On Non-Cayley Vertex-Transitive Graphs of Order a Product of Three Primes

Mohammad A. Iranmanesh\textsuperscript{1}

Department of Mathematics, University of Yazd, Yazd, Iran

and

Cheryl E. Praeger\textsuperscript{2}

Department of Mathematics and Statistics, University of Western Australia, Nedlands, Western Australia 6907, Australia

Received October 6, 1999

This paper completes the determination of all integers of the form $pqr$ (where $p$, $q$, and $r$ are distinct primes) for which there exists a vertex-transitive graph on $pqr$ vertices which is not a Cayley graph. © 2001 Academic Press

Key Words: Cayley graph; vertex-transitive graph.

1. INTRODUCTION

1.1. Background and Statement of Results

In 1983, Marušič [16] asked for a determination of the set $\mathcal{NC}$ of integers $n$ for which there exists a vertex-transitive graph on $n$ vertices which is not a Cayley graph. We call the elements of $\mathcal{NC}$ non-Cayley numbers. The purpose of this paper is to give necessary and sufficient conditions for a product of three distinct primes to be a non-Cayley number, thereby completing previous work of Gamble, Hassani, Miller, Seress, and the authors in [7, 10, 21, 24].

The set $\mathcal{NC}$ has the important, but elementary, property that if $n \in \mathcal{NC}$ then $kn \in \mathcal{NC}$ for every $k \in \mathbb{N}$, since if $\Gamma$ is a non-Cayley vertex-transitive graph of order $n$, then $k \cdot \Gamma$, the vertex-disjoint union of $k$ copies of $\Gamma$, is a non-Cayley vertex-transitive graph of order $kn$. The papers [14, 15], among other things, gave a complete determination of all non-Cayley numbers that are not square-free. Because of this, subsequent work has

\begin{itemize}
  \item[1.] The first author thanks the University of Yazd for partial financial support while carrying out the research for this paper.
  \item[2.] Research for this paper forms part of a project supported by an Australian Research Council grant of the second author.
\end{itemize}
aimed at finding the square-free non-Cayley numbers. For a positive integer $i$, we shall denote by $\mathcal{NC}_i$ the subset of $\mathcal{NC}$ consisting of non-Cayley numbers that are products of $i$ pairwise distinct primes. Now $\mathcal{NC}_1$ is empty, since every vertex-transitive graph of prime order admits a cyclic subgroup acting regularly on vertices and consequently is a Cayley graph. Also the set $\mathcal{NC}_2$ has been completely determined, see [15, Theorem 1], involving work in [2, 6] for the even case and in [1, 18, 19, 23] to characterise the odd numbers in $\mathcal{NC}_2$. We record this result below.

**Theorem 1.1** [1, 2, 6, 15, 18, 19, 23] (The $\mathcal{NC}_2$ Theorem). Let $p$ and $q$ be distinct primes with $p < q$. Then $pq \in \mathcal{NC}_2$ if and only if one of the following holds.

(i) $p^2$ divides $q - 1$.

(ii) $q = 2p - 1 > 3$ or $q = (p^2 + 1)/2$.

(iii) $q = 2^i + 1$, and $p$ divides $2^i - 1$ or $p = 2^i - 1 - 1$.

(iv) $q = 2^i - 1$ and $p = 2^i - 1 + 1$.

(v) $q = 11$ and $p = 7$.

The purpose of this paper is to complete the determination of the set $\mathcal{NC}_3$. From the observation above, for distinct primes $p$, $q$, $r$, if $pq \in \mathcal{NC}$ then automatically $pqr \in \mathcal{NC}$. Let $\mathcal{NC}_i^*$ denote the set of multiples of numbers in $\mathcal{NC}_i$. Thus the products $pqr$ for which membership of $\mathcal{NC}$ needs to be settled are those which lie in $\mathcal{NC}\setminus\mathcal{NC}_2^*$. In 1994, Miller and the second author [21] considered the question of membership of $2pq$ in $\mathcal{NC}$ (where $p$, $q$ are distinct odd primes). In the case where $2pq \not\in \mathcal{NC}_2^*$, the results of [21] provide precise conditions under which there exists a non-Cayley vertex-transitive graph of order $2pq$ which admits a transitive imprimitive subgroup of automorphisms. All other numbers $2pq \in \mathcal{NC}_3$ were determined by Gamble and the second author in [7] (that is, all extra integers of the form $2pq$ for which there exists a non-Cayley vertex-transitive graph of order $2pq$ such that every transitive subgroup of automorphisms is primitive).

**Theorem 1.2** [7, 21] (The $2pq$ Theorem). Let $p$ and $q$ be odd primes with $p < q$.

(a) Then $2pq \in \mathcal{NC}_2^*$ if and only if one of the following holds:

(i) $p \equiv 1 \pmod{4}$ or $q \equiv 1 \pmod{4}$,

(ii) $q \equiv 1 \pmod{p^2}$,

(iii) $q = 11$, $p = 7$. 


Moreover, \(2pq \in \mathcal{NC}_3 \setminus \mathcal{NC}_2\) if and only if \(p \equiv q \equiv 3 \pmod{4}\), and one of the following holds:

(i) \(q \equiv 1 \pmod{p}\) and \(q \not\equiv 1 \pmod{p^2}\),
(ii) \(p = (q + 1)/4\),
(iii) \(q = 19\), \(p = 7\).

In [24] Seress began an investigation of the question of membership of \(pqr\) in \(\mathcal{NC}\) where \(p, q, r\) are distinct odd primes. For \(pqr \notin \mathcal{NC}_2\), he determined precisely when there exists a vertex-primitive non-Cayley graph of order \(pqr\), and, building on work of Marušič, Scapellato, and Zgrablić [20], he determined when there exists a non-Cayley vertex-transitive graph \(\Gamma\) of order \(pqr\) for which \(\text{Aut}(\Gamma)\) is quasiprimitive on vertices (that is, every non-trivial normal subgroup of \(\text{Aut}(\Gamma)\) is transitive on vertices). Thus the problem remaining, following the work of Seress, is that of determining any extra orders \(pqr\) for non-Cayley vertex-transitive graphs \(\Gamma\) such that \(\text{Aut}(\Gamma)\) has a non-trivial intransitive normal subgroup. The paper of Seress also contains a construction [24, Section 2] of an infinite family of graphs of this type which generalises a construction given in [21, Construction 2.1] for graphs of order \(2pq\). Thus, by a series of constructions of non-Cayley vertex-transitive graphs, Seress [24, Theorem 1.2] proved that each number in the subset \(\mathcal{T}\) defined below is a member of \(\mathcal{NC}_3\). In Table I for an integer \(n\) and a prime \(p\), we use \(n_p\) to denote the largest power of \(p\) dividing \(n\), that is to say, \(n_p\) is the \(p\)-part on \(n\).

**Definition 1.3 (The set \(\mathcal{T}\)).** Let \(p, q, r\) be distinct odd primes such that \(pqr \notin \mathcal{NC}_2\). Then \(pqr \in \mathcal{T}\) if and only if one of the following holds.

