ON QUADRUPLY TRANSITIVE GROUPS

E. T. PARKER

1. Introduction. A major unsolved problem in the theory of groups is whether there are any quadruply transitive finite groups other than the alternating and symmetric groups and the four Mathieu groups of degrees 11, 12, 23, and 24, respectively.

In this paper are proved two theorems which impose arithmetic restrictions on primes dividing the order of the subgroup fixing four letters of a finite quadruply transitive group, and on the degrees of Sylow subgroups thereof.

THEOREM 1 is stated, followed by a corollary, which is somewhat less general but of a more direct arithmetic form.

THEOREM 1. *If G is a quadruply transitive finite permutation group, H is the 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 component A_r or S_r permuting the letters fixed by P, and P has no component of degree $\geq p^3$ and no set of $r(r-1)/2$ permutation-isomorphic components, then G is 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 component A_r or S_r permuting the letters fixed by P, then G is A_n or S_n.*

This corollary is a partial generalization of a theorem of G. A. Miller [6], which may be paraphrased to read like the above with " quadruply transitive " replaced by " primitive " and the inequalities replaced by " $k < p, k < r, r \geq 5$ " $-$ " $r \geq 3$ " if the component of the normalizer of P is restricted to be S_r. Miller's theorem is proved for $r \geq 5$ by showing first that the component A_r of the normalizer of $P -$ or a subgroup of P of index 2 – splits off as a direct factor. The argument is completed by invoking the theorem of Netto [3, p. 207, Th. I] on primitive groups with primitive subgroups of lower degree. The proof of Theorem 1 makes use of the techniques in Miller's theorem; and in addition results on the structure of the automorphism groups of noncyclic groups of order p^2, on distribution of primes, and in particular

a theorem of Bochert [1] giving a lower bound on the degrees of per-
mutations in quadruply transitive groups.

A consequence of Miller's theorem, not mentioned in his paper, is
that for infinitely many degrees, namely $p + 3$ and $2p + 3$ with p prime,
quadruply transitive groups can be only the alternating or symmetric
groups.

THEOREM 2. *If G is a quadruply transitive permutation group
of degree n, and the subgroup of G fixing four letters is of order
divisible by an odd prime p, with $5p > n - 4, 4p \neq n - 4$, then G is
A_n or S_n.*

Some comments on terminology are in order: A_n and S_n designate
respectively the alternating group and the symmetric group of degree
n. A *component* of a permutation group is the permutation group in-
duced on a transitive set of letters. "The subgroup fixing four letters"
of a quadruply transitive group is the *largest* subgroup (unique to con-
jugacy) fixing four letters *individually*. (The phrase "fixed set-wise"
is used explicitly when appropriate.)

Included in the author's dissertation is a self-contained proof that
the only quadruply transitive groups of degrees $n \leq 27$ are the alternat-
ing and symmetric groups, $6 \leq n \leq 27$ and $4 \leq n \leq 27$ respectively, and
the Mathieu groups of degrees 11, 12, 23, and 24. As this result is in
the literature (except perhaps for degree 27), though likely in no single
source, these rather lengthy arguments are not included in this paper.

Section 2 contains three lemmas needed to prove Theorem 1. In
§§ 3 and 4 are the proofs respectively of Theorem 1 and its corollary,
and Theorem 2.

2. In this section are three lemmas.

LEMMA 1. *If B is a transitive permutation group of degree p or
p^2 (p prime), and if B has a normal p-subgroup, then B has no com-
position factor[1] isomorphic with $A_r, r > 5$.*

Proof. If B is of degree p, then B is the metacyclic[2] group or
a subgroup thereof, and hence is solvable.

If B is of degree p^2, then the normal p-subgroup T has an ele-
mentary 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 p^2

---

[1] A factor group of a composition series.
[2] The holomorph of the group of order p.

letters, and has all components permutation-isomorphic. C being abelian has all components regular. Thus C is either the regular elementary group of order p^2, or a subdirect product of p p-cycles.

If C is regular, then B is in the holomorph of the elementary group of order p^2. The only unsolvable [3, pp. 428-34] composition factor of this holomorph is $LF(2, p)$. The smallest alternating group of order divisible by p is A_p. $LF(2, p)$ is isomorphic with no alternating group whenever $p > 5$, since $p(p^2 - 1)/2 < p!/2$. The only unsolvable proper subgroup of $LF(2, p)$ is isomorphic with A_5 — $LF(2, p)$ is isomorphic with A_5 for $p = 5$, and has such a subgroup for $p \equiv \pm 1 \pmod 5$ [3, pp. 440-50].

