ON QUADRUPLY TRANSITIVE GROUPS

DISSERTATION
Presented in Partial Fulfillment of the Requirements for the Degree Doctor of Philosophy in the Graduate School of the Ohio State University

By

ERNEST TILDEN PARKER, B. A.

The Ohio State University
1957

Approved by:

[Signature]
Adviser
Department of Mathematics
Acknowledgment

The author wishes to express
his sincere gratitude to
Professor Marshall Hall, Jr.,
for assistance and encouragement
in the preparation of this dissertation.
Table of Contents

1. Introduction --------------------------------- 1
2. Preliminary Theorems ----------------------- 3
3. The Main Theorem ---------------------------- 12
4. Special Cases ------------------------------- 17
5. References ---------------------------------- 42
Introduction

In Section 3 the following theorem is proved:

If $G$ is a quadruply transitive finite permutation group, $H$ is the largest subgroup of $G$ fixing four letters, $P$ is a Sylow $p$-subgroup of $H$, $P$ fixes $r \geq 12$ letters and the normalizer in $G$ of $P$ has its transitive constituent $A_r$ or $S_r$ on the letters fixed by $P$, and $P$ has no transitive constituent of degree $\geq p^3$ and no set of $r(r-1)/2$ similar transitive constituents, then $G$ is alternating or symmetric.

The corollary following the theorem is the main result of this dissertation. While less general than the theorem, it provides arithmetic restrictions on primes dividing the order of the subgroup fixing four letters of a quadruply transitive group, and on the degrees of Sylow subgroups. The corollary is:

If $G$ is a quadruply transitive permutation group of degree $n = kp+r$, with $p$ prime, $k \leq p^2$, $k \leq r(r-1)/2$, $r \geq 12$, and the subgroup of $G$ fixing four letters has a Sylow $p$-subgroup $P$ of degree $kp$, and the normalizer in $G$ of $P$ has its transitive constituent $A_r$ or $S_r$ on the letters fixed by $P$, then $G$ is $A_n$ or $S_n$.

In Section 2 are proved three lemmas used in the proof of the theorem of Section 3. Also proved in Section 2 is a theorem referred to as the theorem of Bochert. A. Bochert [1] proved the theorem with $(n-3)/2$ replaced by the slightly better $(n-2)/2$.

(Number in brackets indicate references to the literature listed)
at the end of this dissertation.) Manning [6] made the improvement to \((n-1)/2\). The form used in this dissertation has a shorter proof, and is adequate for the present applications.

In Section 4 it is shown that the only quadruply transitive groups of degree \(n \geq 27\) are the symmetric groups of degree \(n\) with \(4 \leq n \leq 27\), the alternating groups of degree \(n\) with \(6 \leq n \leq 27\), and the four Mathieu groups of degrees 11, 12, 23, and 24. For degrees through 20 all primitive groups have been determined. As there are several primitive groups of most degrees, and the determination of these is lengthy, a systematic search for quadruply transitive groups of low degrees seems desirable.

A comment on notation is in order: \(A_n\) and \(S_n\) will designate respectively the alternating group of degree \(n\) and the symmetric group of degree \(n\).
Lemma 1. If B is a transitive permutation group of degree p or $p^2$ (p prime), and if B has a normal subgroup T of order a power of p and transitive on the letters of B, then B has no composition factor-group isomorphic with $A_r$, $r > 5$.

Proof. If B is of degree p, then B is contained in the metacyclic group, and hence is solvable.

If B is of degree $p^2$, then T contains an elementary subgroup (not necessarily proper) C normal in B. (For p-groups are solvable, and every minimal normal subgroup is a direct product of isomorphic simple groups.) Since B is transitive, C displaces all letters of B, and has all transitive constituents similar. C, being abelian, has all transitive constituents regular. Thus C is either the regular elementary group of degree $p^2$, or a subdirect product of $p$ transitive cyclic groups of degree p.

If C is regular, then B is contained in the holomorph of the elementary group of order $p^2$. The only unsolvable [3, pp. 428-34] composition factor-group of this holomorph is LF(2,p). The smallest alternating group of order divisible by p is $A_p$; and $p(p^2-1)/2 < p^2/2$ for $p > 5$. Hence LF(2,p) is isomorphic with no alternating group for $p > 5$. The only unsolvable [3, pp. 440-50] proper subgroup of LF(2,p) is isomorphic with $A_5$. LF(2,p) is isomorphic with $A_5$ for $p = 5$, and contains a proper subgroup isomorphic with $A_5$ for $p = 5$ (mod 5).

If C is a subdirect product of $p$ cyclic groups of order p,
then each element of \( B \) must permute the transitive constituents of \( C \) among themselves; the transitive constituents of \( C \) are sets of imprimitivity for \( B \). Let \( K \) be the largest subgroup of \( B \) fixing all these sets of imprimitivity; \( K \) is a normal subgroup of \( B \). \( B/K \) may be regarded as a permutation group with letters the \( p \) transitive sets of \( K \). Since \( T \) is transitive on the original letters, and \( K \) is intransitive, \( T \) is not a subgroup of \( K \). Accordingly, \( B/K \) has a normal \( p \)-subgroup. \( B/K \), being of degree only \( p \), is contained in the metacyclic group and is solvable. \( K \) is a subdirect product of groups contained in the metacyclic group. In this case \( B \) is solvable.

**Lemma 2.** For \( r \geq 9 \), \( A_r \) has no subgroup of index \( t \) with \( r < t < r(r-1)/2 \).

**Proof.** Assume that \( A_r \) has a subgroup \( L \) of index \( t \), \( r \geq 9 \), \( r < t < r(r-1)/2 \).

If \( L \) is intransitive, then \( L \) is contained (not necessarily properly) in the even subgroup \( M_i \) of the direct product of \( S_i \) and \( S_{r-i} \) with \( 0 < i < r \). \( M_i \) is of index \( \binom{r}{i} \) in \( A_r \). Thus, when \( L \) is intransitive, \( L \) is of index at least \( r(r-1)/2 \) in \( A_r \) unless \( i = 1 \) or \( r-1 \). For \( i = 1 \) or \( r-1 \), \( M_i \) is \( A_{r-1} \), of index \( r \) in \( A_r \), failing to satisfy the strict inequality. \( A_{r-1} \) has no proper subgroup of index \( < r-1 \); hence \( M_i \) has no subgroup of index \( < r(r-1)/2 \) in \( A_r \).

There remains for consideration the case of transitive \( L \).

Let \( q \) be a prime, \( r/2 < q < r \). If \( L \) is of order divisible by \( q \),
then $L$ has a cycle of length $q$, and hence is primitive [4, p. 162, Exercise 8]. In turn, $L$ is $(r-q-1)$-ply transitive [3, p. 207, Th. 1]. If further, $q \leq r-3$, then $L$ must be $A_r$ [7]. Thus transitive $L$ contained properly in $A_r$ must be of index divisible by each prime $q$, $r/2 < q \leq r-3$.

A theorem on distribution of primes will now be used [2, 8]: If $x \geq 25$, then there exists a prime $q$ such that $x < q < 6x/5$. It follows for $r \geq 50$ that there exist primes $q_1$, $q_2$, $q_3$, satisfying $r/2 < q_1 < q_2 < q_3 \leq r-3$. The existence of such a triple of primes for $20 \leq r < 50$ is easily verified. Now $q_1 q_2 q_3 > (r/2)^3 > r(r-1)/2$ for $r \geq 20$.

Degrees $9 \leq r \leq 19$ remain to be considered. If $L$ is primitive and a proper subgroup of $A_r$, then $L$ can have no cycle of length $q$, where $q$ is a prime $\leq r-3$. Accordingly, for each odd $q \leq r-3$, a Sylow $q$-subgroup of $L$ must be a proper subgroup of that of $A_r$. The index of $L$ in $A_r$ must be divisible by each odd $q \leq r-3$.

$2 < q \leq r-3$ is satisfied by $q = 3, 5, 7, 11$, when $14 \leq r \leq 19$; and $3 \cdot 5 \cdot 7 \cdot 11 > r(r-1)/2$ for these values of $r$. Similarly, $q = 3, 5, 7$ for $10 \leq r \leq 13$; and $3 \cdot 5 \cdot 7 > r(r-1)/2$. This excludes the existence of primitive $L$ of degree $r$, $10 \leq r \leq 19$.

If $L$ is imprimitive, then $L$ must be of index divisible by each prime $q$ with $r/2 < q \leq r$. For $17 \leq r \leq 19$, the inequality is satisfied by $q = 11, 13, 17$; and $11 \cdot 13 \cdot 17 > r(r-1)/2$. For $13 \leq r \leq 16$, $q = 11, 13$; and $11 \cdot 13 > r(r-1)/2$. For $r = 11$ or 12, $q = 7, 11$; and
The maximal imprimitive subgroups of $A_{10}$ are of orders $\frac{5}{2} \cdot 21(51)^2$ and $\frac{5}{2} \cdot 51(21)^5$, both subgroups being of index $>10 \frac{9}{2}$. A maximal imprimitive subgroup of $A_9$ is of order $\frac{7}{2} \cdot 31(31)^2$; of index $>9 \frac{8}{2}$.