(i) \(pqr = (2^t + 1)(2^{2^t + 1} + 1)\), for some \(t\), or \(pqr = (2^d + 1)(2^d - 1)\), for some prime \(d\);
(ii) re-ordering \([p, q, r]\) if necessary, we have \(pq\) equal to (a) \(2r + 1\), (b) \((r + 1)/2\), (c) \((r^2 + 1)/2\), (d) \((r^2 - 1)/24x\) where \(x = 1, 2, 5\), or (e) \(2^i + 1\), where \(r\) divides \(2^i - 1\) for some \(i\);
(iii) re-ordering \([p, q, r]\) if necessary, \(p < q < r\) and \(p, q, r\) are as in one of the lines of Table I.

We prove in this paper that there are no more integers in \(\mathcal{NC}_3\). To do this we use the results mentioned above, and we also use a sufficient condition given in [10, Theorem 1.1] for a vertex-transitive graph of order \(pqr\) to be a Cayley graph. Thus the main result of this paper is the following theorem.
TABLE I

<table>
<thead>
<tr>
<th>( p )</th>
<th>( q )</th>
<th>( r )</th>
<th>Conditions or comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>( p )</td>
<td>( \frac{3p+1}{2} )</td>
<td>( \frac{3p+2}{2} )</td>
<td>((q-1)_p = p ) and ((r-1)_q = q)</td>
</tr>
<tr>
<td>( p )</td>
<td>( 6p-1 )</td>
<td>( 6p+1 )</td>
<td></td>
</tr>
<tr>
<td>( p )</td>
<td>( \frac{r-1}{2} )</td>
<td>( \frac{r}{2} )</td>
<td>( p ) divides ((r+1)), possibly (p &gt; q) if ( p = \frac{r+1}{2})</td>
</tr>
<tr>
<td>( \frac{k^{2}+1}{k+1} )</td>
<td>( \frac{k^{2}-1}{k-1} )</td>
<td>( \frac{k^{d-1}-1}{k-1} )</td>
<td>( k, d \text{ all prime} )</td>
</tr>
<tr>
<td>( \frac{k^{d-1}+1}{k+1} )</td>
<td>( \frac{k^{d-1}-1}{k-1} )</td>
<td>( \frac{k^{d}-1}{k-1} )</td>
<td>( k, d \text{ all prime})</td>
</tr>
<tr>
<td>( \frac{k^{2}+1}{3} )</td>
<td>( \frac{k^{2}-1}{k-1} )</td>
<td>( \frac{k^{d}-1}{k-1} )</td>
<td>( k ) prime</td>
</tr>
<tr>
<td>( 2d+1 )</td>
<td>( 2d-1 )</td>
<td>( 2d-1 )</td>
<td>( d ) prime</td>
</tr>
<tr>
<td>( 3 )</td>
<td>( 2d+1 \times 2 )</td>
<td>( 2d+1 )</td>
<td>( d = 2^t+1, d ) prime</td>
</tr>
<tr>
<td>5</td>
<td>11</td>
<td>19</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>73</td>
<td>257</td>
<td></td>
</tr>
</tbody>
</table>

**Theorem 1.4 (The Main Theorem).** Let \( p, q, r \) be distinct odd primes such that \( pqr \notin \mathcal{N}_3 \cup \mathcal{S} \). Then every vertex-transitive graph of order \( pqr \) is a Cayley graph.

The following theorem summarises the results discussed above and gives a determination of \( \mathcal{N}_3 \cup \mathcal{S} \). (It follows immediately from the results above.)

**Theorem 1.5 (The \( \mathcal{N}_3 \cup \mathcal{S} \) Theorem).** Let \( p, q, r \) be primes such that \( 2 < p < q < r \). Then \( pqr \notin \mathcal{N}_3 \cup \mathcal{S} \) if and only if one of the following holds.

(i) \( q \equiv 1 \pmod{p^2} \), or \( r \equiv 1 \pmod{p^2} \), or \( q \equiv 1 \pmod{q^2} \);

(ii) for some odd \( s \in \{p, q, r\} \), either \( 2s - 1 \) or \( (s^2 + 1)/2 \) also belongs to \( \{p, q, r\} \);

(iii) \( \{p, q, r\} \) contains \( 2^t+1 \) and also contains either \( 2^{t-1} - 1 \) or a divisor of \( 2^t-1 \), for some \( t \);

(iv) \( \{p, q, r\} \) contains \( 2^t-1 \) and \( 2^{t-1} + 1 \), for some \( t \);

(v) \( 7, 11 \notin \{p, q, r\} \).
Moreover, \( pqr \in \mathcal{N}\mathcal{C}_3 \) if and only if either \( pqr \not\in \mathcal{N}\mathcal{C}_\mathbb{Z} \) or \( p, q, r \) satisfy one of the parts of Definition 1.3 (where \( p \) may be 2 in Definition 1.3(ii)(b) or in line 1 of Table 1) or \( (p, q, r) = (2, 7, 19) \).

The major unresolved question concerning non-Cayley numbers is the following.

**Question 1** [15, Question, p. 334]. Is there a number \( k > 0 \) such that every product of \( k \) distinct primes is in \( \mathcal{N}\mathcal{C} \)?

It was known in [15] that such a number \( k \) must be at least 4, since 138 = 2 \cdot 3 \cdot 23 was known not to lie in \( \mathcal{N}\mathcal{C} \). Although the results of this paper do not increase our knowledge of the size that such a \( k \) must be, by providing complete information on the membership of \( \mathcal{N}\mathcal{C}_3 \) they may assist future attempts to answer this question.

In Section 2 we introduce the notation and concepts needed for the proof of Theorem 1.4 and outline the strategy to be used in the proof. Next, in Section 3, we examine quasiprimitive permutation groups of degree \( pq \), where \( p \) and \( q \) are distinct odd primes, and classify those which are minimal transitive with degree \( pq \not\in \mathcal{N}\mathcal{C} \) (see Theorem 3.4). This information is needed for the proof of Theorem 1.4. (A transitive permutation group is said to be **minimal transitive** if all its proper subgroups are intransitive.) In Section 4 we begin the analysis of a minimal counter-example to Theorem 1.4 and prove in Proposition 4.1 that a minimal vertex-transitive subgroup of automorphisms has an intransitive normal subgroup of prime index. The proof of Theorem 1.4 is completed in Section 5.

2. NOTATION AND THE STRUCTURE OF THE PAPER

We first introduce some concepts and notation concerning graphs and group actions and then explain the structure of the analysis for completing the investigation and proving Theorem 1.4.