If C is a subdirect product of p p-cycles, then each element of B must permute the transitive sets of C among themselves; these are sets of imprimitivity for B. Let K be the largest subgroup of B fixing the sets of imprimitivity; K is a normal subgroup of B. B/K is a permutation group on the transitive sets of K. Since T is transitive and K is intransitive, T is not a subgroup of K. Hence B/K has a normal p-subgroup. B/K of degree p is in the metacyclic group, and is therefore solvable. K is a subdirect product of metacyclic groups. Thus B is solvable.

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

Proof. Assume that A_r has a subgroup L of index t (r, t as above).

If L is intransitive, then L is in the group M_i of even permutations in the direct product of S_i and S_{r-i}, $0 < i < r$. M_i is of index $\binom{r}{i}$ in A_r. $\binom{r}{i} \geq r(r-1)/2$ unless $i = 1$ or $r - 1$. For $i = 1$ or $r - 1$, M_i is A_{r-1}, of index r which fails to satisfy the strict inequality. A_{r-1} has no proper subgroup of index $< r - 1$; hence M_i has no proper subgroup of index $< r(r-1)/2$ in A_r.

There remains for consideration the case of L transitive.

Let q be a prime in the range $r/2 < q \leq r$. If L is of order divisible by q, then an element of L is a q-cycle, and L is primitive [4, p. 162, Exercise 8]. If further $q \leq r - 3$, then L is A_r [6]. Transitive L fulfilling the assumption must be of index in A_r divisible by each prime q, $r/2 < q \leq r - 3$.

A theorem on distribution of primes will now be used [2, 7]: *If $x \geq 25$, then there exists a prime q such that $x < q < 6x/5$.* A computation shows that for all $r \geq 50$ there exist primes q_1, q_2, q_3 satisfying $r/2 < q_1 < q_2 < q_3 \leq r - 3$. The existence of a triple of primes for each r in the range $20 \leq r < 50$ is verified by inspection. For any $r \geq 20$, $q_1 q_2 q_3 > (r/2)^3 > r(r-1)/2$.

Degrees $9 \leqq r \leqq 19$ remain to be considered. A primitive proper subgroup of A_r has no element a q-cycle, with prime $q \leqq r - 3$. If L is primitive, then for each odd prime $q \leqq r - 3$ a Sylow q-subgroup of L must be a proper subgroup of that of A_r. Thus the index of L in A_r must be divisible by each prime $q, 2 < q \leqq r - 3$. This inequality is satisfied by primes $q = 3, 5, 7, 11$ when $14 \leqq r \leqq 19$; and $3 \cdot 5 \cdot 7 \cdot 11 > r(r - 1)/2$ for these values of r. Similarly $q = 3, 5, 7$ for $10 \leqq r \leqq 13$, and $3 \cdot 5 \cdot 7 > r(r - 1)/2$. Primitive L does not exist for $10 \leqq r \leqq 19$.

Imprimitive L must be of index divisible by each prime $q, r/2 < q \leqq r$. For $17 \leqq r \leqq 19, q = 11, 13, 17$, and $11 \cdot 13 \cdot 17 > r(r - 1)/2$. For $13 \leqq r \leqq 16, 11 \cdot 13 > r(r - 1)/2$. For $r = 11$ or $12, 7 \cdot 11 > r(r - 1)/2$. The maximal imprimitive subgroups of A_{10} are of orders $\frac{1}{2} \cdot 2!(5!)^2$ and $\frac{1}{2} \cdot 5!(2!)^5$, both of index $> 10 \cdot 9/2$. Such a subgroup of A_9 has order $\frac{1}{2} \cdot 3!(3!)^3$; index $> 9 \cdot 8/2$.

One case remains, namely degree 9 with L primitive. L must be of index divisible by 3 and 5. Since $3 \cdot 3 \cdot 5 > 9 \cdot 8/2$, L can be of index only 15 or 30 in A_9. L, having a 7-cycle, is triply transitive. If L is of index 30 in A_9, then the subgroup of L fixing two letters has order 84; a group of order 84 has only one Sylow 7-subgroup. If L is of index 15, then the largest subgroup of L fixing two letters set-wise is of order 336; but a group of degree 7 and order divisible by 2^4 contains a transposition.