One case remains, namely degree 9 with $L$ primitive. $L$ must be of index divisible by 3 and 5. Since $3 \cdot 5 > 9 \frac{8}{2}$, $L$ can be of index only 15 or 30 in $A_9$. $L$, having a cycle of length 7, is triply transitive. If $L$ is of index 30 in $A_9$, then the largest subgroup of $L$ fixing two letters is of order 84; but a group of order 84 must have only one Sylow 7-subgroup. If $L$ is of index 15 in $A_9$, then the largest subgroup of $L$ fixing two letters set-wise is of order 336; a group of degree 7 and order divisible by 24 contains a transposition.

**Lemma 3.** If $G$ is a transitive permutation group homomorphic onto $K$, and the kernel $G_0$ of the mapping onto $K$ is transitive on the letters permuted by $G$, then the largest subgroup $G_1$ of $G$ fixing the letter 1 admits the same homomorphism onto $K$.

**Proof.** For any $k \in K$, there exists $g_k \in G$ such that $g_k \rightarrow k$ in the homomorphism. Let $i$ be the letter onto which 1 is mapped by $g_k$. Being transitive, $G_0$ has an element $g'_i$ mapping $i$ onto 1. Then $g_k g'_i$ maps 1 onto 1, and corresponds to $k \cdot l = k$ in the homomorphism. Since $k$ was chosen as an arbitrary element of $K$, it follows that $G_1$ has an element corresponding to any element of $K$. 
The Theorem of Bochert will be preceded by the following:

Lemma. If $x$ and $y$ are permutations displacing $r$ common letters, and $x$ maps $s$ letters fixed by $y$ onto commonly displaced letters, and $y$ maps $t$ letters fixed by $x$ onto commonly displaced letters, then $xyx^{-1}y^{-1}$ displaces at most $r+s+t$ letters.

Proof. Trivially, any letter fixed by both $x$ and $y$ is fixed by $xyx^{-1}y^{-1}$. Let $a, a'$ denote any letters displaced by $x$ and fixed by $y$. Let $b, b'$ denote any letters displaced by $y$ and fixed by $x$. If $x$ maps $a \rightarrow a'$, then the sequence of mappings is

$$a \xrightarrow{x} a' \xrightarrow{y} a' \xrightarrow{x^{-1}} a \xrightarrow{y^{-1}} a,$$

and $xyx^{-1}y^{-1}$ fixes $a$.

If $y$ maps $b \rightarrow b'$, then

$$b \xrightarrow{x} b \xrightarrow{y} b' \xrightarrow{x^{-1}} b' \xrightarrow{y^{-1}} b,$$

and $xyx^{-1}y^{-1}$ fixes $b$.

Thus any $a$ displaced by $xyx^{-1}y^{-1}$ must be mapped by $x$ onto a commonly displaced letter; any $b$ displaced by $xyx^{-1}y^{-1}$ must be mapped by $y$ onto a commonly displaced letter. $xyx^{-1}y^{-1}$ displaces at most $s$ $a$'s and $t$ $b$'s, hence at most $r+s+t$ letters.

Theorem of Bochert. If $G$ is a quadruply transitive group of degree $n$, neither $A_n$ nor $S_n$, then each non-identical element of $G$ displaces at least $(n-3)/2$ letters.

Proof. Let $c$ be the smallest number of letters displaced by a non-identical element of $G$. ($c$ is called the class of $G$.) Let $g$ be an element of $G$ displacing exactly $c$ letters. The letters can be
designated so that \( g \) displaces 1, 2, \( \ldots, c \), maps 1 onto 2, and fixes \( c+1, \ldots, n \). Let \( g_1 \) be an element of \( G \) displacing only \( c \) letters, fixing 1 and displacing 2. (The quadruple transitivity of \( G \) guarantees existence of such a \( g_1 \).) Let \( H \) be the largest subgroup of \( G \) fixing 1 and 2. And let \( g_1, g_2, \ldots, g_k \) be all the distinct elements conjugate to \( g_1 \) under transformation by elements of \( H \). Each \( g_i \) fixes 1 and displaces 2. Thus each \( g_i \) is non-permutable with \( g \), for \( g_1 g \) maps 1 onto 2, but \( g g_1 \) does not map 1 onto 2. And each \( g_1 g_i g_1^{-1} g_i^{-1} \), being different from the identity, must displace at least \( c \) letters. Let \( Z \) be the centralizer in \( H \) of \( g_1 \). Now \( h_1^{-1} g_1 h_1 = h_2^{-1} g_1 h_2 \) if and only if \( Z h_1 = Z h_2 \). Thus the set of \( h_1^{-1} g_1 h \) contains each \( g_1 \) as many times as the order of \( Z \). Since \( G \) is quadruply transitive by hypothesis, \( H \) is doubly transitive. Hence for each letter \( u \), not 1 or 2, \( u \) is displaced by equally many \( g_i \). And for each pair \( u, v \) of distinct letters, both different from 1 and 2, \( u \) is mapped onto \( v \) by equally many \( g_i \).

Each \( g_i \) maps 2 onto a letter different from 1 and 2, and maps one letter different from 1 and 2 onto 2. For each \( g_i \) exactly \( c-2 \) displaced letters not 1 or 2 are mapped onto letters not 1 or 2. The total number of mappings of \( u \) onto \( v \) under the \( g_i \) is \( k(c-2) \), as \( u, v \) range over all ordered pairs of distinct letters, both different from 1 and 2. Thus for each fixed choice of the pair \( u, v \), the number of \( g_i \) mapping \( u \) onto \( v \) is \( k(c-2)/(n-2)(n-3) \). In turn the total number of mappings of \( u \) onto \( v \) under the \( g_i \) with \( u \) ranging
over \( c+1, \ldots, n \), and \( v \) ranging over 3, 4, \ldots, \( c \), is

\[(n-c)(c-2)\cdot \frac{c(c-2)}{(n-2)(n-3)}. \]

2 is displaced by all the \( g_1 \), and is the map of any letter other than 1 and 2 under equally many \( g_1 \); thus this number of \( g_1 \) is \( k/(n-2) \). The total number of \( g_1 \) mapping letters \( c+1, \ldots, n \) onto 2 is \( (n-c)\cdot k/(n-2) \). Hence the total number of mappings under the \( g_1 \) of letters fixed by \( g \) onto letters displaced by \( g \) is

\[
(1) \quad \frac{(n-c)(c-2)\cdot k(c-2)}{(n-2)(n-3)} + (n-c)\cdot \frac{k}{n-2}.
\]

The letter 2 is displaced by \( g \) and all \( k \) of the \( g_1 \). Each \( g_1 \) displaces \( c-1 \) letters different from 1 and 2. As each such letter is displaced by equally many \( g_1 \), each is displaced by \( k(c-1)/(n-2) \) of the \( g_1 \). The total number of times letters 3, 4, \ldots, \( c \) are displaced by the \( g_1 \) is \( (c-2)\cdot k(c-1)/(n-2) \). Thus the sum with respect to the \( g_1 \) of the number of letters commonly displaced by \( g \) and a \( g_1 \) is

\[
(2) \quad k + k(c-1)(c-2)/(n-2).
\]

Next will be computed the sum with respect to the \( g_1 \) of the number of mappings under \( g \) of letters fixed by a \( g_1 \) onto letters displaced by that \( g_1 \). \( g \) consists of \( c \) mappings of letters onto distinct letters. Relative to all \( k \) of the \( g_1 \), the fixed letter 1 is mapped by \( g \) onto the displaced letter 2. No contribution is made to the sum by the mappings \( g^{-1}(1) \rightarrow 1 \) and \( 2 \rightarrow g(2) \). These are the same mapping if \( g \) transposes 1 and 2. The number of mappings by
g of $u$ onto $v$, where $u$ and $v$ are distinct letters among $1, \ldots, c$ is $c-2$ or $c-3$, depending upon whether $g$ does or does not transpose 1 and 2. The inequality relating $c$ and $n$ is weaker when $c-2$ mappings remain; this case will therefore be assumed. For any one of the mappings $u_0 \rightarrow v_0$ under $g$, the number of the $g_1$ which fix $u_0$ and displace $v_0$ is

$$K \cdot \frac{c-2}{n-2} \cdot \frac{n-c}{n-3}.$$ 

Thus the desired sum is

$$(3) \quad K + (c-2)K \cdot \frac{c-2}{n-2} \cdot \frac{n-c}{n-3}.$$ 

Now, since each $g_1g_2^{-1}g_1^{-1}$ must displace at least $c$ letters the total number of letters displaced by these commutators is at least $kc$. In turn, applying the preceding lemma, the sum of expressions (1), (2), (3) must be at least $kc$. Dividing out the common factor of $k$,

$$\left\lceil \frac{(c-2)^2(n-c)}{(n-2)(n-3)} + \frac{n-c}{n-2} \right\rceil + \left[ 1 + \frac{(c-1)(c-2)}{n-2} \right] + \left[ 1 + \frac{(c-2)^2(n-c)}{(n-2)(n-3)} \right] \geq c.$$ 