2.1. Notation: Graphs

For a graph \( I = (V, E) \) with vertex set \( V \) and edge set \( E \), we denote by \( \text{Aut}(I) \) the automorphism group of \( I \). The cardinality of \( V \) is called the **order** of \( I \). We say that \( I \) is *vertex-transitive* if \( \text{Aut}(I) \) acts transitively on \( V \). For a group \( G \), and a subset \( S \) of \( G \) such that \( 1_G \not\in S \) and \( S = S^{-1} \), the **Cayley graph** \( \text{Cay}(G, S) \) of \( G \) relative to \( S \) is defined as the graph \( (G, E(S)) \) where \( E(S) \) consists of those pairs \( \{x, y\} \) from \( G \) for which \( xy^{-1} \in S \) (and hence also \( yx^{-1} \in S \) since \( S = S^{-1} \)). All Cayley graphs \( \text{Cay}(G, S) \) for \( G \) admit the group \( G \), acting by right multiplication, as a subgroup of automorphisms, and this action of \( G \) is **regular** on vertices, that is, \( G \) is transitive.
on vertices and only the identity element of \( G \) fixes a vertex. Thus, identifying \( G \) with this subgroup of automorphisms, we have \( G \leqslant \text{Aut}(\text{Cay}(G, S)) \). In particular each Cayley graph is vertex-transitive. Moreover, a vertex-transitive graph \( \Gamma \) is a Cayley graph for some group if and only if \( \text{Aut}(\Gamma) \) contains a subgroup which is regular on vertices. The focus of this paper is on the existence of vertex-transitive graphs which are not Cayley graphs, that is, which have no regular subgroups of automorphisms.

We need to use several graph theoretic constructions in the proof. These are defined as follows. The lexicographic product \( \Gamma_1[\Gamma_2] \) of \( \Gamma_1 = (V_1, E_1) \) has vertex set \( V_1 \times V_2 \), and two vertices \((\alpha_1, \beta_1) \) and \((\alpha_2, \beta_2) \) are adjacent if and only if either \( \{\alpha_1, \alpha_2\} \in E_1 \) or \( \alpha_1 = \alpha_2 \) and \( \beta_1 = \beta_2 \). Now we consider a graph \( \Gamma = (V, E) \). For a subset \( D \) of the vertex set \( V \), the induced subgraph \( \overline{D} \) on \( D \) is the graph with vertex set \( D \) and edge set consisting of all the pairs in \( E \) with both vertices in \( D \). For a partition \( \Sigma \) of \( V \) the quotient graph \( \Gamma / \Sigma \) of \( \Gamma \) relative to \( \Sigma \) is the graph with vertex set \( \Sigma \) and \( ([B, B'] \in \Sigma \) if and only if there exists \( \alpha \in B \) and \( \alpha' \in B' \) such that \( \{\alpha, \alpha'\} \in E \). Finally, two disjoint subsets \( B, B' \) of \( V \) are said to be trivially joined if either (a) there are no edges of \( \Gamma \) consisting of a vertex of \( B \) and a vertex of \( B' \), or (b) \( \{\alpha, \alpha'\} \in E \) for all \( \alpha \in B \) and all \( \alpha' \in B' \).

2.2. Notation: Group Actions

For a group \( G \) acting on a set \( V \) and a \( G \)-invariant subset \( U \) of \( V \), we denote by \( G^U \) the group of permutations of \( U \) induced by \( G \). The normal subgroup of \( G \) consisting of the elements of \( G \) which fix every point of \( V \) is called the kernel of the action, and \( G \) is said to be faithful or unfaithful on \( V \) as the kernel is trivial or non-trivial, respectively. We say that a partition \( \Sigma \) of \( V \) is \( G \)-invariant if \( G \) permutes the blocks of \( \Sigma \), that is, for \( B \in \Sigma \) and \( g \in G \), the image \( B^g = \{x^g \mid a \in B\} \) is also a block of \( \Sigma \). If \( G \) is transitive on \( V \) and \( \Sigma \) is a \( G \)-invariant partition of \( V \), then \( G \) induces a transitive action on \( \Sigma \) and consequently all the blocks of \( \Sigma \) have the same cardinality. If either all blocks of \( \Sigma \) are singletons, or \( \Sigma \) consists of the single block \( V \), then \( \Sigma \) is said to be trivial, and all other partitions are called non-trivial. A transitive action of \( G \) on \( V \) is said to be imprimitive if there exists a non-trivial \( G \)-invariant partition of \( V \), and otherwise \( G \) is said to be primitive. A natural way in which \( G \)-invariant partitions arise for transitive groups \( G \) on \( V \) is as the set of orbits of a normal subgroup of \( G \). Such partitions are always \( G \)-invariant. However there are many examples of imprimitive actions of a group \( G \) for which no non-trivial \( G \)-invariant partition arises in this way. Such a group action is said to be quasiprimitive: that is, \( G \) is quasiprimitive on \( V \) if every normal subgroup of \( G \) not contained in the kernel is transitive on \( V \).
2.3. Structure of the Proof of Theorem 1.4.

We need to prove that there are no non-Cayley vertex-transitive graphs $\Gamma$ of order $pq\ell$ such that $pq\ell \notin \mathcal{N} \cup \mathcal{S}$. Suppose to the contrary that $\Gamma$ is such a graph. From our discussion in Section 1, $\text{Aut}(\Gamma)$ is transitive but not quasiprimitive on vertices. The main result of [10] gives us important additional information about a minimal transitive subgroup of $\text{Aut}(\Gamma)$. We explain this below.

The construction of Seress [24, Section 2] of a family of imprimitive vertex-transitive graphs of order $pq\ell$ produces graphs $\Gamma$ for which $\text{Aut}(\Gamma)$ has a sequence of normal subgroups, $1 < N < K < \text{Aut}(\Gamma)$ with $N$, $K$ intransitive on vertices, the $N$-orbits being proper subsets of the $K$-orbits. (For these graphs, $pq\ell$ is as in line 1 of Table I, and in particular $pq\ell \notin \mathcal{S}$.) It turns out that this property of $\text{Aut}(\Gamma)$ is important.

**Definition 2.1.** A transitive action of a group $G$ on a set $V$ is said to be genuinely $3$-step imprimitive if $G$ has a sequence of normal subgroups, $1 < N < K < G$, such that $N$ and $K$ are intransitive and non-trivial on $V$ and the $N$-orbits in $V$ are proper subsets of the $K$-orbits. This terminology reflects the fact that the lattice of $G$-invariant partitions of $V$ contains a chain of length $3$ corresponding to the chain $1 < N < K < G$ of normal subgroups of $G$.

In [10], a very delicate analysis of vertex-transitive graphs $\Gamma$ of order $pq\ell \notin \mathcal{N} \cup \mathcal{S}$ such that $\text{Aut}(\Gamma)$ has a genuinely $3$-step imprimitive subgroup showed that all such graphs are Cayley graphs. Thus, for a non-Cayley vertex-transitive graph $\Gamma$ of order $pq\ell$, where $pq\ell \notin \mathcal{N} \cup \mathcal{S}$, $\text{Aut}(\Gamma)$ is not quasiprimitive and has no genuinely $3$-step imprimitive subgroup. Our strategy for investigating $\Gamma$ is to choose a subgroup $G$ of $\text{Aut}(\Gamma)$ which is transitive but not quasiprimitive on the vertex set $V$ and is minimal (by inclusion) subject to this condition. Since $\Gamma$ is not a Cayley graph, $G$ is not regular on $V$, and since $G$ is not quasiprimitive on $V$, there exists a non-trivial intransitive normal subgroup $K$ of $G$. The number of $K$-orbits may be either a prime or a product of two primes, dividing $pq\ell$. Let $\Sigma$ denote the $G$-invariant partition of $V$ consisting of the $K$-orbits.