LEMMA 3. *If G is a transitive permutation group homomorphic onto K, and the kernel of the homomorphism is transitive on the letters permuted by G, then the subgroup of G fixing one letter is homomorphic onto K. Moreover, the two homomorphisms belong to the same many-to-one mapping.*

Proof. Let G_1 be the subgroup of G fixing the letter 1. For any $k \in K$, there exists $g_k \in G$ such that $g_k \to k$ in the homomorphism. Let i be the letter onto which 1 is mapped by g_k. Being transitive, the kernel has an element g'_k mapping i onto 1. Then $g_k g'_k$ maps 1 onto 1, and corresponds to k in the homomorphism. Since k is an arbitrary element of K, it follows that G_1 has an element corresponding to any element of K.

3. In this section will be established.

THEOREM 1. *If G is a quadruply transitive finite permutation*

group, H is the subgroup of G fixing four letters, P is a Sylow p-subgroup of H, P fixes $r \geqq 12$ letters and the normalizer in G of P has component A_r or S_r permuting the letters fixed by P, and P has no component of degree $\geqq p^3$ and no set of $r(r-1)/2$ permutation-isomorphic components, then G is alternating or symmetric

Proof. Let $N(P)$ be the normalizer in G of P. Each element of $N(P)$ maps any component of P onto a permutation-isomorphic component. Let P' be the largest subgroup of $N(P)$ fixing set-wise all components of P. P' is a normal subgroup of P. The components of P will be called *points*. $N^* = N(P)/P'$ is a permutation group on points.

By hypothesis all points are of degrees $\leqq p^2$. By Lemma 1 no transitive group of degree p or p^2 with a normal p-subgroup has a composition factor isomorphic with A_r, $r > 5$. By hypothesis $N(P)$ has component A_r or S_r on the $r \geqq 12$ letters fixed by P. Thus $N(P)$, or a subgroup thereof of index 2, is homomorphic with A_r. It follows that N^* has a composition factor of A_r, since P' has none.

N^* has a subgroup N with properties:

1. N has an element permuting the r letters fixed by P according to a, where a 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^*, having only finitely many subgroups, has a minimal subgroup with property 1. It is not asserted that N is unique.

By the minimality condition on N, each component of N is either a single point or is homomorphic with A_r, the image being represented on the letters fixed by P. Let J designate a component of N permuting more than one point (not letters fixed by P). J is homomorphic with A_r, with kernel J_0 the subgroup of J corresponding to the identity permutation of the letters fixed by P. Assume that the kernel J_0 is transitive on the points permuted by J. Then by Lemma 3 the subgroup of J fixing one point possesses the homomorphism onto A_r; this contradicts the minimality property of N. Thus each J has intransitive kernel.

For any J, the components of the kernel J_0 will be called *blocks*. Since J_0 is intransitive on the points permuted transitively by J, it follows that J permutes more than one block. In fact, J permutes blocks according to a group isomorphic with A_r, since J_0 is the kernel of the homomorphism of J onto A_r. By hypothesis P has no set of $r(r-1)/2$ permutation-isomorphic components; thus each J permutes fewer than $r(r-1)/2$ points, and *a fortiori* fewer than this number of blocks. By

Lemma 2 A_r for $r \geqq 9$ has no transitive permutation representation of degree strictly between r and $r(r-1)/2$ (by hypothesis $r \geqq 12$). 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 conjugations by elements of S_r. Thus there is a natural one-to-one correspondence between the letters fixed by P and the blocks permuted by any J such that each element of N permutes the sets alike.

Select a set of $s = [r/2]$ letters among the r fixed by P. Let N_0 be a minimal subgroup of N inducing all even permutations on these s letters. (That N_0 exists is argued as for N.) As each J is of degree $< r(r-1)/2$, each block contains fewer than $(r-1)/2$ points, hence fewer than s. The points of a block cannot be permuted according to any group homomorphic with A_s. By the minimality of N_0, each block fixed set-wise by N_0 is fixed point-wise by N_0. This is the case because N_0 has a composition factor of A_s, while the group permuting the points of one block has none.

