then $t = s$.

**Proof.** We will prove (iii). We can write $s^t - 1 = \alpha(s + 1)$ and $\alpha \equiv 3 \text{ (mod } s)$, so $\alpha = (s - 1)/3 + (s^t - 1)/s$.

3. Hyperbolic lines

Let $\mathcal{G}$ be any strongly regular graph on point $x$. $\Gamma(x)$ will denote the set of points $\not\in x$ not joined to $x$. We have

(3.1) $xy = \cap \{w^t : w \not\in \mathcal{G} \}$

This line is called singular.

**Lemma 3.2.** (Higman [2], Theorem 2.4)

(i) Two adjacent points are singular.

(ii) Two non-adjacent points are singular, if $\mathcal{G}$ is the point line.

Consider the following hypotheses:

(H) Each hyperbolic line is singular.

This will be the case, for instance, when all pairs of non-adjacent points are singular.
Theorem 2.4. (Higman [1]) Assume \( G \leq \text{Aut } \mathcal{Q} \) has rank 3 on points, and \( s = t = |G(x^*)| \). Then \( \mathcal{Q} \) is isomorphic to the usual quadrangle for \( Sp(4, s) \), and \( G \cong PSp(4, s) \).

Theorem 2.5. (Higman [3]) Assume \( G \leq \text{Aut } \mathcal{Q} \) has rank 3 on points, \( s = t^2 \) and \( |G(x^*)| = t \). Then \( \mathcal{Q} \) is isomorphic to the usual quadrangle for \( PSU(4, t) \), and \( G \cong PSU(4, t) \).

Lemma 2.6. (Higman [2, (6.1)]) \( s^2(1 + st)/(s + t) \) is an integer.

Corollary 2.7. Suppose \((s, t) = 1, s > 1 \) and \( t > 1 \).

(i) If \( s | t \) then \( t = s^2 - s - 1 \).

(ii) If \( s | t - 3 \) and \( 3 | s - 1 \) then \( t = 2s + 3 \).

(iii) If \( s | t - 2 \) then \( t = s + 2 \).

Proof. We will prove (ii); (i) and (iii) are similar. By (2.6), \( s + t | s^2 - 1 \). We can write \( s^2 - 1 = \alpha(\alpha + t) \) and \( t - 3 = \beta s \) for integers \( \alpha \) and \( \beta \). Then \( -1 = 3a \mod s \), so \( \alpha = (s - 1)/3 \mod s \). Write \( \alpha = ((s - 1)/3) + sy \). Then \( s^2 - 1 = \((s - 1)/3 + sy)(s + t) \) implies that \( y = 0 \) and \( 3(s + 1) = s + t \), as required.

3. Hyperbolic lines

Let \( \mathcal{G} \) be any strongly regular graph with parameters \( n, k, \lambda, \mu \). For each point \( x \), \( \Gamma(x) \) will denote the set of points joined to \( x \), and \( \Delta(x) \) the set of points \( x \) not joined to \( x \). Write \( x^* = \{x\} \cup \Gamma(x) \). The line \( xy, x \neq y \), is defined by

\[
xy = \bigcap \{w^* \mid x, y \in w^*\} = \bigcap \{w^* \mid w \in x^* \Delta(x)\}.
\]

This line is called singular if \( y \in \Gamma(x) \) and hyperbolic if \( y \in \Delta(x) \).

Lemma 3.2. (Higman [2, p. 282].)

(i) Two adjacent points are on a unique singular line.

(ii) Two non-adjacent points are on at most one hyperbolic line, and are on no singular line, if \( \mathcal{G} \) is the point-graph of a generalized quadrangle.

Consider the following hypothesis:

(H) Each hyperbolic line has \( h + 1 \) points, and two distinct lines meet at most once.

This will be the case, for example, if (3.2i) holds and \( \text{Aut } \mathcal{G} \) is transitive on pairs of non-adjacent points.
LEMMA 3.3. Assume (H). Then the following hold.
(i) \( x \) is on \( l/h \) hyperbolic lines.
(ii) There are \( nl/h(h + 1) \) hyperbolic lines.
(iii) \( h \mid k - \lambda - 1. \)
(iv) If \( w \in \Delta(x) \) then \( w \) is on \( l/h - (k - \mu + 1) \) hyperbolic lines missing \( x^\perp \).
(v) There are \( [(l/h - (k - \mu + 1))/(h + 1)] \) hyperbolic lines missing \( x^\perp \).

PROOF. (i) and (ii) are easy. If \( y \in \Gamma(x) \) then \( y^\perp \cap \Delta(x) \) is a union of hyperbolic lines with \( x \) removed; this implies (iii).