A major part of the paper is devoted to proving that $K$ may be chosen in such a way that $|\Sigma|$ is prime and is equal to $|G : K|$, This is Proposition 4.1 which is proved in Section 4. Its proof requires detailed information about quasiprimitive permutation groups of degree $pq$, a product of the two distinct odd primes $p$ and $q$, and this information is derived in Section 3. A classification of quasiprimitive permutation groups of degree $pq$ is available, see [13, 23, 26], and depends on the finite simple group classification. We work with this classification, specifying which of the degrees lie in $\mathcal{N}$, and which of the groups are minimal transitive. Section 5 contains an analysis...
of the final case in which \(|G : K|\) is prime and there is no normal subgroup of \(G\), contained in \(K\), with orbits of prime length. We show that there are no non-Cayley graphs with this property.

3. QUASIPRIMITIVE PERMUTATION GROUPS OF DEGREE \(pq\)

Let \(p, q\) be distinct odd primes and let \(G\) be a quasiprimitive permutation group on a set \(V\) of cardinality \(pq\). By definition this means that \(G \leq \text{Sym}(V) = S_{pq}\) and all nontrivial normal subgroups of \(G\) are transitive on \(V\). Some of these groups will be primitive on \(V\), while others will be imprimitive. The latter groups are called \textit{imprimitive quasiprimitive permutation groups} of degree \(pq\). It follows from the O’Nan–Scott theorem for quasiprimitive groups [22] that \(G\) is \textit{almost simple}, that is, \(G\) has a unique minimal normal subgroup which is a nonabelian simple group and \(T \leq G \leq \text{Aut}(T)\). As we shall discuss in detail in this section, all such groups have been classified, and their classification depends on the finite simple group classification. We shall need some detailed information about these groups. For example we shall need to know, for each such group, whether or not the socle \(T\) is minimal transitive and also whether or not \(pq \notin \mathcal{NC}\). We derive this information below in a series of three propositions.

Most of the information about the groups is contained in Tables II–IV below. In the columns of these tables headed “\(\mathcal{NC}\)” an entry “yes” or “no” means that \(pq\) is or is not in \(\mathcal{NC}\), respectively, while an entry “?” denotes that for some, but not all, values of \(pq\) corresponding to that line of the table we have \(pq \notin \mathcal{NC}\). In the columns headed “min.trans.”, an entry “?” means that for some but not all groups in that line \(T\) may be minimal transitive, an entry “intrans” means that \(T\) is not even transitive, and an entry which is the name of a group, for example the Frobenius group \(F_{pq}\) of order \(pq\), means that \(T\) has a transitive subgroup isomorphic to this group.

First we consider those groups \(G\) which act faithfully on a nontrivial \(G\)-invariant partition \(\Sigma\), so that \(G\) is isomorphic to a transitive permutation group of degree \(|\Sigma|\). Then as both \(p\) and \(q\) divide \(|G|\), it follows that \(|\Sigma|\) is equal to the larger of \(p\) and \(q\), say \(p\). Also a stabiliser in \(G\) of a point of \(V\) is a subgroup of index \(q\) in the stabiliser of an element of \(\Sigma\). Note that the socle \(T\) is transitive on \(V\) since \(G\) quasiprimitive.

**Proposition 3.1 (The imprimitive case).** Let \(p, q\) be distinct odd primes such that \(q < p\). Suppose that \(G \leq S_p\) and that \(G\) is a transitive permutation group of degree \(p\) with socle \(T\) such that a point stabiliser \(H\) in this action has a subgroup \(L\) of index \(q\). Then
(a) $G$ acting by right multiplication on the set $[G:L]$ of right cosets of $L$ is a transitive permutation group of degree $pq$ which acts faithfully on a non-trivial $G$-invariant partition, and all possibilities for $T$, $p$, $q$ are given in Table II.

(b) Moreover, $G$ is quasiprimitive on $[G:L]$ if and only if $|H \cap T : L \cap T| = q$, and all imprimitive quasiprimitive permutation groups of degree $pq$ arise in this way. The examples are precisely the groups in lines 3–7 of Table II.

Table II also contains information on whether $pq \in \mathcal{N} \mathcal{C}$ and whether $T$ is minimal transitive on $[G:L]$.

**Proof.** By an old result of Burnside [11, Satz 21.3, 3.6], either $G$ is a subgroup of $AGL(1,p)$ or $T$ is a nonabelian simple group. In the former case $T = Z_p$ and $q$ divides $p - 1$, so $H \cap T = 1$ and the condition $|H \cap T : L \cap T| = q$ cannot hold; also $pq$ lies in $\mathcal{N} \mathcal{C}$ in this case for some, but not all, values of $p$, $q$ (see Theorem 1.1). Assume now that $T$ is a nonabelian simple group. The condition $|H \cap T : L \cap T| = q$ is equivalent to the condition that $T$ is transitive on $V := [G:L]$, and this is equivalent to the condition that $G$ is quasiprimitive on $V$.

Conversely, if $G$ is transitive of degree $pq$ and $G$ acts faithfully on a non-trivial partition $\Sigma$, then as we noted above, $|\Sigma|$ is equal to the larger of $p$ and $q$, namely $p$, and $G$ in its action on $\Sigma$ is a transitive permutation group of degree $p$. The stabiliser $H$ in $G$ of a block $B$ in $\Sigma$ has a subgroup $L$ of index $q$, namely the stabiliser of a point of $B$. Moreover, $G$ is quasiprimitive.

### Table II

<table>
<thead>
<tr>
<th>$T$</th>
<th>$p$</th>
<th>$q$</th>
<th>$L \cap T$</th>
<th>$\mathcal{N} \mathcal{C}$</th>
<th>Min. trans.</th>
</tr>
</thead>
<tbody>
<tr>
<td>$Z_p$</td>
<td>-</td>
<td>$q \mid (p - 1)$</td>
<td>1</td>
<td>?</td>
<td>intrans.</td>
</tr>
<tr>
<td>$PSL(n,s)$</td>
<td>$s^a - 1$</td>
<td>$q \mid \gcd(s-1, GL(n-1,s))$</td>
<td>?</td>
<td>intrans.</td>
<td></td>
</tr>
<tr>
<td>$s = s_p$</td>
<td>prime $(n, s - 1)$</td>
<td>$NC(Z_p)$</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$PSL(n,s)$</td>
<td>$s^a - 1$</td>
<td>$q \mid (s - 1)$</td>
<td>contains</td>
<td>?</td>
<td>?</td>
</tr>
<tr>
<td>$PSL(3,2)$</td>
<td>7</td>
<td>3</td>
<td>$D_6$</td>
<td>no</td>
<td>$F_{14}$</td>
</tr>
<tr>
<td>$PSL(3,3)$</td>
<td>13</td>
<td>3</td>
<td>$[3^2 : [16]]$</td>
<td>no</td>
<td>$F_{19}$</td>
</tr>
<tr>
<td>$PSL(2,11)$</td>
<td>11</td>
<td>5</td>
<td>$A_4$</td>
<td>no</td>
<td>$F_{15}$</td>
</tr>
</tbody>
</table>
of degree $pq$ if and only if $T$ is transitive, that is, $|H \cap T : L \cap T| = q$, and in this case $T$ is a nonabelian simple group.