N_0 is a group of permutations of points (transitive sets of P') and letters fixed by P. Thus N_0 determines a subgroup M of $N(P)$ such that $N_0 = M/P'$. M permutes the chosen set of s letters fixed by P according to A_s. Let M_0 be a minimal subgroup of M with this property. Each component of P' (point) is transitive of degree p or p^2 and has a normal p-subgroup. Hence by Lemma 1, no component of M_0 containing a single component of P' has a composition factor of A_s ($s > 5$, since $r \geqq 12$). Since M_0 is a minimal group homomorphic with A_s, each component of P' fixed set-wise by M_0 is fixed letter-wise by M_0. Thus each element of M_0 displaces at most $s/r \leqq 1/2$ of the letters of any component of $N(P)$; that is, at most half the letters displaced by P. M_0 has an element m displacing exactly three letters fixed by P. As $r \geqq 12$, m displaces at most half as many letters as the degree of G, diminished by 3. The theorem of Bochert [1] asserts that quadruply transitive G, with a non-identical element displacing so few letters as does m, is alternating or symmetric.

COROLLARY. *If G is a quadruply transitive permutation group of degree $n = kp + r$, with p prime, $k < p^2, k < r(r-1)/2, r \geqq 12$, 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 component A_r or S_r permuting 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 component of degree $\geqq p^3$. Since components of P are of degree at least p, the hypothesis $k < r(r-1)/2$ implies that P has no set of $r(r-1)/2$ permutation-isomorphic components. The hypothesis of Theorem

1 is fulfilled, so that G is A_n or S_n.

4. THEOREM 2. *If G is a quadruply transitive permutation group of degree n, and the subgroup of G fixing four letters is of order divisible by an odd prime p, with $5p > n - 4$, $4p \neq n - 4$, then G is A_n or S_n.*

Proof. Let H be the subgroup of G fixing four letters, and P be a Sylow p-subgroup of H. Since $5p > n - 4$, P is of degree $kp \leq 4p$.

If $kp = n - 4$, then $k \leq 3$, since $4p \neq n - 4$ by hypothesis. The theorem of Miller [6] applies with $n = kp + 4$ except for $k = p = 3$. However, $13 = 2 \cdot 5 + 3$, so that Miller's theorem is applicable to this case.

If $kp < n - 4$, then at least five letters are fixed by P. $N_G(P)$, the normalizer in G of P, has component T permuting the letters fixed by P quadruply transitive [5, Lemma 2.2]. A normal subgroup (not the identity) of a quadruply transitive group (other than S_4) is triply transitive [3, p. 198, Th. XI]. Thus T is primitive and has no regular normal subgroup, hence is unsolvable. The final subgroup in the commutator series of T is triply transitive.

P has at most four transitive sets, which cannot be permuted by an unsolvable group. If $p > 3$, then each component of P is of degree p and has a solvable holomorph. For $p = 3$, a component of degree 9 has a solvable automorphism group. Accordingly, the final member of the commutator series of $N_G(P)$ is a primitive group permuting only letters fixed by P. By Bochert's theorem [1], P is of degree at least $(n - 2)/2$, so that at most $(n + 2)/2$ letters are fixed by P. Hence G is at least $n + 1 - (n + 2)/2 = n/2 -$ ply transitive [3, p. 207, Th. I.] But G can be at most $(n + 3)/3 -$ ply transitive, or contains A_n. [4, p. 148, Th. VI.] The theorem is established for $n > 6$, and is trivial for the smaller degrees.

REFERENCES

1. Alfred Bochert, *Ueber die Classe der Transitiven Substitutionen-gruppen*, Math. Annalen **40** (1892), 176-193.
2. Robert Breusch, *Zur Verallgemeinerung des Bertrandschen Postulates, dass zwischen x und 2x stets Primzahlen liegen*, Math. Zeits., **34** (1932), 505-526.
3. W. Burnside, *Theory of Groups of Finite Order*, 2nd ed., Cambridge Univ. Press, 1911; reprinted Dover, New York, 1955.
4. Robert D. Carmichael, *Introduction to the Theory of Groups of Finite Order*, Ginn, New York, 1937.
5. Marshall Hall, Jr., *On a theorem of Jordan*, Pacific J. Math. **4** (1954), 219-226.
6. G. A. Miller, *Limits of the degree of transitivity of substitution groups*, Bull. Amer.

Math. Soc. **22** (1915), 68–71.   See also Marshall Hall, Jr., *The Theory of Groups*, Macmillan, New York, 1959, pp. 68–72.

7. J. Nagura, *On the interval containing at least one prime number*, Proc. Japan Acad. **28** (1952), 177–181.

REMINGTON RAND UNIVAC
DIVISION OF SPERRY RAND CORPORATION
ST. PAUL, MINNESOTA