Replacing $(n-c)/(n-2)$ by $1 - (c-2)/(n-2)$, and adding terms with like denominators gives

$$\frac{2(c-2)^2(n-c)}{(n-2)(n-3)} + \frac{(c-1)(c-2)-(c-2)}{n-2} + 3 \geq c.$$ 

Substituting $b = c-2$ and $m = n-2$ yields

$$\frac{2b^2(m-b)}{m(m-1)} + \frac{b^2}{m} \geq b-1.$$
Multiplying through by the positive denominator \( m(m-1) \) and transposing,
\[
0 \geq -2b^2m - b^2m + (b-1)m(m-1).
\]
Expanding, and rearranging terms according to powers of \( m \),
\[
0 \geq m^2(b-1) - m(b-1 + 3b^2) + (2b^3 + b^2).
\]
This inequality is valid if \( G \) is \( A_n \) or \( S_n \). The hypothesis that \( G \) is not alternating or symmetric requires that \( c > 3 \), and in turn \( b-1 > 0 \). Regarding \( b \) as a fixed number greater than one, the right member of the inequality is a quadratic polynomial in \( m \). In order that the polynomial be non-positive, it is necessary that
\[
m \leq \frac{(b-1 + 3b^2) + \sqrt{(b-1 + 3b^2)^2 - 4(b-1)(2b^3 + b^2) - 2b^2(m-b) - b^2(m-1) + (b-1)m(m-1)}}{2(b-1)}.
\]
The expression under the radical is \( b^4 + 10b^3 - b^2 - 2b + 1 \), which is less than \( (b^2 + 5b - 3)^2 = b^4 + 10b^3 + 19b^2 - 30b + 9 \) for \( b > 1 \). Thus
\[
m < \frac{(b-1 + 3b^2) + (b^2 + 5b - 3)}{2(b-1)} = \frac{2b^2 + 3b - 2}{b-1} = 2b + 5 + \frac{3}{b-1}.
\]
Substituting back \( n \) and \( c \),
\[
n < 2c + 3 + \frac{3}{c-3}.
\]
c=4 or 5 is impossible in a quadruply transitive group. Thus \( 3/(c-3) \leq 3/(6-3) = 1 \). And \( n < 2c + 3 + 1 \), so that \( c > (n-4)/2 \). Since \( c \) is an integer, \( c \geq (n-3)/2 \).
The Main Theorem

Theorem. If G is a quadruply transitive finite permutation group, H is the largest subgroup of G fixing four letters, P is a Sylow p-subgroup of H, P fixes \( r \geq 12 \) letters and the normalizer in G of P has its transitive constituent \( A_r \) or \( S_r \) on the letters fixed by P, and P has no transitive constituent of degree \( \leq p^3 \) and no set of \( r(r-1)/2 \) similar transitive constituents, then G is alternating or symmetric.

Proof. Let \( N_G(P) \) be the normalizer in G of P. Each element of \( N_G(P) \) maps any transitive constituent of P set-wise onto a similar transitive constituent of P. Let \( P' \) be the largest subgroup of \( N_G(P) \) fixing set-wise all transitive constituents of P. Let \( n \) be an element of \( N_G(P) \), and let \( p' \) be an element of \( P' \). \( n^{-1}p'n \) fixes set-wise all transitive constituents of P; hence \( P' \) is a normal subgroup of \( N_G(P) \). The transitive constituents of P will be referred to below as points. \( N^* = N_G(P)/P' \) is a permutation group on points.

By hypothesis, all points are of degree \( \leq p^2 \). By Lemma 1, no transitive group of degree \( \leq p^2 \) with a normal transitive p-subgroup can have a composition factor-group of \( A_r \), \( r > 5 \). By hypothesis, \( N_G(P) \) has transitive constituent \( A_r \) or \( S_r \) on \( r \geq 12 \) letters fixed by P. Thus \( N_G(p) \) has a composition factor-group isomorphic with \( A_r \), but \( P' \) has no such composition factor-group. It follows that \( N^* \) has a composition factor-group of \( A_r \).
N* has a subgroup N (not necessarily proper) minimal in the following sense:

(1). N has an element permuting the r letters fixed by P according to \( \alpha \), where \( \alpha \) is any even permutation.

(2). No proper subgroup of N has property (1).

A subgroup (not necessarily proper) of N* with property (1) exists, since N* itself has property (1). N*, being a finite group, has only finitely many subgroups, so that a minimal subgroup with property (1) must exist. It is not asserted that N is unique.

By the minimality of N, each transitive constituent of N is either a single point or admits a homomorphic mapping onto \( A_r \) represented on the letters fixed by P. Let J designate any transitive constituent of N not a single point and permuting points other than letters fixed by P. J is homomorphic onto \( A_r \), and the kernel \( J_0 \) of the homomorphism is the group of permutations of J corresponding to the identity permutation of the letters fixed by P. Assume that J has its kernel \( J_0 \) transitive on the points permuted by J. Then by Lemma 3, the largest subgroup of J fixing one point possesses the homomorphism onto \( A_r \). By the minimality of N, each J must have an intransitive kernel.

For any J, the transitive constituents of the kernel \( J_0 \) will be called blocks. As \( J_0 \) is intransitive on the points permuted transitively by J, it follows that J permutes more than one block.
As $J_0$ is precisely the kernel of the homomorphism of $J$ onto $A_r$, $J$ permutes blocks according to a group isomorphic with $A_r$. By hypothesis, $P$ has no set of $r(r-1)/2$ similar transitive constituents. Thus $J$ is of degree $< r(r-1)/2$ on points; since each block contains at least one point, $J$ certainly permutes fewer than $r(r-1)/2$ blocks. By Lemma 2, $A_r$ has no transitive permutation representation of degree strictly between $r$ and $r(r-1)/2$. (By hypothesis $r \geq 12 > 9$.) Accordingly, each $J$ permutes exactly $r$ blocks according to $A_r$.

For $r \neq 6$, the only automorphisms [3, p. 209] of $A_r$ are induced by transformation by elements of $S_r$, and preserve similarity of permutations. Accordingly, between the letters fixed by $P$ and the blocks of any $J$ there is a unique one-to-one correspondence such that an element of $N$ displaces a letter if and only if it displaces the corresponding block.

Select a set of $s = \lceil r/2 \rceil$ letters among the $r$ fixed by $P$. Let $N_0$ be a minimal subgroup of $N$ inducing all even permutations on these $s$ letters. (The argument for the existence of $N_0$ is the same as that for $N$ above.) As each $J$ is of degree $< r(r-1)/2$, each block contains fewer than $(r-1)/2 \leq s$ points. The points of a block cannot be permuted according to any group homomorphic onto $A_s$. By the minimality of $N_0$, each block fixed set-wise by $N_0$ is fixed point-wise by $N_0$. This follows since $N_0$ has a composition factor-group $A_s$, which is not a composition factor-
group of the group permuting the points of one block among themselves.

Returning to the letters permuted by \( G \), the elements of \( N_0 \) determine two-sided cosets of \( P' \); let \( M \) designate the group whose elements comprise these cosets. \( M \) permutes the set of \( s \) letters, selected among the \( r \) letters fixed by \( P \), according to \( A_s \). Let \( M \) be a minimal subgroup of \( M \) with this property. \( r \geq 12 \), so that \( s > 5 \). By the minimality of \( M_0 \), and by Lemma 1, each transitive constituent (point) of \( P \) fixed set-wise by \( M_0 \) is fixed letter-wise by \( M_0 \).

Thus each element of \( M_0 \) displaces at most \( s/r \leq r/2r = 1/2 \) of the letters of any transitive constituent of \( N_0(P) \); that is, at most half the letters displaced by \( P \). \( M_0 \) has a non-identical element \( m \) displacing only three letters fixed by \( P \). As \( r \geq 12 \), \( m \) displaces at most half as many letters as the degree of \( G \), diminished by 3. By the Theorem of Bochert, quadruply transitive \( G \), with an element displacing so few letters as \( m \), must be alternating or symmetric.

Corollary. If \( G \) is a quadruply transitive permutation group of degree \( n = kp+r \), with \( p \) prime, \( k < p^2 \), \( k < r(r-1)/2 \), \( r \geq 12 \), and the subgroup of \( G \) fixing four letters has a Sylow \( p \)-subgroup \( P \) of degree \( kp \), and the normalizer in \( G \) of \( P \) has its transitive constituent \( A_r \) or \( S_r \) on the letters fixed by \( P \), then \( G \) is \( A_n \) or \( S_n \).
Proof. Since \( k < p^2 \), \( P \) is of degree \( kp < p^3 \), so that \( P \) has no transitive constituent of degree \( \geq p^3 \). Since transitive constituents of \( P \) are of degree at least \( p \), \( k < r(r-1)/2 \) implies that \( P \) has no set of \( r(r-1)/2 \) similar transitive constituents. The hypothesis of the preceding theorem is fulfilled; thus \( G \) is \( A_n \) or \( S_n \).