The list of possibilities for the socle $T$ of an almost simple group of degree $p$ is given, for example, in [9] and is the following: (i) $A_p$, (ii) $PSL(n, s)$ with $p = (s^n - 1)/(s - 1)$ with $n$ prime and $(n, s) \neq (2, 2)$ or $(2, 3)$, (iii) $M_{11}$ or $PSL(2, 11)$ with $p = 11$, or (iv) $M_{23}$ with $p = 23$. In case (i), the group $H \cap T = A_{p-1}$ has no subgroup of odd index $q$ unless $p = 5$, $q = 3$, and this occurs in line 3 of the table since $A_5 \cong PSL(2, 4)$. Note that $15 \in \mathcal{N}^C_{p}$ and $A_5$ is minimal transitive.

Suppose now that (ii) holds with $s = s_o^a$ for a prime $s_o$. In this case $H \cap T$ is equal to $[s^{s_o^a-1}] GL(n - 1, s)$. If $L$ contains $H \cap T$ then $T$ is intransitive and $q = |H : L|$ divides $|H : H \cap T| = [G : T]$ which divides $a \cdot \gcd(n, s - 1)$, as in line 2 of the table. In this case, $L \cap T = H \cap T$ so $|G : LT| = [HT : LT] = |H : L| = q$. If $P$ is a Sylow $p$-subgroup of $T$ then $G = N_G(P) T$, and it follows that $N_G(P)$ is transitive on $V$ so $G$ is not minimal transitive. We now suppose that $T$ is transitive, that is, $|H \cap T : L \cap T| = q$. If $n = 2$ then $p = s + 1$ so $s_o = 2$ and the only odd primes dividing $|H \cap T|$ are divisors of $s - 1$ as in line 3 of the table; in this case $pq \in \mathcal{N}^C_{p}$ and $T$ is minimal transitive (but $T$ is not always minimal transitive in line 3 when $n$ is at least 3).

Suppose now that $n \geq 3$. If $(n, s) = (3, 2)$ then $p = 7$, $q = 3$ as in line 4, and a Frobenius subgroup $F_{23}$ of order 21 is transitive on $V$. If $(n, s) = (3, 3)$ then $p = 13$, $q = 3$ as in line 5, and a Frobenius subgroup $F_{39}$ of order 39 is transitive on $V$. (This can be seen from the Atlas [4, p. 13]; $F_{39}$ contains no 3A-elements whereas a Sylow 3-subgroup of $L = [3^2] \cdot [16]$ contains only 3A-elements whence $F_{39} \cap L = 1$, that is, $F_{39}$ is transitive on $V$.) If $(n, s) = (3, 5)$ then $p = 31$, $q = 5$ as in line 6, and in this case $T$ is minimal transitive.

Suppose now that when $n = 3, s$ is not 2, 3, or 5. Then $H = [s^{s_o^a} - 1]$. $GL(n - 1, s)$ involves the nonabelian simple group $PSL(n - 1, s)$. If $L$ also involves $PSL(n - 1, s)$ then, since $SL(n - 1, s)$ acts irreducibly on the elementary abelian normal subgroup $[s^{s_o^a} - 1]$ of $H$, it follows that $q$ divides $s - 1$ as in line 3 of the table. If this is not the case then $PSL(n - 1, s)$ has a subgroup of prime index $q$. By [9] again, $q$ is one of $(s^{s_o^a} - 1)/(s - 1)$, 7 (with $n = 3$, $s = 7$), or 11 (with $n = 3$, $s = 11$). If both $p = (s^{s_o^a} - 1)/(s - 1)$ and $q = (s^{s_o^a} - 1)/(s - 1)$ are prime, then $n = 3$, $s = 2^{3n}$, $q = s + 1 \geq 3$, and $p = s^2 + s + 1 = 0$ (mod 3), which is a contradiction. In the other two cases, $p = 57$ or 133, neither of which is prime.

Of the groups in cases (iii) and (iv), the only one for which $H$ has a subgroup of odd prime index is $PSL(2, 11)$ where $p = 11$, $q = 5$, and a Frobenius group $F_{23}$ is transitive on $V$ as in line 8 of the table.

We need to deal with the primitive groups of degree $pq$. First we consider those which are 2-transitive.
Proposition 3.2 (The 2-transitive case). Let \( p, q \) be distinct odd primes such that \( q < p \). Suppose that \( G \leq S_{pq} \) and that \( G \) is a 2-transitive permutation group of degree \( pq \) with socle \( T \). Then \( T \) is a nonabelian simple group and Table III contains all the possibilities for \( T, p, q \), together with some information on whether \( pq \in \mathcal{N} \mathcal{C} \) and whether \( T \) is minimal transitive.

Proof. As in our discussion above \( T \) is a nonabelian simple group, and all possibilities for the socles of almost simple 2-transitive groups are given, for example, in [3] and are as follows: those recorded in lines 1–3 and 5 of Table III (and for these groups deriving the values of \( p, q \) is straightforward) together with several families and individual groups of even degree or prime degree, and the groups \( Sz(s) \) with \( s = 2^{3^a+1} = r^2/2 \geq 8 \) so \( pq = s^2 + 1 = (s + r + 1)(s - r + 1) \). In this last case, 5 divides \( s^2 + 1 \) and hence \( q = 5 = s - r + 1 < p = s + r + 1 \), so \( s = 8 \) and \( p = 13 \) as in line 4. The information about membership of \( pq \) in \( \mathcal{N} \mathcal{C} \) is obtained from Theorem 1.1.

Finally we deal with the primitive permutation groups of degree \( pq \) which are not 2-transitive, that is, the simply primitive groups of degree \( pq \). A classification of these can be derived from [13]; see [23].

Proposition 3.3 (The simply primitive case). Let \( p \) and \( q \) be distinct odd primes such that \( q < p \). Suppose that \( G \leq S_{pq} \) and that \( G \) is a simply primitive permutation group of degree \( pq \) with socle \( T \). Then \( T \) is a nonabelian simple group and Table IV contains all the possibilities for \( T, p, q \), together with some information on whether \( pq \in \mathcal{N} \mathcal{C} \) and whether \( T \) is minimal transitive. In particular, if \( pq \notin \mathcal{N} \mathcal{C} \) then \( T \) is not minimal transitive.