To prove (iv), note that \( w \) is joined to \( \mu \) points of \( \Gamma(x) \). Let \( y \) be any of the remaining \( k - \mu \) points of \( \Gamma(x) \). If \( wy \) meets \( \Gamma(x) \) at a second point \( y' \neq y \), then by (H), \( y' \in \Delta(y) \) and \( wy = yy' \). But now, \( y, y' \in x^\perp \) implies that \( yy' \subseteq x^\perp \), and hence that \( w \in x^\perp \).

Thus, \( w \) is on exactly \( k - \mu \) hyperbolic lines meeting \( x^\perp \). By (i), this proves (iv).

Finally, count the pairs \((w, L)\) with \( w \in \Delta(x) \cap L \), \( L \) a hyperbolic line, and \( L \cap x^\perp = \phi \), in order to obtain (v).

COROLLARY 3.4. If (H) holds, and \( Aut \mathcal{F} \) is transitive on hyperbolic lines, then each hyperbolic line misses exactly \( l - h(k - \mu + 1) \) sets \( x^\perp \).

PROOF. By (3.3), the desired number is
\[
n \cdot l[[l/h - (k - \mu + 1)]/(h + 1)] \cdot (nl/h(h + 1))^-1.
\]

LEMMA 3.5. If (H) and (3.2ii) hold, then
(i) \( x^\perp \) contains \( s't(t + 1)/h(h + 1) \) hyperbolic lines; and
(ii) \( |G(x^\perp)| \) divides \( h \).

PROOF.
(i) Count the pairs \((y, H)\) with \( y \in H \subset x^\perp \) and \( H \) a hyperbolic line.
(ii) Higman [2, (6.17)].

4. The case \( s = t = p \)

Theorem 1.1 is particularly easy when \( s = t = p \) is prime. We may assume \( p > 2 \). Let \( P \) be a Sylow \( p \)-subgroup of \( G \). Then \( P \) fixes some \( x \) and some (singular) line \( L \) on \( x \). Moreover, \( P \) is transitive on \( L - \{x\}, \Delta(x) \) and \( x^\perp = L \) (by (2.2)). Set \( Z = Z=P \cap P(x) \cap P(L) \). Since \( p^2 = |\Delta(x)| \) \( |G|, Z \neq 1. \)

Let \( w \in \Delta(x) \), and suppose \( P_w \neq 1 \). Then \( P_w = P(wy) \) if \( y \in L \cap \Gamma(w) \). If now \( Z \) is transitive on the lines \( \neq L \) on \( y \), then \( P_w \subseteq G(y^\perp) \) and Higman's result (2.4)

applies. Assume next that \( Z \neq 1 \) and fixes every line meeting \( L \). Hence, if \( G \) has rank 3 on lines. But by \( |K^p| \leq p^r \) for a line \( K \) on \( w \). Thus by (2.1), the set of fixed points and \( (p, p) \), which is absurd.

Thus, we may assume \( |P| = p \) and \( n \) is a nonadjacent points. In particular, regular on \( \Delta(x) \), so \( G \) has rank 3 on lines, and \( P \) has a subgroup of order \( p \) by the Frattini argument. \( N(P) \) hence induces at least \( SL(2, p) \) on \( P(L) \).

Moreover, \( |Z| = p \) here, and we may permit (2.4) to be applied to the \( 2 \)-transitive on the \( p + 1 \) subgroups, \( SL(2, p) \) on \( P(L) \).

In view of the action of \( N(P(x)), N(P(L)) \) which inversions each of the \( p + 1 \) subgroups, hence \( t \in G(x) \). Similarly, there then centralizes \( P(L) \) and centralizes \( P = \{t, t'\} \leq N(P(x)) \cap N(P(L)) \) is a subgroup of \( P \).

Now \( t' \) centralizes \( Z \) and is \( t \) as well.

Then also \( t' \) fixes one of the \( p + 1 \) points of \( L, s \) shows that \( t \in G(L_1) \), and hence \( Z \) is transitive on the lines \( \neq l \).

The case \( s = t = p \) is completed.

5. The case \( s = p \) and \( p > 2 \)

Let \( G \) and \( P \) be as in Theorem 1.1. Assume \( P \) fixes some point \( x \). Set \( Z = P \cap P(L_1) \).

It is easy to handle the case \( p > 2 \). By Section 4, we may assume \( t' = t \).

Throughout this section we will use the following lemma.