Remark. When \( n = kp+r \), with \( p \), \( k \), and \( r \) satisfying the inequalities of the corollary, then any quadruply transitive group of degree \( n \) having \( P \) of degree \( kp \) is \( A_n \) or \( S_n \), whenever \( r \) is a degree for which the only quadruply transitive groups are \( A_r \) and \( S_r \). For the normalizer of a Sylow subgroup of the subgroup fixing four letters of a quadruply transitive group is quadruply transitive on the fixed letters [5, Lemma 2.2]. If \( r \) is of the form \( q+3 \) or \( 2q+3 \), with \( q \) prime, then the only quadruply transitive groups of degree \( r \) are \( A_r \) and \( S_r \) [?]; thus there are infinitely many degrees \( r \) having this property. It is likely that the degrees \( r \) for which there exist quadruply transitive groups neither \( A_r \) nor \( S_r \) are distributed sparsely among the integers.
Special Cases

It will be demonstrated that the only quadruply transitive permutation groups of degrees \( n \leq 27 \) are \( S_n, 4 \leq n \leq 27; A_n, 6 \leq n \leq 27 \), and the four Mathieu groups of degrees 11, 12, 23, and 24.

Trivially the lowest degree of a quadruply transitive group is 4. For degrees 4 and 5, the only quadruply transitive groups are symmetric. For degree 6 a quadruply transitive group must be alternating or symmetric. A quadruply transitive group of degree 7 is of index dividing 6 in \( S_7 \). \( S_7 \) contains no subgroup of index \( < 7 \) except \( A_7 \). Of course, for all \( n \geq 6 \), \( A_n \) and \( S_n \) are quadruply transitive.

There remain to be determined all quadruply transitive groups of degree \( n \), other than \( A_n \) and \( S_n \), \( 8 \leq n \leq 27 \).

The following theorems will be used, and are listed for reference:

(A). If \( G \) is an \( (r+1) \)-ply transitive permutation group of degree \( n = kp+r \), with \( p \) prime, \( k < p, k < r, r \geq 3 \), then \( G \) is \( A_n \) or \( S_n \) [?].

(B). If \( G \) is a primitive group of degree \( n \) with a primitive subgroup of degree \( m \), then \( G \) is \( (n-m+1) \)-ply transitive [3, p. 207, Th. I].

(C). If \( G \) is a finite quadruply transitive permutation group, then \( G \) has an element of order 2 fixing four letters, or \( G \) is \( S_4 \).
S₅, A₆, A₇, or the Mathieu group of degree 11 [5].

(D). If G is a finite r-ply transitive permutation group, H is the largest subgroup of G fixing r letters, and P is a Sylow p-subgroup of H, then the normalizer in G of P is r-ply transitive on the letters fixed by P [5, Lemma 2.2]. By the definition of Sylow subgroup, the subgroup fixing r letters of the transitive constituent on the letters fixed by P is of order prime to p. By (C), if G is quadruply transitive and p=2, then P fixes 4, 5, 6, 7, or 11 letters, and the transitive constituent on the letters fixed by P of the normalizer in G of P is S₄, S₅, A₆, A₇, or the Mathieu group of degree 11.

(E). If G is a quadruply transitive permutation group of degree n, neither Aₙ nor Sₙ, then each non-identical element of G displaces at least (n-3)/2 letters [1]. (This is the theorem of Bochert proved in Section 2.)

The following lemma, which will be used repeatedly, is stated and proved:

(F). If G is a quadruply transitive group of degree n, and the largest subgroup of G fixing four letters is of order divisible by an odd prime p, with 5p≥n-4, 4p∤n-4, then G is Aₙ or Sₙ.

Proof. Let H be the largest subgroup of G fixing four letters, and P be a Sylow p-subgroup of H. Since 5p≥n-4, P is of degree≥4p.
If $P$ is of degree $n-4$, then $P$ is of degree $kp$ with $k \leq 3$, since $4p \nmid n-4$ by hypothesis. In this case, the theorem of Miller (A) is applicable with $n = kp+4$, except when $k=p=3$. However, for $k=p=3$, $3 \cdot 3 + 4 = 13 = 2 \cdot 5 + 3$, so that $G$ is $A_{13}$ or $S_{13}$.

If $P$ is of degree $< n-4$, then by (E) $P$ is of degree at least $(n-3)/2$. Then $r \leq (n+3)/2$ letters are fixed by $P$. By (D), $N_G(P)$, the normalizer in $G$ of $P$, has a quadruply transitive constituent $T$ on these $r \geq 5$ letters.

A normal subgroup (not the identity) of a quadruply transitive group (other than $S_n$) is triply transitive \cite{3, p. 198, Th. XI}. $T$ is primitive and has no regular normal subgroup; therefore $T$ is unsolvable. The final subgroup in the derived series of $T$ is triply transitive.

If $p > 3$, then each transitive constituent of $P$ is of degree $p$ and has a solvable holomorph. For $p=3$, a transitive constituent of degree 9 has a solvable automorphism group. As $P$ has at most four transitive constituents, these cannot be permuted set-wise by an unsolvable group. Accordingly, the final derived group of $N_G(P)$ is primitive of degree $\leq (n+3)/2$. By (B), $G$ is at least $n + 1 - (n+3)/2 = (n-1)/2$-ply transitive. But $G$ can be at most $(1 + n/3)$-ply transitive, or contains $A_n$ \cite[4, p. 148, Th. VI]{4}. For $n > 9$, $G$ is $A_n$ or $S_n$. That there are no exceptions for $n \leq 9$ follows from the next paragraph.
By (A), each quadruply transitive group of degree $n = p+3$ or $2p+3$, with $p$ an odd prime, is $A_n$ or $S_n$. In the range $8 \leq n \leq 27$, all $n$ are of one of these forms except $n = 11, 12, 15, 18, 19, 21, 23, 24,$ and $27$. It will be shown first that no quadruply transitive group other than $A_n$ and $S_n$ exists for $n = 15, 18, 19, 21,$ and $27$. Then it will be shown that for $n = 11, 12, 23,$ and $24$ there exists no quadruply transitive group other than $A_n$, $S_n$, and the unique Mathieu group of the degree.

In the following, $G$ will denote a quadruply transitive group of degree $n$, not $A_n$ or $S_n$; $G_1, G_2, G_3$, and $H$ the largest subgroups of $G$ fixing respectively one, two, three, and four letters; $h$ the order of $H$; $P_p$ (with a specific subscript) a Sylow $p$-subgroup of $H$; $N_G(P_p)$ the normalizer in $G$ of $P_p$; and $T$ the quadruply transitive constituent of $N_G(P_p)$ on the letters fixed by $P$.

**Degree 15.** By (F), $h$ can be divisible only by $p=2$. By (C), $2|h$. By (E), $P_2$ is of degree at least 6. Thus, by (D), $P_2$ is of degree 10 and $T$ is $S_5$; or $P_2$ is of degree 8 and $T$ is $A_7$. In either case $N_G(P_2)$ must have an element $x$ of order 5. Since $5|h$, $x$ must displace all letters. This excludes $T$ being $A_7$. If $T$ is $S_5$, then $x$ displacing all 15 letters may fix no transitive constituent of $P_2$, and must permute cyclically five constituents of degree 2. These five constituents must be permuted set-wise in $N_G(P_2)$ according to $S_5$. $N_G(P_2)$ has an element of order 3, which must fix two transitive constituents of $P_2$, necessarily
letter-wise. This conflicts with $3^h$.

**Degree 18.** By (F) and (C), $h$ is divisible by $p=2$, but by no other prime. By (D) $T$ is $A_6$ and $P_2$ is of degree 12, or $T$ is $S_4$ and $P_2$ is of degree 14. No transitive 2-group of degree $\leq 12$ has an automorphism of order 5; for a transitive group of degree 8 with an element of order 5 is $A_8$ or $S_8$. In order that $N_G(P_2)$ permute transitive constituents of $P_2$ according to a group homomorphic onto $A_6$, $P_2$ must have six constituents of degree 2 permuted set-wise according to $A_6$. Then $N_G(P_2)$ has an element of order 3 fixing three of these constituents, necessarily letter-wise, conflicting with $3^h$. The only possibility is that $T$ is $S_4$, and $P_2$ is of degree 14.

Let $G'$ be the subgroup consisting of the even permutations of $G$. ($G'$ will denote the largest subgroup of $G'$ fixing one letter, etc.) $G'$ has elements $a$ of order 3 and $b$ of order 5, both displacing 15 letters. $a$ and $b$ must generate a transitive group of degree 15. $G_1'$ is transitive of prime degree, hence primitive, and has $G_3'$ as a transitive subgroup of lower degree. Thus $G_1'$ is doubly transitive [3, p. 207, Th. I], and $G_2'$ is transitive. In turn, $G_2'$ must be doubly transitive. Thus $G'$ is quadruply transitive. To show the non-existence of $G$ of degree 18, it is sufficient to consider $G$ without odd permutations.