<table>
<thead>
<tr>
<th>( T )</th>
<th>2-Transitive Groups of Degree ( pq )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( A_{pq} )</td>
<td>( p ) ( q ) ( ? ) ( Z_{pq} )</td>
</tr>
<tr>
<td>( \text{PSL}(n, s) )</td>
<td>( p ) ( \frac{s^n - 1}{p(s - 1)} ) ( ? ) ( Z_{pq} )</td>
</tr>
<tr>
<td>( \text{PSU}(3, 2^a) )</td>
<td>( 2^{3^a} - 2^a + 1 ) ( 2^a + 1 &gt; 3 ) no, except for ( a = 2 ) ( ? )</td>
</tr>
<tr>
<td>( Sz(8) )</td>
<td>13 5 yes yes</td>
</tr>
<tr>
<td>( A_7 )</td>
<td>5 3 no ( A_6 )</td>
</tr>
</tbody>
</table>

TABLE III
Simply Primitive Permutation Groups of Degree $pq$

<table>
<thead>
<tr>
<th>$T$</th>
<th>$p$</th>
<th>$q$</th>
<th>Action</th>
<th>$\psi \sigma$</th>
<th>Min. trans.</th>
</tr>
</thead>
<tbody>
<tr>
<td>$A_p$</td>
<td>$p \geq 5$</td>
<td>$\frac{p-1}{2}$</td>
<td>pairs</td>
<td>no</td>
<td>$F_{pq}$</td>
</tr>
<tr>
<td>$A_{p+1}$</td>
<td>$p \geq 5$</td>
<td>$\frac{p+1}{2}$</td>
<td>pairs</td>
<td>yes</td>
<td>$PSL(2, p)$</td>
</tr>
<tr>
<td>$A_7$</td>
<td>7</td>
<td>5</td>
<td>triples</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>$PSL(4, 2)$</td>
<td>7</td>
<td>5</td>
<td>2-spaces</td>
<td>yes</td>
<td>$A_7$</td>
</tr>
<tr>
<td>$PSL(5, 2)$</td>
<td>31</td>
<td>5</td>
<td>2-spaces</td>
<td>no</td>
<td>$F_{pq}$</td>
</tr>
<tr>
<td>$PSp(4, 2^a)$</td>
<td>$2^a+1$</td>
<td>$2^a+1$</td>
<td>1-spaces</td>
<td>yes</td>
<td>$PSL(2, 2^a)$</td>
</tr>
<tr>
<td>$D^{+}(2n, 2)$</td>
<td>$2^{n-1}+1$</td>
<td>$2^{n-1}+1$</td>
<td>sing. 1-spaces</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>$PSL(2, p)$</td>
<td>$p \geq 13$</td>
<td>$\frac{p+1}{2}$</td>
<td>cosets of $D_{p+1}$</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>$PSL(2, q^2)$</td>
<td>$q^2+1$</td>
<td>$q^2+1$</td>
<td>cosets of $PGL(2, q)$</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>$PSL(2, 19)$</td>
<td>19</td>
<td>3</td>
<td>cosets of $A_5$</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>$PSL(2, 29)$</td>
<td>29</td>
<td>7</td>
<td>cosets of $A_5$</td>
<td>no</td>
<td>$F_{pq}$</td>
</tr>
<tr>
<td>$PSL(2, 59)$</td>
<td>59</td>
<td>29</td>
<td>cosets of $A_5$</td>
<td>no</td>
<td>$F_{pq}$</td>
</tr>
<tr>
<td>$PSL(2, 61)$</td>
<td>61</td>
<td>31</td>
<td>cosets of $A_5$</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>$PSL(2, 23)$</td>
<td>23</td>
<td>11</td>
<td>cosets of $S_4$</td>
<td>no</td>
<td>$F_{pq}$</td>
</tr>
<tr>
<td>$PSL(2, 11)$</td>
<td>11</td>
<td>5</td>
<td>cosets of $A_4$</td>
<td>no</td>
<td>$F_{pq}$</td>
</tr>
<tr>
<td>$PSL(2, 13)$</td>
<td>13</td>
<td>7</td>
<td>cosets of $A_4$</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>$M_{23}$</td>
<td>23</td>
<td>11</td>
<td>no</td>
<td></td>
<td>$F_{pq}$</td>
</tr>
<tr>
<td>$M_{22}$</td>
<td>11</td>
<td>7</td>
<td>no</td>
<td></td>
<td>$F_{pq}$</td>
</tr>
<tr>
<td>$M_{11}$</td>
<td>11</td>
<td>5</td>
<td>no</td>
<td></td>
<td>$F_{pq}$</td>
</tr>
</tbody>
</table>

**Proof.** As in our discussion above $T$ is a nonabelian simple group, and all possibilities for the socles of simply primitive groups of degree $pq$ are given, for example, in [23] or [20] based on [13]. (Note the omission of $PSL(2, 13)$ from the list in [23].)

Suppose that there is a proper transitive subgroup $L$ of $T$. If $L$ is primitive then $L$ is almost simple and $soc(L)$ is transitive, so we may assume that $L = soc(L)$. Then $L$ also must be one of the simple groups listed in Table IV, so we check this. (Often all we need to do is to check the values of $p$ and $q$.) For example for $T$ in line 2 we see that $L$ in line 8 is a proper transitive subgroup, and the group $T$ in line 4 contains the group $L$ in line 3 as a transitive proper subgroup. So suppose now that $L$
is imprimitive and that $L$ preserves a nontrivial block system $\Sigma$. If $L$ acts faithfully on $\Sigma$ then $\Sigma$ consists of $p$ blocks of size $q$, and $L$ is listed in Table II. This identifies the transitive subgroup $\text{PSL}(2, 2^a)$ of $T = \text{PSp}(4, 2^a)$ and also many of the examples for which a Frobenius subgroup $L$ of order $pq$ is transitive. In particular, the cases where $T = \text{PSL}(2, p)$ may be dealt with by referring to the classification of subgroups of these groups due to Dickson [5], and the groups $T = A_5$, $\text{PSL}(5, 2)$, $M_{23}$ may be dealt with by referring to the Atlas [4]. This leaves one family of groups, namely, $T = \Omega(2n, 2)$, where $v = \pm$, and we note that, because of the values of $p$ and $q$, we have $(2n, v) \neq (8, +), (10, -)$, and if $v = -$ then $n$ must be even. In this case we have a factorisation $T = LP_1$ where $P_1$ is the stabiliser of a singular 1-space. However, by [12], there are no such factorisations.

There are two consequences of these propositions which are important for our work, and we record them below.

**Theorem 3.4.** Let $p$, $q$ be distinct odd primes such that $q < p$ and $pq \notin \mathbb{N} \setminus \mathcal{C}$, and let $T$ be a nonabelian simple group. Then $T$ can be represented as a minimal transitive permutation group on a set $V$ of cardinality $pq$ if and only if one of the following holds.