LEMMA 5.1. \( t > p \).
applies. Assume next that \( Z \leq G(y) \). Then the transitivity of \( P \) shows that \( Z \) fixes every line meeting \( L \). Hence, Higman’s result (2.4) applies to the dual of \( Z \) if \( G \) has rank 3 on lines. But by (2.2), if \( G \) does not have rank 3 on lines, then \( |K^x| \leq p^3 \) for a line \( K \) on \( w \). This implies that \( |P_x| \geq p^3 \), so \( P_{xw} \neq 1 \). Then, by (2.1), the set of fixed points and lines of \( P_{xw} \) form a subquadrangle of order \((p,p)\), which is absurd.

Thus, we may assume \( |P| = p^3 \). Then no nontrivial \( p \)-element can fix two nonadjacent points. In particular, \( P(L) = P \), is regular on \( x^+ - L \). (Also, \( P \) is regular on \( \Delta(x) \), so \( G \) has rank 3 on lines.) Since \( |P(x)| = p^3 \), we see that \( P(x) \) has \( p + 1 \) subgroups of order \( p \), each fixing a unique line on \( x \) pointwise. Hence, by the Frattini argument, \( N(P(x)) \), is 2-transitive on these \( p + 1 \) subgroups, and hence induces at least \( SL(2,p) \) on \( P(x) \).

Moreover, \( |Z| = p \) here, and \( Z = P(x) \cap P(L) \). Thus, \( Z \leq P(y) \) would again permit (2.4) to be applied to the dual of \( Z \). It follows as above that \( N(P(L)) \), is 2-transitive on the \( p + 1 \) subgroups of order \( p \) of \( P(L) \), and induces at least \( SL(2,p) \) on \( P(L) \).

In view of the action of \( N(P(x)) \), on \( P(x) \), there is a 2-element \( t \in N(P(x)) \cap N(P(L)) \) which inverts \( P(x) \) and centralizes \( P(L) / Z \). Then \( t \) normalizes each of the \( p + 1 \) subgroups of \( P(x) \) corresponding to the lines on \( x \), and hence \( t \in G(x) \). Similarly, there is a 2-element \( t' \in N(P(L)) \cap N(P(x)) \) which inverts \( P(L) \) and centralizes \( P(x) / Z \). By Sylow’s theorem, we may assume that \( (t,t') \leq N(P(x)) \cap N(P(L)) \) is a 2-group.

Now \( t' \) centralizes \( Z \) and inverts \( P/Z \) and \( t' \) fixes some line \( L_1 \neq L \) on \( x \). Then also \( t' \) fixes one of the \( p \) points of \( L_1 - \{x\} \), and the transitivity of \( Z \) on \( L_1 - \{x\} \) shows that \( t' \in G(L_1) \). Dually, \( t' \in G(y) \) for some \( y \in L - \{x\} \). (Recall that \( Z \) is transitive on the lines \( \neq L \) on \( y \).) Thus, (2.11) implies that the set of fixed points and lines of \( t' \) is a subquadrangle of order \((p,p)\). This is ridiculous, and the case \( s = t = p \) is completed.

5. The case \( s = p \) and \( p^3 \mid G \)

Let \( Z \) and \( G \) be as in Theorem 1.1. Let \( P \) be a Sylow \( p \)-subgroup of \( G \). Then \( P \) fixes some point \( x \). Set \( Z = Z(P) \).

It is easy to handle the case \( p = 2 \) (since \( t \leq p^2 \) by (2.1)). We may thus assume \( p > 2 \). By Section 4, we may also assume \( p \neq t \).

Throughout this section we will assume \( p^3 \mid G \).

**Lemma 5.1.** \( t > p \).
PROOF. Suppose $t < p$. Then $P \leq G(x)$. As $|\Delta(x)| = p^t$, $P_\omega \neq 1$ for some $w \in \Delta(x)$. Certainly, $P_\omega = P(\omega y)$ for each $y \in x^\omega \cap w^\omega$. By (2.1i), the set of fixed points and lines of $P_\omega$ form a subquadrangle of order $(p, t)$, which is absurd.

**Lemma 5.2.** $p \not| t$.

**Proof.** Suppose $p \not| t$. By (2.1) and (5.1), $p < t < p^2$. Also, for some $w \in \Delta(x)$, $P_\omega \neq 1$ and $P_\omega$ is Sylow in $G_\omega$.

Consider first the possibility $p | t + 1$. Here no nontrivial subgroup of $P$ can fix elementwise a subquadrangle of $I_2$. For, by (2.1) such a quadrangle would have order $(p, t)$ with $p|t + 1 < p^2$ and $p | t + 1$, so $t = p - 1$. However, by (6.2) no quadrangle of order $(p, p - 1)$ can exist.