A Sylow 17-subgroup $R$ of $G$ must have normalizer in $G$ of order $17 \cdot 2^c$, $c = 0, 1, 2, 3$, or 4. $c=4$ implies that $G$ has odd
permutations. \( c=0 \) implies that \( R \) is in the center of its normalizer in \( G \); in turn, \( G \) has a normal subgroup of index 17 \([3, \text{p.327, Th. II}]\). But a normal subgroup of \( G \) must be triply transitive \([3, \text{p. 198, Th. XI}]\). Thus \( c = 1, 2, \) or \( 3 \). Let \( G \) be of order \( 13 \cdot 17 \cdot 16 \cdot 15 \cdot 2^m \). Having determined the possible orders of the normalizer of a 17-subgroup, and by Sylow's theorem, \( 13 \cdot 16 \cdot 15 \cdot 2^m \equiv 2, 4, \) or \( 8 \) \( (\text{mod 17}) \). Thus \( m \equiv 0, 1, \) or \( 2 \) \( (\text{mod 8}) \); \( m = 1 \) or \( 2 \), or \( m \equiv 8 \).

By (E) each non-identical element of \( G \) displaces at least 8 letters. If \( P_2 \) has an element displacing 10 or fewer letters, then \( P_2 \) has an element of order 2 and degree only 8, since \( P_2 \) is assumed to have all permutations even. Then by the quadruple transitivity of \( G \), there are elements \( s \) and \( t \) of \( G \), both of order 2 and degree 8 permuting four letters \( a, b, c, d \) according to \( s = (a)(bc)(de)(\cdots)(\cdots) \) and \( t = (ab)(c)(df)(\cdots)(\cdots) \), where \( e \) and \( f \) may be the same letter. \( s \) and \( t \) are conjugate under any element of \( G \) permuting \( (ac)(b)(d) \cdots \). \( st \) is of order divisible by 3. As \( s \) and \( t \) displace at least two common letters (\( b \) and \( d \)), together they displace at most 14. \( G \) then has an element of order 3 fixing four letters. Thus \( P_2 \) must have all non-identical elements displacing at least 12 letters.

Since 14 is not a sum of two powers of 2, \( P_2 \) must have at least three transitive constituents. If \( P_2 \) is of order \( \geq 2^9 \), then \( P_2 \) has a subgroup \( P' \) (not necessarily proper) of order \( 2^8 \). If \( P' \)
has three transitive constituents, then the sum of the letters fixed \(3, p. 191, \text{Th. VII}\) by all elements is \(3 \cdot 256\), of which 14 are fixed by the identity. \((3 \cdot 256 - 14)/255 > 2\), so that some non-identical element of \(P_2\) fixes more than two of the 14 letters. The inequality is stronger if \(P_2\) has more than three transitive constituents. The only cases remaining are \(P_2\) of order 2 or 4.

If \(P_2\) is of order 2, however, then \(P_2\) has a unique element of order 2, which must displace all 14 letters, but is then an odd permutation. Thus \(G\) can be of order only 18\cdot17\cdot16\cdot15\cdot4.

Let \(M\) be a Sylow 5-subgroup of \(G\). Since 5th, \(M\) is of order only 5. By (D), \(N_G(M)\), the normalizer in \(G\) of \(M\), is triply transitive on the letters fixed by \(M\). \(N_G(M)\) has an element \(x\) of order 3 permuting cyclically the three letters fixed by \(M\). The group of order 5 has no automorphism of order 3. In order that \(x\) not be a 3-cycle, \(x\) must permute with a generator of \(M\) and interchange cyclically the three transitive constituents of \(M\).

If \(N_G(M)\) also has an element \(y\) of order 3 fixing the letters fixed by \(M\), then \(y\) must also permute with a generator of \(M\) and interchange the constituents cyclically. One of \(xy, xy^2\) must fix the letters displaced by \(M\), and hence be a 3-cycle, displacing the letters fixed by \(M\). Thus \(M\) has its normalizer in \(G_3\) of order prime to 3, so that \(G_3\) has at least 6 Sylow 5-subgroups. The only group of order 60 with 6 Sylow 5-subgroups is \(A_5\). \(A_5\) has a unique transitive permutation representation of degree 15; in this
representation a Sylow 2-subgroup fixes 3 letters, for its normalizer is of order 12. But G cannot have \( P_2 \) of degree 12.

Degree 12. By (C), \( 2|h \). As G is of odd degree, \( P_2 \) has by (D) its T one of \( S_5, A_7 \), or the Mathieu group of degree 11. All alternatives imply that G is of order divisible by 5. This conflicts with (F).

Degree 21. By (F) and (C), \( h \) is divisible by 2, and by no other prime except possibly 3. By (E), \( P_3 \) must be of degree at least 9. If \( P_3 \) is of degree 9, then T is quadruply transitive of degree 12, implying that \( 11|h \). If \( P_3 \) is of degree 12, then T is of degree 9, so that G has an element of order 7 fixing two letters; this implies that \( 7|h \). If \( P_3 \) is of degree 15, then T is \( A_6 \) or \( S_6 \). But a transitive 3-group of degree 9 has solvable automorphism group, and five transitive constituents of degree 3 cannot be permuted set-wise according to a group with a composition factor-group of \( A_6 \). Thus \( 3|h \).

Since G is of odd degree, by (D) \( P_2 \) fixes 5, 7, or 11 letters. If \( P_2 \) fixes 11 letters, then T is of order divisible by 11, so that \( 11|h \). If \( P_2 \) fixes 7 letters, then T is \( A_7 \), and G has an element of order 5 fixing at least two letters, so that \( 5|h \). The only possibility is that \( P_2 \) fixes 5 letters, and is of degree 16.

G must be of order \( 21 \cdot 20 \cdot 19 \cdot 18 \cdot 2^c \cdot c \cdot 5^1 \cdot 11 \cdot 7 \cdot 5 \cdot 3 \cdot 2 \cdot 1 \). Let M be a Sylow 19-subgroup of G. M has normalizer in G of order dividing 19 \cdot 18,
since $G$ cannot contain a transposition. And $M$ has normalizer in $G_2$ of order half as large as in $G$, thus dividing 19·3. Were $M$ in the center of its normalizer in $G_2$, then $G_2$ would have a normal subgroup of index 19 \[3, \text{ p. 327, Th. II}\]. But $G_2$, being doubly transitive, is primitive; and a normal subgroup (not the identity) of a primitive group is transitive \[3, \text{ p. 196, Th. X}\]. Thus $M$ has its normalizer in $G_2$ of order 19·3 or 19·9. By Sylow’s theorem, it is necessary that $6^2 \equiv 1 \pmod{19}$ or $2^2 \equiv 1 \pmod{19}$. The solutions of the congruences are respectively $c \equiv 4 \pmod{18}$ and $c \equiv 17 \pmod{18}$. As the order of a Sylow 2-subgroup of $S_{16}$ is only $2^{15}$, the only possibility is $c=4$.

$G$ must be of order 21·20·19·18·16. $P_2$ is of order 16 and of degree 16. $N_G(P_2)$ has an element $x$ of order 5. As no element of order 5 of $G$ can fix more than one letter, $x$ fixes only one letter displaced by $P_2$. If $x$ interchanges transitive constituents of $P_2$, then $x$ interchanges only 5 constituents of degree 2, and fixes set-wise transitive constituents the sum of whose degrees is 6. These six letters must be fixed by $x$, implying that $5|h$. Thus $x$ must fix each transitive constituent of $P_2$. $x$, being of odd prime order, must fix at least one letter in each transitive constituent of $P_2$. Hence $P_2$ must have only one transitive constituent, which will be of degree 16. $P_2$ is regular.

$N_G(P_2)$ has an element $y$ of order 3. As no element of order 3 of $G$ can fix more than three letters, $y$ fixes only one letter
of $P_2$. Some conjugate $y'$ of $y$ fixes the letter fixed by $x$. $x$ and $y'$ must generate a group transitive on 15 letters displaced by $P_2$. Thus $P_2$ has automorphism group transitive on its non-identical elements, and must be elementary abelian.

$G_j$ must be imprimitive on the nine pairs of letters fixed by the conjugate class of subgroups including $P_2$. For if $a$, $b$ are the two letters fixed by $P_2$, and an element $z$ of $G_3$ maps $a$, $b$ set-wise onto $a$, $c$ with $b \neq c$, then $z^{-1}P_2z$ fixes $a$, $c$ and is transitive on the other letters. It would follow that $P_2 \cup z^{-1}P_2z$ must be transitive on all letters but $a$. The normal subgroup $K$ of $G_j$ fixing the nine pairs set-wise has all non-identical elements of order 2. As each non-identical element of $G_j$ displaces at least 16 letters, $K$ is of order at most 2. If $K$ is of order 2, then $K$, being a normal subgroup of $G_j$, must displace all letters. And $K$ intersects each conjugate of $P_2$ in only the identity. Let the nine pairs of imprimitivity of $G_j$ be designated as points. Then $B = G_j/K$ is a transitive permutation group of degree 9 on points; and of order $9 \cdot 2^5$ or $9 \cdot 2^4$, depending upon whether $K$ is of order one or two. In either case, all elements of $P_2$ represent distinct cosets of $K$, so that $B$ has an elementary subgroup of order 16. Since no element of order 3 of $G_3$ fixes a letter, no element of order 3 of $B$ fixes a point. If $B$ is imprimitive, the partition must be into three triples of points. The largest subgroup of $B$ fixing the triples set-wise can be of order at most $3!$, if of
order divisible by 3 (otherwise an element of order 3 fixes a point); or 8 if of order prime to 3. And the factor-group permuting triples set-wise is of order dividing 3! Imprimitive B therefore cannot be of order as large as $9 \cdot 2^4$. B is solvable [3, p. 323, Cor. III], being of order divisible by only two primes. Hence B has a normal regular elementary subgroup A of order 9. The elements of a Sylow 2-subgroup of B must induce distinct automorphisms on A. The automorphism group of the elementary group of order 9 is or order $(9-1)(9-3)$, which is divisible by $2^4$ but not by $2^5$. A Sylow 2-subgroup of this automorphism group is not the elementary group of order $2^4$. For the elementary group of order 9, generated by u and v, has an automorphism determined by $u \rightarrow v, v \rightarrow u^2$, which is of order 4, permuting $(u, v, u^2, v^2)(uv, u^2v, u^2v^2, uv^2)$.