(i) $T = \text{PSU}(3, 2^a)$, $p = 2^{2a} - 2^a + 1$, $q = 2^a + 1 > 3$, and $T$ is 2-transitive of degree $pq$ (line 3 of Table III); or

(ii) $T = \text{PSL}(n, s)$ where $p = (s^n - 1)/(s - 1)$, and either

(a) $q$ divides $s - 1$ and $n \geq 3$ (line 3 of Table II); or

(b) $n = 3$, $q = s = 5$ (line 6 of Table II).

In case (ii), $T$ has a nontrivial block $D$ of imprimitivity in $V$ of cardinality $q$ and, if $\alpha \in D$, then $T_\alpha$ is transitive on $V \setminus D$.

That there are only the two cases (i) and (ii) can be read off from Tables II–IV. The transitivity assertion is proved in, for example, [21, Lemma 4.4], for case (ii)(a) and in [18] for case (ii)(b). Note that $n \geq 3$ in part (ii)(a) since $pq \notin \mathbb{N} \setminus \mathcal{C}$. Note also that, in cases (i) and (ii)(a), the group $T$ may not be minimal transitive for all values of the parameters, and so these groups also arise in the next theorem.

**Theorem 3.5.** Let $p$, $q$ be distinct odd primes such that $pq \notin \mathbb{N} \setminus \mathcal{C}$. Suppose that $T$ is a nonabelian simple group which can be represented as a transitive permutation group on a set $V$ of cardinality $pq$ such that $T$ is not minimal transitive. Then either $T$ is one of the groups in Theorem 3.4 or $T$ is one of the groups in Tables II–IV for which a proper transitive subgroup, $H$ say, is listed in the last column. In each of the latter cases, the set of subgroups of $T$ which are isomorphic to $H$ forms a single conjugacy class.
4. A MAXIMAL INTRANSITIVE NORMAL SUBGROUP

Let $p$, $q$, $r$ be distinct odd primes such that $pqr \notin \mathcal{H}_2 \cup \mathcal{H}_3$. The main result of this paper, Theorem 1.4, asserts that for such primes all vertex-transitive graphs of order $pqr$ are Cayley graphs. We shall prove this by assuming to the contrary that $\Gamma = (V, E)$ is a vertex-transitive, non-Cayley graph of order $pqr$ and deriving a contradiction. Our work builds on the results in [10, 24]. First we obtain some important information about the structure of a certain transitive subgroup $G$ of $\text{Aut}(\Gamma)$.

**Proposition 4.1.** Let $p$, $q$, $r$ be distinct odd primes such that $pqr \notin \mathcal{H}_2 \cup \mathcal{H}_3$. Let $\Gamma = (V, E)$ be a vertex-transitive, non-Cayley graph of order $pqr$. Then $\text{Aut}(\Gamma)$ is not quasiprimitive on $V$, and if $G$ is a subgroup of $\text{Aut}(\Gamma)$ which is minimal by inclusion subject to being transitive, but not quasiprimitive on $V$, then $G$ has an intransitive normal subgroup of prime index.

**Proof.** From our discussion in Section 2, $\text{Aut}(\Gamma)$ is not quasiprimitive on $V$. For a subgroup $G$ as in the statement, let $K$ be a non-trivial intransitive normal subgroup of $G$, and let $\Sigma$ denote the set of $K$-orbits in $V$. We may assume that $K$ is equal to the kernel of the action of $G$ on $\Sigma$. Suppose first that $|\Sigma|$ is a prime, say $|\Sigma| = r$. Then there exists an $r$-element $x \in G \setminus K$; $(x)$ must permute the $r$ orbits of $K$ transitively, and hence $(K, x)$ is transitive on $V$. Since $(K, x)$ has a non-trivial intransitive normal subgroup $K$, it follows from the minimality of $G$ that $G = (K, x)$. Moreover $x$ fixes each $K$-orbit setwise, and hence $x' \in K$ and $|G/K| = r$. Thus the result holds in this case.

We may therefore suppose that the $K$-orbits have prime length, say length $r$, and that $G/K$ is faithful and transitive on $\Sigma$ of degree $pq$. If $G/K$ is not quasiprimitive then $G$ has a normal subgroup $N$ containing $K$ such that the number of $N$-orbits is a prime. In this case, replacing $K$ by $N$, the argument of the previous paragraph shows that the result holds. Hence we may assume that $G/K$ is quasiprimitive on $\Sigma$ of degree $pq$. Let $K < N \leq G$ be such that $N/K$ is a minimal normal subgroup of $G/K$. Since $G/K$ is quasiprimitive on $\Sigma$, we have that $N/K$ is transitive on $\Sigma$, so $N$ is transitive on $V$ with intransitive normal subgroup $K$. By the minimality of $G$, therefore, $G = N$, whence $G/K$ is a simple group. Since $pq$ divides $|G/K|$, it follows that $G/K$ is a nonabelian simple group. Further, by the minimality of $G$ it follows that $G/K$ is a minimal transitive permutation group of degree $pq$, so $G/K$ is one of the simple groups $T$ of Theorem 3.4.

Let $R$ be a Sylow $r$-subgroup of $K$. Then $G = KN_{G}(R)$, so the group induced by $N_{G}(R)$ on $\Sigma$ is isomorphic to $T$ and in particular is transitive. Since $R$ is transitive on each of the $K$-orbits, $N_{G}(R)$ is transitive on $V$ with
intransitive normal subgroup $R$, and by minimality $G = N_G(R)$. Now $R$ has $pq$ orbits of length $r$, so $R \cong \mathbb{Z}_r^*$ for some $a \leq pq$. Let $\alpha \in V$, and let $B \in \Sigma$ be the $K$-orbit containing $\alpha$. Note that $\Sigma$ is the set of $R$-orbits. The set $\text{fix}_R(R_\alpha)$ of fixed points of $R_\alpha$ in $V$ is a union of $R$-orbits and is a block of imprimitivity for $G$ in $V$.

If $\text{fix}_R(R_\alpha)$ is a single $R$-orbit, then, for each $C \in \Sigma \setminus \{B\}$, $R_\alpha$ is transitive on $C$. In this case it follows, for example, from [10, Lemma 3.4], that $G$ is isomorphic to the lexicographic product $G_x [\hat{B}]$ of the quotient graph $G_x$ and the induced subgraph $\hat{B}$ on $B$. Since $pq, r \not\equiv s \pmod{\ell}$, both $G_x$ and $\hat{B}$ are Cayley graphs, and hence $G_x [\hat{B}]$ is a Cayley graph (see, for example, [10, Lemma 3.4]), contrary to our assumption. Hence $|\text{fix}_R(R_\alpha)| = rt$, where $t = p, q$ or $pq$.