On the other hand, $|P_\omega| \equiv p^2$ for one of the $p^2$ lines $K$ not on $x$. Then $P(K) \neq 1$, and we may assume $w \in K$. Now $P(K)$ fixes at least $p$ lines $L$ on $x$, and at least $p$ on $w$. Since $w$ is joined to some point of $L' - \{x\}$, this contradicts (2.1) and the preceding paragraph.

From now on we may assume $p \not| t + 1$. Then $p$ fixes some line $L$ on $x$. Moreover, the set $L$ of fixed points and lines of $P_\omega$ forms a subquadrangle, necessarily of order $(p, t)$ for some $t \equiv 1 \pmod p$. Here $t = t (\mod p)$, while $p|t < p^2$ by (2.1), also, since $P_\omega$ is Sylow in $G_\omega$, $N(P_\omega)$ is transitive on the ordered pairs of non-adjacent points of $\omega$.

We claim that $|P| = p^3$. For suppose $|P| \geq p^4$. Then $1 \neq P_\omega < P^\omega$ for some line $L$ on $x$. The set of fixed points and lines of $P_\omega$ forms a subquadrangle $I_2 \supset I_1$ of $I_2$ of order $(p, t)$ for some $t$. By (2.1), $p^2 < p^2 < t < p^3$, which is impossible.

Thus, $|P| = p^3$ and $|P_\omega| = p$. But the transitivity of $N(P_\omega)$ implies that $P^3 | (N(P_\omega))$. Hence $P_\omega \leq Z(P)$.

Since $x^\omega - L = \omega \not= 0 \pmod p^2$, $|P_\omega| \equiv p^2$ for some $u \in x^\omega - L$. Then $P_\omega$ is not conjugate in $G$ to any $P_\omega$, so $P_\omega$ fixes no point of $x^\omega - x$. Thus, $Z(P)$ fixes $x$. There are thus exactly $t + 1$ lines $xu$ with $|P(xu)| \geq p^2$. If $v$ is any point of $x^\omega$ not on any of these lines, then $v^p < p^t$, so $P_\omega \neq 1$ and $Z(P) \equiv C(P(xu))$ implies that $P(xu)$ fixes a second line on $x$ pointwise, and hence determines a subquadrangle of order $(p, t)$, say. But this time, $p \equiv t$, and this contradicts (2.1).

By (5.2), we now know $P$ fixes some line $L$ on $x$. Let $t_\omega$ denote the $p$-part of $t$.

**Lemma 5.3.** If $p^2 t_\omega$ divides $|G|$, then the conclusions of (1.1) hold.

**Proof.** By (5.2), $p | t$, then $|P| \geq p^4$, and $|P| \geq p^3$ if $t = p^2$. By (2.1), $t \leq p^2$.

We have $|\Delta(x)| = p^2 t = 0 \pmod {p^2}$. Let $w \in \Delta(x)$. Then $p^3 \geq p^2 t \equiv w^p \equiv p^3$, so $w^p \equiv p^3$. In particular, $P_\omega \equiv P^3$. Note that $P_\omega = P(xy)$ if $y = L \cap w^\omega$.
We claim that $P_x$ fixes no point of $\Delta(y)$. For otherwise, by (2.1) $P_x$ fixes elementwise a subquadrangle of order $(p, t_1)$, where $pt_1 \leq p^2$ and $p | t_1$. Thus, $t = p^2$, so $P_x \cong p^3$. Now $t - t_1 < p^3$ implies that, for some line $M \neq L$ on $x$, $P_x > P_{x.M}$. Then $P_{x.M}$ fixes more than $p + 1$ lines through $x$; by (2.1), it determines a subquadrangle of order $(p, t_3)$ with $pt_3 \leq p^2$ and $t_3 > t_1$. This contradiction proves our claim.

Thus, $P_x$ fixes only points of $y^2$. Since $w$ and $y$ are arbitrary, $Z = Z(P)$ fixes each point of $L$.

Let $u \in x^4 - L$. Since $pt \leq p^3$, by (2.2) each $P$-orbit on $x^4 - L$ has length $pt$. Thus, $P: P_{x.L} = p_t$. Clearly, $P_x$ has an orbit $\{ux\}$ of lines $K$ on $u$ of length $\leq t$. Thus, $P: P_{x.L} = |P: P_{x.L}| \leq pt$, so $P_{x.K} \neq 1$.