Degree 27. By (F) and (C), h is divisible by 2, and by no other prime except perhaps 3. By (E), $P_3$ must be of degree at least 12. If $P_3$ is of degree 12, then quadruply transitive T is of degree 15, implying that $7|h$. $P_3$ of degree 15 and T of degree 12 implies that $11|h$. $P_3$ of degree 18 and T of degree 9 implies that $7|h$. The remaining possibility is $P_3$ of degree 21, in which case T is $A_6$ or $S_6$. Then $N_T(P_3)$ has an element $x$ of order 5, which fixes only one letter displaced by $P_3$, since $5|h$. No transitive 3-group of degree $<21$ has an automorphism of order 5; hence $x$ must permute similar transitive constituents of $P_3$. The only
possibility is that \( x \) permutes five constituents of degree 3 cyclically and fixes two constituents of degree 3. But then \( x \) fixes the letters of the fixed constituents, implying that \( 5|h \). Accordingly, \( 3|h \).

\( G \) being of odd degree, by (D) \( P_2 \) fixes 5, 7, or 11 letters. The latter two cases imply respectively that 7 and 11 divide \( h \). Thus \( P_2 \) is necessarily of degree 22 and \( T = S_5 \). \( N_G(P_2) \) has an element \( y \) of order 3, which must fix exactly one letter displaced by \( P_2 \). Accordingly, \( y \) fixes set-wise exactly one transitive constituent of \( P_2 \), since 3 is prime to 2; this constituent fixed by \( y \) must be of degree \( 1 \pmod{3} \). The remaining transitive constituents of \( P_2 \) are then of equal degrees in triples. The possibilities are 16; 2, 2, 2; and 4; 4, 4, 4; 2, 2, 2; and 4; 2, 2, 2; 2, 2, 2; 2, 2, 2. \( N_G(P_2) \) has also an element \( z \) of order 5, which must fix only two letters displaced by \( P_2 \). But in all three indicated partitions of the letters displaced by \( P_2 \) into transitive constituents, \( z \) must fix at least three constituents of degree 2, necessarily letter-wise.

**Degree 11.** By (C), either \( G \) is the Mathieu group of degree 11, or \( 2|h \). If \( 2|h \), then by (D), since \( G \) is of odd degree, \( T \) associated with \( P_2 \) is either \( S_5 \) or \( A_7 \). (\( T \) is, of course, of lower degree than \( G \).) In either case \( N_G(P_2) \) has an element of order 5, which can only fix all 4 or 6 letters of \( P_2 \), implying that \( 5|h \).

This argument for the uniqueness of \( G \) of degree 11 is in-
CLUDED on account of its brevity. The result will be obtained again from arguments below.

**Degrees 11, 23.** The following will be established:

(L). If $K$ is a triply transitive group of degree 11 or 23, then $K$ is alternating, symmetric, or the Mathieu group of that degree.

Proof. Let $K_2$ be the largest subgroup of $K$ fixing two letters. Let $K'$ be the subgroup of even permutations of $K$, and let $K'_1$ and $K'_2$ be the largest subgroups of $K'$ fixing respectively one and two letters. $K'_2$, being of odd degree, is transitive; otherwise transitive $K'_2$ would have a normal subgroup of index 2, which must have exactly two transitive constituents of like degree. $K'_1$, being transitive of prime degree, is primitive. Having $K'_2$ as a transitive subgroup of lower degree $[3, p. 207, Th. 1]$, $K'$ is doubly transitive. Therefore $K'_1$ is transitive, and necessarily doubly transitive. In turn $K'$ is triply transitive. The Mathieu groups are simple $[4, p. 283, Exercises 3, 4]$, thus have no odd permutations.

To prove (L), it is now sufficient to demonstrate two propositions:

(M). If $K$ is a triply transitive group of degree 11 or 23 without odd permutations, then $K$ is alternating or a Mathieu group.

(N). If the Mathieu group of degree 11 or 23 is a subgroup
of a group $K$ of the same degree, and $K$ contains odd permutations, then $K$ is symmetric.

Proof of (M). The degrees $p=11$ and $p=23$ of $K$ are both of the form $p = 2q+1$, with $p$ and $q$ both primes. Let $P$ be a Sylow $p$-subgroup of $K$. As $K$ has no normal subgroup of index $p$, $P$ cannot be in the center of its normalizer in $K$ [3, p. 327, Th. II]. $P$ is cyclic; let $a$ be a generator of $P$. $K$ has an element $b$ not permutable with $a$, and transforming $a$ into a power of itself. $b$ must be of order dividing $p-1$. The elements of even order of the holomorph of $P$ are odd permutations. Hence $b$ must be of order $q$. $a$ and $b$ generate the unique subgroup of index 2 of the holomorph of $P$; thus $b$ may be chosen as any element of order $q$ normalizing $P$.

Let $Q$ be a Sylow $q$-subgroup of $K$. $Q$ is a subdirect product of two groups of order $q$. Were $Q$ of order $q^2$, then $K$ would have as an element a single cycle of length $q$. $K$ is primitive; thus by (B), $K$ would be $(q+2)$-ply transitive of degree $q + (q+1)$. By (A), $K$ is then alternating. Accordingly, $Q$ is of order $q$, and $b$ generates a Sylow $q$-subgroup of $K$.

Were $Q$ in the center of its normalizer in $K$, then the commutator-subgroup $K^*$ of $K$ would be of order prime to $q$. Then $P$ would be its own normalizer in $K^*$, so that the second derived subgroup of $K$ would be of order prime to $p$. Thus $K$ must have an element $c$ not permutable with $b$, and transforming $b$ into a
power of itself.

The normalizer of $Q$ in $S_p$ has a subgroup $J$ of index 2 fixing the cycles of $b$ set-wise. Each element $j$ of $J$ not in $Q$ transforms the two cycles of $b$ into like powers of themselves. $j$ fixes the single letter fixed by $Q$, and exactly one letter of each cycle of $b$, hence a total of three letters. Thus $j$ displaces $2(q-1)$ letters in cycles all of length equal to the same divisor of $q-1$. Accordingly, $J$ has all permutations even. On the other hand, an element of order 2 permuting with $b$ and interchanging the cycles is an odd permutation. $J$ is precisely the subgroup of even permutations normalizing $Q$; $c$ must fix the cycles of $b$ set-wise.

It is expedient to identify the letters permuted by $K$ with the residue classes $(\text{mod } p)$. Without loss of generality, $a$ can be chosen as $x \mapsto x+1 \pmod{p}$; that is, $(0, 1, \ldots, p-1)$. $b$ permutes the quadratic residues of $p$ in one cycle, and the quadratic non-residues in the other. As pointed out above, $b$ may be chosen as any element of order $q$ normalizing $P$. Thus $b$ may be identified with $x \mapsto 4x \pmod{p}$. In the normalizer of $Q$ each letter displaced by $Q$ is fixed by one conjugate of $c$. Thus $c$ may be chosen to fix letter 1. $c$ fixes the cycles of $b$ set-wise and transforms the cycles into like powers of themselves. Thus $c$ is of the form $(x^2 \mapsto x^{2t}) \cdot (nx^2 \mapsto nx^{2t}) \pmod{p}$, where $t$ is a fixed positive integer and $n$ is a fixed quadratic non-residue.
of p. Under the operation of conjugation in $S_p$ by $x \rightarrow nx \pmod{p}$, $a$ is transformed into $a^{-n}$, $b$ into itself, and $c$ (displayed above) into $(x^2 \rightarrow x^{2t}) \cdot (x^{2/n} \rightarrow x^{2t/n}) \pmod{p}$. The groups generated by $a$, $b$, $c$, and by transformed $a$, $b$, $c$ are distinct for $n^r-1 \pmod{p}$, but permutation-isomorphic. Accordingly, it is sufficient, for a given $t$, to examine the groups generated by $a$, $b$, and $c$, where the c's are $(x^2 \rightarrow x^{2t}) \cdot (x^m \rightarrow x^{mt}) \pmod{p}$, with the range on $m$ being $0 \leq m \leq (p-3)/4$; $-1$ is, of course, a quadratic non-residue of $p=11$ and $p=23$. As $Q$ has a cyclic automorphism group, and a cyclic group has all subgroups characteristic, the group generated by $a$, $b$, and $c$ is determined by $m$ and the order of $c$. From the arguments on Sylow subgroups of $K$, it follows that $a$ and $c$ generate the group generated by $a$, $b$, and $c$. ($c$ is, of course, not the identity.)

For $p=11$, the order of $c$ is a divisor, greater than 1, of $q-1 = 4$. If $c$ is of order 2, then $t$ may be chosen as 9. For $m = 0, 1, 2$, the three choices of $c$ are respectively:

$c_0 = (1)(3,4)(9,5)(10)(8,7)(2,6)$;
$c_1 = (1)(3,4)(9,5)(7)(10,6)(8,2)$;
$c_2 = (1)(3,4)(9,5)(6)(7,2)(10,8)$.

It is now easily checked that

$a^3c_0 = (0,4,8)(1,3,2,9)(5,7,10,6)$;

$ac_2 = (0,1,7,10)(2,4,9,8,5,6)(3)$.

The fourth power of $a^3c_0$ is a 3-cycle; the sixth power of $ac_2$ is
a product of two transpositions. Thus $a, c_0$; and $a, c_2$ are both pairs of generators of $A_p$. On the other hand, $a$ and $c_1$ generate the doubly transitive group of order $11 \cdot 10 \cdot 6$ [4, p. 288]. For $c$ of order 4, $m=0$ and $m=2$ must again with $a$ give a pair of generators of $A_p$. For $c$ of order 4 and $m=1$, $a$ and $c_1$ generate the Mathieu group. To display the pair of generators of the Mathieu group given by Carmichael [4, p. 151, Exercise 12], one must select $c$ with $m=4$, giving a group conjugate in $S_{11}$ to that with $m=1$. The generator given by Carmichael is

$$c = (4, 5, 3, 9)(10, 7, 2, 6).$$

The group $D$ of order $11 \cdot 10 \cdot 6$ is, of course, not triply transitive. Any group $D'$ of even permutations properly containing $D$, but not containing the Mathieu group, must have normalizer of $P$ of order exactly $11 \cdot 5$, and normalizer of $Q$ of order exactly $5 \cdot 2$, as does $D$. That is, the index $f$ of $D$ in $D'$ must be $\equiv 1 \pmod{11}$ and $\equiv 1 \pmod{5}$. Since $D'$ is assumed to be a subgroup of $A_{11}$, $f$ must divide $(\frac{2}{11} 11)!/(11 \cdot 10 \cdot 6)$. In order that $D'$ not be alternating, $f$ must be prime to 5 and 7. Thus $f \equiv 1 \pmod{55}$, and $f \mid 25 \cdot 3^3$. No such $f$ exists. Accordingly, any triply transitive group of degree 11 consisting of even permutations contains the Mathieu group.

A group of even permutations containing the Mathieu group must have normalizers of $P$ and $Q$ of the same orders as in the Mathieu group. The above arguments apply again with, in fact,
the index of the group in $A_5$ a divisor of $2^3 \cdot 3^2$. (M) is established for degree 11: the only triply transitive proper subgroup of $A_{11}$ is the Mathieu group.

Triply transitive $K$ of degree 23 properly contained in $A_{23}$ must have normalizer of $Q$ of order $11 \cdot 2$, $11 \cdot 5$, or $11 \cdot 10$. If the normalizer of $Q$ is of even order, then (up to permutation-isomorphism) $K$ must contain $a$, and $c$ of order 2. For $c$ of order 2, $t$ may be chosen equal to 21. For $m = 0, 1, 2, 3, 4, 5$, the respective permutations $c$ are:

- $c_0 = (1)(2,12)(4,6)(8,3)(16,13)(9,18)
  (22)(21,11)(19,17)(15,20)(7,10)(14,5);
- $c_1 = (1)(2,12)(4,6)(8,3)(16,13)(9,18)
  (19)(15,21)(7,22)(14,11)(5,17)(10,20);
- $c_2 = (1)(2,12)(4,6)(8,3)(16,13)(9,18)
  (7)(14,15)(5,19)(10,21)(20,22)(17,11);
- $c_3 = (1)(2,12)(4,6)(8,3)(16,13)(9,18)
  (5)(10,14)(20,7)(17,15)(11,19)(22,21);
- $c_4 = (1)(2,12)(4,6)(8,3)(16,13)(9,18)
  (20)(17,10)(11,5)(22,14)(21,7)(19,15);
- $c_5 = (1)(2,12)(4,6)(8,3)(16,13)(9,18)

The following products are exhibited:

- $a^c_0 = (0,6,7,21,12,13,19)(1,14,9,16,15,17,11,20)
  (2,4,3,10,5,18,22,8);
\[ a^4 c_1 = (0,6,20,1,17,15,19)(2,4,3,22,8) \]
\[ \quad (5,18,7,14,9,16,10,11,21,12,13); \]
\[ a c_2 = (0,1,12,16,11,2,8,18,5,4,19,22)(3,6,7) \]
\[ \quad (9,21,20,10,17)(13,15)(14); \]
\[ a c_3 = (0,1,12,16,15,13,10,19,7,3,6,20,22) \]
\[ \quad (2,8,18,11)(4,5)(9,14)(7,12,13,19,20); \]
\[ a^4 c_4 = (0,6,17,7,5,18,14,9,16,20,1,11,19) \]
\[ \quad (2,4,3,21,12,13,10,22,8)(15); \]
\[ a^2 c_5 = (0,12,7,18,21)(1,8,19,20,17,10,2,6,3,15,22) \]
\[ \quad (4)(5,14,13)(9,11,16). \]

The eighth, seventy-seventh, twelfth, fifty-second, ninth, and thirty-third powers of the above products are single cycles of lengths respectively the primes 7, 5, 5, 3, 13, and 5. Thus, if c is of even order, then a and c generate \( A_{23} \).

There remains the possibility that c is of order 5. It can be chosen equal to 4. For \( m = 0, 1, 2, 3, 4, 5 \), the c are respectively:

\[ c_0 = (1)(2,16,9,6,8)(4,3,12,13,18) \]
\[ \quad (22)(21,7,14,17,15)(19,20,11,10,5); \]
\[ c_1 = (1)(2,16,9,6,8)(4,3,12,13,18) \]
\[ \quad (19)(15,5,10,22,14)(7,11,21,17,20); \]
\[ c_2 = (1)(2,16,9,6,8)(4,3,12,13,18) \]
\[ \quad (7)(14,20,17,19,10)(5,21,15,22,11); \]
\[ c_3 = (1)(2,16,9,6,8)(4,3,12,13,18) \\
\quad (5)(10,11,22,7,17)(20,15,14,19,21); \]
\[ c_4 = (1)(2,16,9,6,8)(4,3,12,13,18) \\
\quad (20)(17,21,19,5,22)(11,14,10,7,15); \]
\[ c_5 = (1)(2,16,9,6,8)(4,3,12,13,18) \\
\quad (11)(22,15,7,20,19)(21,10,17,5,14). \]

\[ a \text{ and } c_3 \text{ are generators of the Mathieu group} \begin{Large}[4, p. 164, \end{Large} \]

Exercise 9]. On the other hand, some products are:

\[ ac_0 = (0,1,16,15,9,5,8,6,14,21,22)(2,12,18,20,7) \]
\[ (3)(4,19,11,13,17)(10); \]
\[ ac_1 = (0,1,16,20,17,4,10,21,14,5,8,6,11,13,15,9,22) \]
\[ (2,12,18,19,7)(3); \]
\[ a^3c_2 = (0,12,22,16,10,18,15,4,7,14,19,11,20) \]
\[ (1,3,8,5,2,21)(6)(9,13)(17); \]
\[ ac_4 = (0,1,16,21,17,4,22)(2,12,18,5,8,6,15,9,7) \]
\[ (3)(10,14,11,13)(19,20); \]
\[ a^2c_5 = (0,16,4,8,17,22,1,12,21) \]
\[ (2,3,14,9,11,18,19,10,13,7,6)(5,20,15). \]

The fifth, seventeenth, sixth, thirty-sixth, and ninth powers of the above are single cycles of lengths the respective primes 11, 5, 13, 7, and 11. Thus triply transitive \( K \) of degree 23 consisting of even permutations contains the Mathieu group.

Let \( W \) be a group of even permutations of degree 23 containing the Mathieu group of degree 23, and not \( A_{23} \). Thus the normalizers
in \( W \) of \( P \) and \( Q \) are of orders \( 23 \cdot 11 \) and \( 11 \cdot 5 \) respectively, as in the Mathieu group. The index \( f \) of the Mathieu group in \( W \) is a divisor of \( (\frac{1}{2} \cdot 23!) / (23 \cdot 22 \cdot 21 \cdot 20 \cdot 16 \cdot 3) \). \( W \) is quadruply transitive; thus by (F), \( h \) is divisible by 2 and 3, but by no other prime.

The conditions on \( f \) are \( f > 1, f \equiv 1 \pmod{11 \cdot 23}, f \mid 2^{11} \cdot 3^7 \). Set \( f = 2^s \cdot 3^t \). Then, using indices, \( s + 8t \equiv 0 \pmod{10} \), and \( 2s + 16t \equiv 0 \pmod{22} \), with \( 0 \leq s \leq 11, \ 0 \leq t \leq 7 \). Then \( s \) is even.