We claim that all fixed lines of $P_{x.K}$ are adjacent to $ux$. For otherwise, by (2.1) the set $\mathfrak{Z}$ of fixed points and lines of $P_{x.K}$ is a subquadrangle of order $(p, t_3)$ (as $P_{x.K} \cong P(ux)$ fixes at least $p + 1$ lines on $x$). Here $p^2 \leq t \leq pt$, by (2.1), while $p | t_3$. Thus, $t = p^2$ and $t_3 = p$. By (2.1), $P_{x.K}$ must be semiregular on the $t - t_3$ lines through $x$ it moves, so $|P_{x.K}| = p$. Thus, $|K^p| \geq p^3$, so $K^p$ consists of all lines not adjacent to $L$. Moreover, $N_x(P_{x.K})$ is transitive on $K^p \cap \mathfrak{Z}$, and hence (by intersecting these lines with $x^3$) also on $(x^4 - L) \cap \mathfrak{Z}$. Since $L$ can be any line of $\mathfrak{Z}$, it follows that $N(P_{x.K})$ has rank 3 on the dual of $\mathfrak{Z}$. Moreover, $p^4 \nmid |N(P_{x.K})|$, since $P_{x.K}^p = 1$. By Section 4, this is impossible, and our claim is proved.

Thus, $Z \cong C(P_{x.K})$ must fix $ux$. As $u \in x^4 - L$ was arbitrary, we now have $Z \cong P(x) \cap P(L)$.

Let $G(L^*)$ denote the set of elements of $G$ fixing every line adjacent to $L$. Suppose that $Z \cap G(L^*) \neq 1$. By (2.3) (applied to the dual of $\mathfrak{Z}$), $|G(L^*)| \geq p$. Thus, $G(L^*) \cong Z$. Clearly, $G(L^*) \cong G_e$. Set $E = (G(M^*P)|x \in M)$. Then $E \subseteq G(x)$ is elementary abelian, and $G_e$ acts 2-transitively on the $t + 1 > p + 1$ groups $G(M^*)$. In particular, $|E| \geq p^3$. But $GL(3, p)$ has no such 2-transitive subgroup since $t + 1 > p^2 + p + 1$ (Mitchell [5]). Thus, $|E| \geq p^5$. If now $t < p^2$ then $|P| \geq p^3$. Then $|P_e*| = p^3$, so $P_e > P_e* \neq 1$ for some line $K$ adjacent to $y^w$. (Note that $P_{x.K} \cong G((yx)^w)$.) As usual, $P_e*_{x.K}$ determines a subquadrangle, and (2.1) produces a contradiction. Thus, $t = p^2$, so $|xu^w| = p^3$. By (2.5), we may assume that $G$ does not have rank 3 on lines. Then $|K^p| \leq p^4$ for each line $K$ not adjacent to $L$, so $|P_{x.K}| \geq p^3$. As usual, (2.1) implies that for $w \in K \cap \Delta(x)$, the set of fixed points and lines of $P_{x.K}$ form a quadrangle of order (p, p). Hence, again by (2.1), $|P_{x.K}| = p$, $|P_{x.K}| = p^3$, and hence $|P| = p^6$. Now $P: P(x) \cong p^3 = |xu^w| = t$ shows that no subgroup of $P$ can fix exactly $p + 1$ lines on $x$, whereas $P_{x.K}$ is such a subgroup.

Thus, we may assume that $Z \cap G(L^*) = 1$, and (eventually) will derive a
contradiction from this assumption. Since \( P \) is transitive on \( L - \{ x \} \), \( Z \cap P(y) = 1 \) for each \( y \in L - \{ x \} \). Since \( P(L) \) is Sylow in \( G(L) \), we can find \( g \in G_t \) such that \( P^t \cong P(L) \) and \( P^t \) is Sylow in \( G_{at} \). Set \( W = Z^t \). Then \( W \leq P(L) \).

Moreover, \( P_c \leq P(L) \leq C_t(W) \).

Recall that all fixed points of \( P_c \) are in \( y^t \). Since \( P_c \) fixes \( L \) and \( wy \), pointwise, while \( N(P_c) \) is transitive on ordered pairs of non-adjacent fixed points of \( P_c \), we must have \( |N : P_c| \equiv |L - \{ y \} : wy - \{ y \}| = p^2 \), where \( N = N_t(P_c) \).

We can now prove \( t = p^2 \). By (2.1), \( P_c \) is semiregular on the lines \( L \) through \( x \), so \( |P_c| = p \) and \( |P| = p^4 \). In particular, \( N = C_t(P_c) \) and \( |P : N| = p \). Also, \( P_c \leq P(x) \) implies that \( P_c \not\leq Z \), so \( |N| = p^2 \). Then \( P_c \times Z \cong Z(N) \) implies that \( N \) is abelian. Hence, \( N \) centralizes its subgroup \( W \). But the transitivity of \( N(P_c) \) implies that \( N \) is transitive on \( L - \{ x \} \). Thus, \( W \leq P(y) \) fixes every line meeting \( L - \{ x \} \). Since \( Z \) conjugates to \( W \), \( Z \) must fix every line meeting \( L - \{ y \} \), which is not the case.

Thus, \( t = p^2 \) and \( |P| \geq p^4 \).

Next note that \( P(x^t) = 1 \). For otherwise, \( h \) is a power of \( p \) by (3.3), so \( h = p^t \) by (3.5i), whereas \( s^t/h \equiv (s - 1)(t + 1) + 1 \) by (3.5iv).

Hence, the transitivity of \( P \) on \( x^t - L \) (see (2.2)) implies that \( Z \) is semiregular on \( x^t - L \). Thus, for each \( L' \) on \( x, P(x) \cap P(L') \) contains a \( G_t \)-conjugate \( Z' \not\leq Z \) of \( Z \). In fact, if \( P' \) is a Sylow \( p \)-subgroup of \( G_{at} \) such that \( P'(x) = P(x) \), then we can choose \( Z' = Z(P') \). Thus, \( P(x) \) has \( p^2 + 1 \) nontrivial subgroups, any two meeting trivially. In particular, \( |Z(P(x))| \geq p^3 \). But \( \langle P, P \rangle \) permutes \( p^2 + 1 \) such subgroups 2-transitively, so \( |Z(P(x))| \geq p^4 \).

If \( |P(x)| \geq p^4 \), then \( P(x) \not\cong 1 \), and this contradicts (2.1).

Thus, \( |P(x)| = p^2 \) and \( P(x) \) is elementary abelian. Moreover, \( |P(x) \cap P(L)| = p^2 \). Since \( P(x) \) is transitive on \( L - \{ x \} \) and centralizes \( P(y) \cap P(L) \), we have \( P(x) \cap P(y) \leq P(L^t) = 1 \). Thus, since \( |P(y) \cap P(L)| = p^2 \), necessarily \( |P(L)| \equiv p^2 \cdot p^2 \), so \( |P| \equiv p^7 \) and \( P_c \| p^2 \). Consequently, \( P = 1 \) for some \( M \neq L \) on \( x \). By (2.1), \( P_{at} \cap P(x) = 1 \).

\( N(P(x)) \) induces the same 2-transitive representation on the \( p^2 + 1 \) lines on \( x \) and the \( p^2 + 1 \) subgroups \( P(x) \cap P(L) \) of \( P(x) \). It thus induces a subgroup of \( GL(4, p) \), 2-transitive on \( p^2 + 1 \) hyperplanes, and having a nontrivial \( p \)-subgroup (induced by \( P_{at} \)) fixing more than one such hyperplane. However, \( GL(4, p) \) has no such subgroup.

**Proof of Theorem 1.1 when \( p^2 \mid |G| \)**

In view of the preceding lemmas, it remains to eliminate the case \( p \mid t, p < t \), and \( p^2 \mid |G| \). By (2.1iii), either \( t = p^2 \) or \( p \).

Suppose first that \( t < p^2 \). Then \( P \) and \( P \leq P(L) \) is semiregular on \( x \) (which is nontrivial as otherwise \( x^t - xu \)). In particular, \( Z \mid P(L) \leq P(x) \), so \( Z \mid P(L) \). Thus, \( Z = Z(P) \) and \( Z \) is conjugate in \( G_t \), by \( t + 1 > p + 1 \) distinct proper subgroup impossible.

Thus, \( t = p^2 \). Suppose next that \( t \mid \Delta(x), P \not\cong 1 \) for each \( u \in x^t - L \).

Moreover, \( |Z \cap P(L)| = p = |P_c| = |P(x)| \). Thus, \( Z \cap P(L) = P(L) \), \( P_c \leq P(x) \), and \( P \leq P(x) \) conjugate to \( Z \cap P(L) \).

For each \( u \in x^t - L \), thus, \( Z \cap P(L) \) is again ridiculous.

Consequently, \( |P| = p^2 \). Now \( |P| = p^2 \).

Also, \( Z \cap P(L) \not\cong 1 \). Since \( P(x) \) is \( p \)-semiregular on \( x^t - L \). Thus, \( |Z \cap P(L)| \geq p^2 \).

For each \( u \in x^t - L, Z(P(x)) \cap P = 1 \). Thus, \( Z(P(x)) \) has \( p^2 + 1 \) such subgroups \( P \) permutes these subgroups 2-transitively, is again ridiculous.

This completes the proof of (1.1).