Setting \( s = 2u \), the congruences are \( 2u + 8t \equiv 0 \pmod{10} \), and \( 4u + 16t \equiv 0 \pmod{22} \), with \( 0 \leq u \leq 5, \ 0 \leq t \leq 7 \). In turn, \( u + 4t \equiv 0 \pmod{55} \). The only solution is \( u = t = 0 \), for which \( f = 1 \).

No \( W \) exists. (M) is established for degree 23. The non-existence of \( W \) could be shown alternatively by considering normalizers in \( W \) of Sylow 2- and 3-subgroups of \( H \), knowing their structures in the Mathieu group.

**Proof of (N).** Let \( K \) be a triply transitive group of degree 11 or 23, containing odd permutations. Let \( K' \) be the subgroup of even permutations of \( K \). \( K \) is symmetric if and only if \( K' \) is alternating. Assume that \( K \) is not symmetric. \( K' \) is triply transitive, as pointed out earlier; by (M), \( K' \) is the Mathieu group.

\( P \) must have normalizer in \( K \) of order twice as large as in the Mathieu group. Thus \( K \) is the group generated by the Mathieu group and \( x \mapsto x \pmod{p} \); this permutation will be designated by \( d \).

\( d \) is then \( x \mapsto x + 1 \pmod{p} \). For degree \( p = 11 \),

\[
da = (0,1)(2,10)(3,9)(4,8)(5,7)(6).
\]
The square of the displayed generator $\mathsf{c}$ of the Mathieu group of degree 11 is
\[
\mathsf{c}^2 = (0)(1)(4,3)(5,9)(8)(10,2)(7,6).
\]
Thus
\[
\mathsf{dac}^2 = (0,1)(2)(3,5,6,7,9,4,8)(10),
\]
with seventh power a transposition. For degree 23,
\[
\mathsf{da} = (0,1)(2,22)(3,21)(4,20)(5,19)(6,18)
\]
\[
\]
And the generator of the Mathieu group,
\[
\mathsf{c} = (0)(1)(2,16,9,6,8)(4,3,12,13,18)
\]
\[
(5)(10,11,22,7,17)(20,15,14,19,21).
\]
And
\[
\mathsf{dac} = (0,1)(2,7,10,19,5,21,12,13,22,16)(3,20)
\]
\[
(4,15,6)(8,9,14,11,18)(17),
\]
with tenth power a 3-cycle. For both degrees the group generated by the Mathieu group and $\mathsf{d}$ is symmetric. This establishes (N), and in turn (L):
For degrees 11 and 23, the only triply transitive groups are alternating, symmetric, and the Mathieu groups. A fortiori, these are the only quadruply transitive groups of these degrees.

**Degrees 12, 24.** If $\mathsf{G}$ is quadruply transitive of degree 12 or 24, then the largest subgroup $\mathsf{G}_1$ of $\mathsf{G}$ fixing one letter is triply transitive of degree respectively 11 or 23. Assume that $\mathsf{G}$ is neither alternating nor symmetric. Then by (L), $\mathsf{G}_1$ is the Mathieu group of appropriate degree. It is well known that the Mathieu groups of degrees 11 and 23 are simple \[4, p. 283, Exercises 3, 4\]. For neither degree can $\mathsf{G}$ have a normal subgroup
with all non-identical elements displacing all letters. Thus \( G \) must be simple. In particular, \( G \) lacks odd permutations.

Let \( X \) be the letter fixed by \( G_1 \) and let \( G_2 \) be the largest subgroup of \( G \) fixing \( X \) and 0. \( Q \) is a Sylow subgroup of \( G_2 \).

The normalizer of \( Q \) in \( G_2 \) is the same as that in \( G_1 \); and \( Q \) has normalizer of twice this order in \( G \). All elements of the normalizer in \( G \) of \( Q \), but not in \( G_1 \), interchange \( X \) and 0. The triply transitive groups of degrees 11 and 23 have been determined, it follows that \( G \) is generated by the Mathieu group of degree 11 or 23 and one element \( e \) interchanging \( X, 0 \) and normalizing \( Q \).

Of course, \( e \) cannot be the transposition \((X0)\).

In the Mathieu group of degree 11, \( Q \) is of order 5 and its normalizer is of order \( 5^4 \). All automorphisms of \( Q \) are induced under transformation by elements of its normalizer in the Mathieu group. \( e \) must interchange the cycles of \( b \), and may be chosen to transform \( b \) into any non-identical power of \( b \). It will be assumed that \( e \) is of order 2, and that \( b \) and \( b^{-1} \) are conjugate under \( e \). \( b \) and \( e \) generate a dihedral group, with all elements of order 2 conjugate; thus \( G \) is completely determined by the conditions that \( e \) is of order 2, interchanges the cycles of \( b \), and transforms \( b \) into \( b^{-1} \).

\[
b = (X)(0)(1,4,5,9,3)(10,7,6,2,8).
\]

Thus one may set

\[
e = (X,0)(1,10)(4,8)(5,2)(9,6)(3,7).
\]

This \( e \) is a generator, with \( a \) and \( c \), of the Mathieu group of
degree 12 \([4, \text{p. } 151, \text{Exercise } 12]\). For degree 12, the only quad-
ruply transitive groups are alternating, symmetric, and the
Mathieu group.

For degree 24 there are more possibilities to consider. Q
will have normalizer in G of order 11·10. As 4 does not divide
the order of this normalizer, e may be chosen of order 2. By
earlier considerations, any odd permutation of \(S_{23}\) normalizing
Q interchanges the cycles of Q. In order that e be an even
permutation of degree 24, e must induce an odd permutation on
the letters displaced by Q. Hence e interchanges the cycles of b.
Either e permutes with b, or e transforms b into \(b^{-1}\). (Unlike the
situation for degree 12, these cases are essentially different;
for here the normalizer of Q in \(G_1\) is of odd order.) If e trans­
forms b into \(b^{-1}\), then G is determined, for b and e generate a
dihedral group with all elements of order 2 conjugate. e may be
chosen as \(x \rightarrow -1/x \pmod{23}\), with \(-1/0\) identified with X. With
a and c, this e generates the Mathieu group of degree 24 \([4,
\text{p. } 164, \text{Exercise } 9]\).

There remains the alternative that e permutes with b. Of
course, each 2-cycle of e on the letters displaced by b inter-
changes a quadratic residue and a quadratic non-residue of 23.
There are initially 11 choices for e; fortunately, only three of
these are essentially distinct. e is determined by the map of
letter 1, which is fixed by c. If e maps 1 onto a letter in
either 5-cycle of quadratic non-residues of \( c \), then \( e \) is in a set of 5 conjugates under \( c \). The following are representatives of the three conjugate classes of choices for \( e \):

\[
e_1 = (X,0)(1,5)(4,20)(16,11)(18,21)(3,15)(12,14) \\
(2,10)(8,17)(9,22)(13,19)(6,7);
\]

\[
e_2 = (X,0)(1,10)(4,17)(16,22)(18,19)(3,7)(12,5) \\
(2,20)(8,11)(9,21)(13,15)(6,14);
\]

\[
e_3 = (X,0)(1,20)(4,11)(16,21)(18,15)(3,14)(12,10) \\
(2,17)(8,22)(9,19)(13,7)(6,5).
\]

Some products are displayed:

\[
a^3e_1 = (X,0,15,21,5,17,4,6,22,10,19,9,14,8,16,13, \\
11,12,3,7,2,1,20)(18);
\]

\[
a^4e_1 = (X,0,20,5,22,15,13,8,14,21,10,12,11,3,6,2, \\
7,16,4,17,18,9,19)(1). \text{ Thus}
\]

\[
a^3e_1a^4e_1 = (X,20,0,13,3,16,8,4,2,1,5,18,9,21,22,12,6,15,10) \\
(7)(11)(14)(17)(19),
\]

which is a 19-cycle; thus \( a, c, \) and \( e_1 \) generate \( A_{24} \).

\[
ae_2 = (X,0,10,8,21,16,4,12,15,22)(1,20,9) \\
(2,7,11,5,14,13,6,3,17,19)(18),
\]

whose tenth power is a 3-cycle.

\[
 ae_3 = (X,0,20,16,2,14,18,9,12,7,22)(1,17,15,21,8,19) \\
(3,11,10,4,6,13)(5), \text{ whose sixth power is an 11-cycle.}
\]

The only quadruply transitive groups of degree 24 are alternating, symmetric, and the Mathieu group.
References


Autobiography

I, Ernest Tilden Parker, was born in Royal Oak, Michigan, July 26, 1926. I received my secondary education in the public schools of Evanston, Illinois, and my undergraduate training at Northwestern University, which granted me the Bachelor of Arts degree with honors in 1947. I was enrolled in the Graduate School at Northwestern University from 1947 to 1949, during which time I held the position of Tutorial Fellow. At the University of Texas between 1949 and 1954, I held fellowships most of the time, and was appointed temporarily to the position of Instructor in Mathematics during the summer semester of 1952. I was a Teaching Assistant in Mathematics at the Ohio State University during the academic year 1954-55. From 1955 to 1957, I held the position of Research Assistant in Mathematics at the Ohio State University, during which time I completed the requirements for the degree Doctor of Philosophy.