**6. The case \( p^3 \mid |G| \)**

We now consider the case \( p^3 \mid |G| \). Since \( |\Delta(x)| = p^3 \), thus, a Sylow \( p \) of \( \Delta(x) \) some point \( x \). By (2.7), \( p \not\mid t + 1 \), so \( P \) is semiregular on \( \Delta(x) \), so \( P \not\cong 1 \).

**Lemmas 6.1.** \( e = 1 \) or \( 3 \), so \( p \mid p_1 \).

**Proof.** By (2.2), \( N(P) \), is 2-transitive on \( \Delta(x) \), the lemma does not hold when \( e = 3 \). Then (2.6) implies \( t = p_1 \).
transitive on \( L - \{ x \} \), \( Z \cap P(y) = \emptyset \) in \( G(L) \), we can find \( g \in G_t \).

Set \( W = Z^t \). Then \( W \leq P(L) \).

Since \( P \), fixes \( L \) and \( \delta \), non-adjacent fixed points of \( P \), we get \( N = N_\delta(P) \).

By (2.1), \( P \), is semiregular on \( \Delta(x) \). In particular, \( N = C_{G_r}(P) \) and \( Z \), so \( | N | = p^2 \). Then \( P, Z \leq Z(N) \) realizes its subgroup \( W \). But the cycle on \( L - \{ x \} \). Thus, \( W \leq P(y) \) conjugate to \( W \), \( Z \) must fix every line \( h \) is a power of \( p \) by (3.3), so \( h = p^2 \).

\( (3.3iv) \).

\( (2.2) \) implies that \( Z \) is semiregular on \( \delta \). \( Z \) contains a \( G_r \)-conjugate \( Z' \neq Z \) such that \( P(x) = P(x) \), then \( we \) + 1 nontrivial subgroups, any two \( P \), \( \langle P, P' \rangle \) permutes \( p^2 + 1 \) such subgroups.

\( \delta \) is abelian. Moreover, \( | P(x) \cap P(y) \rangle \) and centralizes \( P(x) \cap P(y) \), we get
\[ | P(y) \cap P(L) | = p^k \] necessarily.

Consequently, \( P_{u,v} \neq 1 \) for some \( u \), \( v \).

\( \delta \) presentation on the \( p^2 + 1 \) lines on \( x \).

It thus induces a subgroup of \( P \) and having a nontrivial \( p \)-subgroup hyperplane. However, \( GL(4, p) \) has

and \( p^2 \cdot \delta (G) | G | \). By (2.iii), either \( t < p^2 \) and \( | P | = p^2 \), or \( t = p^2 \) and \( | P | = p^2 \) or \( p^3 \).

Suppose first that \( t < p^2 \). Then \( P \) is semiregular on \( \Delta(x) \). Hence, if \( y \in L - \{ x \} \) then \( P \) is semiregular on \( x^i - L \). Consequently, if \( u \in x^i - L \), then \( P \) (which is nontrivial as otherwise \( p^2 = | u^i | \leq | x^i - L | = p^t \)) is semiregular on \( x^i - xu \). In particular, \( Z = Z(P) \leq G(x) \). By (2.2), \( Z < P \), so \( | Z | = p \). But \( P(L) \neq P, \) \( Z \leq P(L) \). Thus, \( Z = P(L) \), whenever \( x \in L' \neq L \). Consequently, \( P \), and \( Z \) are conjugate in \( G \), by (2.2), so \( P \), \( P(x) \) and \( P(xu) \). Now \( P(x) \) has \( t + 1 \) \( p^2 + 1 \) distinct proper subgroups, so \( | P(x) | \geq p^3 | | P \). By (2.2ii), this is impossible.

Thus, \( t = p^2 \). Suppose next that \( | P | = p^3 \). Then once again, \( P \) is semiregular on \( \Delta(x) \), \( P \neq 1 \) for each \( u \in x^i - L \), \( P \) is semiregular on \( x^i - xu \), and \( Z \leq G(x) \).

Moreover, \( | Z \cap P(L) | = p = | P \rangle \) by the semiregularity of \( P(L) \), and \( P \), \( P(xu) \).

Thus, \( Z \cap P(L) = P(L) \), whenever \( x \in L' \neq L \). As above, we then have \( P \), \( P(xu) \), conjugate to \( Z \cap P(L) \), so \( P \), \( P(x) \), \( | P(x) | \geq p^3 \), and hence \( | P : P(x) | \leq p \). Once again, this contradicts (2.2ii).

Consequently, \( | P | = p \). Now \( | P \rangle \neq 1 \) for each \( w \in \Delta(x) \), while \( | P \rangle = p^3 \) for each \( u \in x^i - L \). Thus, \( P \), fixes no points of \( x^i - xu \), so \( Z \leq P(x) \) once again.

Also, \( Z \cap P(L) \neq 1 \). Since \( P(x^i) = 1 \) as in the proof of (5.3), \( Z \cap P(L) \) is semiregular on \( x^i - L \). Thus, \( | Z \cap P(L) | = p \).

For each \( u \in x^i - L \), \( Z(P(x)) \cap P(xu) \) contains a \( G_r \)-conjugate of \( Z \cap P(L) \). Thus, \( Z(P(x)) \) has \( p^2 + 1 \) such subgroups, and \( | Z(P(x)) | \geq p^3 \). Since \( N(P(x)) \) permutes these subgroups 2-transitively, \( | Z(P(x)) | \geq p^4 \). But now \( | P : P(X) | \leq p \) is again ridiculous.

This completes the proof of (1.1) when \( p^3 | G | \).

6. The case \( p^2 \lor G | \)

We now consider the case \( p^2 \lor G | \) of Theorem 1.1. Certainly, \( p^2 | G | \) since \( | \Delta(x) | = p^t \).

Thus, a Sylow \( p \)-subgroup \( P \) of \( G \) has order \( p^2 \), and fixes some point \( x \).

By (2.7), \( p \lor t + 1 \), so \( P \) fixes \( 1 + \epsilon \) \( 2 \) lines on \( x \).

Let \( L \) be such a line. \( P \) is semiregular on \( \Delta(x) \), so \( P(L) \) is semiregular on \( x^i - L \).

**Lemma 6.1.** \( \epsilon = 1 \lor r \) or \( 3 \), so \( t \lor t - 1 \lor t - 3 \). If \( \epsilon = 3 \) then \( 3 \lor p - 1 \) and \( N(P) \lor C(P) \lor SL(2, 3) \).

**Proof.** By (2.2), \( N(P) \), is 2-transitive on the \( 1 + \epsilon \) subgroups \( P(L) \). Hence, if the lemma does not hold then \( \epsilon = 2 \) and \( N(P) \lor C(P) \) induces \( S_1 \) on these subgroups. Then (2.6) implies \( t = p + 2 \). Since \( N(P) \) acts irreducibly on \( P \) and
1 + \epsilon > 1 + \epsilon, P \neq P(x) and hence P(x) = 1. Thus, G, acts on the lines through x as a group of degree p + 3 and order divisible by p^2, which is absurd since p \neq 3 here (as t \neq p^2 - p - 1).

COMPLETION OF THE PROOF OF (1.1). By (6.1) and (2.7), t = 2p + 3 and \epsilon = 3.
Then P has just 2 nontrivial orbits C_1 and C_2 of lines on x. Then the commutator group N(P) fixes C_1 and C_2, and induces a metacyclic group in each C_i, so N(P)\langle g \rangle induces the identity on both orbits by (6.1). N(P)\langle g \rangle has an element g inverting P.
Then g normalizes P(L), so g \in G(x). Now P = [P, g] \leq [P, G(x)] \leq G(x), so \epsilon = 1 + t. This contradiction proves the theorem.

REFERENCES
3. D. G. Higman, Characterizations of families of rank 3 permutation groups by the subdegrees III (unpublished)

UNIVERSITY OF OREGON
EUGENE, OREGON, U.S.A.

MONOMIAL CHARACTERIZATIONS

LOUISE KANTOR

Dradin introduced the notion of monomial conditions and developed monomials in a ring. For primitive rings which have primitive rings which have prime G, monomial conditions related to the characterization of prime G, o monomials.

1. Preliminaries

In this paper, all rings are associative rings, with \( R \) such that \( R \neq 0 \) (without 1) generated by the commutative subring \( X = \{X_1, X_2, \cdots \} \). Let \( Z[X; t] \) be subring of \( \{\text{monic monomials } h \in Z[X]| h^n \neq 0\} \). Say \( y \in R \) is \( \pi(t) \cap Z[X; k] \). Say \( y \in R \) is \( R \)-essentially if \( yr \neq 0 \) and \( b \neq 0 \) in \( R \), there are nonzero and nonessential. Weakening Dradin's definition of \( X_1, \cdots, X_r \) is \( R \)-pivotal if every homomorphism \( \varphi: Z[X; t] \to R \), \( \varphi \) is \( R \)-regular and \( y \) is \( R \)-essential. The \( R \)-pivotal will be the ring obtained by adjoining the group \( Z \oplus R \), endowed with the \( (n_1, n_2, n_3, r_1, r_2, r_3) \), and the maps \( n_1, r + r \) and \( r(n_1, r_2) = m_1 + m_2 \). The \( R \)-pivotal will merely be called \( R \)-pivotal for \( R \) a domain.

Received December 13, 1974