Suppose next that $t = pq$, that is, $R_\alpha = 1$. Then $G/C_G(R)$ is isomorphic to a subgroup of $\text{Aut}(G) \cong \mathbb{Z}_{pq-1}$, and it follows that $C_G(R)$ involves the simple group $T$, and in particular that $C_G(R)$ is transitive on $\Sigma$. Since $C_G(R)$ contains $R$, $C_G(R)$ is transitive on $V$ and has an intransitive normal subgroup $R$. By minimality, $G = C_G(R)$. For each $C \in \Sigma$, since $K^C$ centralises the transitive abelian group $R^C$, and since a transitive abelian permutation group is self-centralising (see [27, Proposition 4.4]), it follows that $K^C = R^C$. Then since $R$ is a Sylow $r$-subgroup of $K$, we have that $K = R$. Since $G/G'$ is abelian and $G/K$ is a nonabelian simple group, it follows that $G = KG'$ and $G'$ is transitive on $\Sigma$. Suppose that $K \cap G' \neq 1$.

Then $K \cap G'$ is transitive on each block of $\Sigma$, so $G'$ is transitive on $V$ with intransitive normal subgroup $K \cap G'$. Thus by minimality, $G = G'$; and in this case $K \cap G' \leq Z(G) \cap G'$ so $r$ divides the order $M$ of the Schur multiplier of $T$. If Theorem 3.4(i) holds for $T$ then $T = \text{PSU}(3, 2^s)$ with $2^s > 2$, and $M = \gcd(3, 2^s+1) = 1$ (see, for example, [8, Section 6]), which is a contradiction. Hence Theorem 3.4(ii) holds and we have $T = \text{PSL}(n, s)$ and (again, see [8]) $M = \gcd(n, s-1)$ is divisible by $r$. This means that, modulo $r$,

$$s^n - 1 \equiv s^{n-1} + s^{n-2} + \cdots + 1 \equiv 1 + 1 + \cdots + 1 = n \equiv 0 \pmod{r},$$

which contradicts the fact that $(s^n - 1)/(s-1)$ divides $pq$.

Thus we have proved that $K \cap G' = 1$, so we have $G = K \times G'$ and $G' \cong G/K \cong \mathbb{Z}_{pq}$. If $G'$ is intransitive on $V$ then, replacing $K$ by $G'$, the result holds. Thus we may assume that $G'$ is transitive on $V$. If $G' = \text{PSU}(3, 2^s)$ with $2^s > 2$, we have, say, $p = s^2 - s + 1, q = s + 1$, and for $B \in \Sigma, G'_B \subseteq [s^2 - 1]$. As $r$ divides $|G'_B|$ (and $s$ is even and $r \not\equiv q$), $r$ must divide $s - 1$. However this means that $qr \not\equiv r \pmod{\ell}$ (see Theorem 1.1) which is a contradiction.

Hence $G' = \text{PSL}(n, s)$ with, say, $p = (s^2 - 1)/(s-1)$ and $n \geq 3$. Here $G'$ preserves a block system $A$ of $p$ blocks of size $qr$. Let $D \in A$ be the block
containing \( x \), so \( B \in D \). Consider the case where \( q \) divides \( s - 1 \) and \( G_B \geq [s^{n-1}] \text{SL}(n-1, s) \). Since \( s \equiv q + 1 \not\equiv 4 \), the group \( \text{SL}(n-1, s) \) is insoluble. Now the group \( G_B \) induced by \( G_B \) on \( B \) has a normal subgroup \( R_B \cong \mathbb{Z}_s \), and \( R_B \) is central in \( G_B^2 \) (since \( R \) is central in \( G \)). Since a transitive abelian permutation group is self-centralising (see [27, Proposition 4.4]), it follows that \( G_B^2 = R_B \). Hence \( (G_B)^2 \) is cyclic and so \( G_A \geq [s^{n-1}] \text{SL}(n-1, s) \) and \( r \) divides \( s - 1 \). However, in this case, it follows from Theorem 3.4 that \( G_a \) is transitive on \( V \setminus D \), and hence (applying, for example, [21, Lemma 3.1]), \( \Gamma \cong \Gamma(G, D) \). Since \( p, q \notin \mathcal{N} \), both \( (G_a) \) and \( D \) are Cayley graphs and it follows (see [10, Lemma 3.4]) that \( \Gamma \) is a Cayley graph, contradicting our assumption. The remaining case is where \( n = 3 \), \( s = 5 \), \( p = 31 \), \( q = 5 \). Here \( G_B = [5^2] \cdot [4] \cdot S_4 \), and since \( G_B \) has a subgroup of odd prime index \( r \), we have \( r = 3 \); but then \( qr \in \mathcal{N} \), which is a contradiction.

Thus \( |\text{fix}_V R_a| = tr \) with \( t = p \) or \( q \). Let \( \Delta \) denote the corresponding partition of \( V \) consisting of \( pq/t \) blocks of size \( tr \), and set \( D := \text{fix}_V R_a \), the block of \( \Delta \) containing \( x \). It follows that \( G^2 \) is imprimitive preserving a partition with \( pq/t \) blocks of size \( t \). By Theorem 3.4, \( G^2 = \text{PSL}(n, s) \), \( pq/t = (s^n - 1)/(s - 1) \), and \( n \geq 3 \). Moreover, \( G_a^2 \) is transitive on the set of \( pq - q \) blocks of \( \Sigma \) contained in \( V \setminus D \). Since \( G_a = G_a R \), the subgroup \( G_a \) is transitive on this set of \( pq - q \) blocks of \( \Sigma \). Since we also have that \( R_a \) is transitive on each of these \( pq - q \) blocks, it follows that \( G_a \) is transitive on \( V \setminus D \). As before this implies that \( \Gamma \cong \Gamma(G, D) \) and hence that \( \Gamma \) is a Cayley graph (since \( r, pq \notin \mathcal{N} \)), which is a contradiction. This contradiction completes the proof of Proposition 4.1.

5. PROOF OF THE MAIN THEOREM

Let \( p, q, r \) be distinct odd primes such that \( pq \notin \mathcal{N} \cup \mathcal{S} \), and let \( \Gamma = (V, E) \) be a vertex-transitive graph of order \( pqr \) which is not a Cayley graph. By Proposition 4.1, \( \text{Aut}(\Gamma) \) is not quasiprimitive on \( V \), and if \( G \) is a subgroup of \( \text{Aut}(\Gamma) \) which is minimal by inclusion subject to being transitive, but not quasiprimitive on \( V \), then \( G \) has an intransitive normal subgroup \( K \) of prime index, say \( r \). Let \( G, K \) be such subgroups, and let \( \Sigma \) denote the set of \( K \)-orbits in \( V \). Since \( \Gamma \) is not a Cayley graph, it follows from the main result of [10] that \( G \) is not genuinely 3-step imprimitive (see Definition 2.1). Thus every non-trivial normal subgroup of \( G \) contained in \( K \) is transitive on each of the \( K \)-orbits in \( \Sigma \). Now let \( M \) be a minimal normal subgroup of \( G \) contained in \( K \). If \( M \) is elementary abelian then the \( M \)-orbits have prime length, since their length must divide both \( |V| = pqr \) and \( |M| \), and this is a contradiction. Thus \( M \) is nonabelian, that is, \( M \cong T^a \) for some nonabelian simple group \( T \) and positive integer \( a \). There is an
r-element \( x \) in \( G \setminus K \), and for such an element, \( \langle M, x \rangle \) is transitive on \( V \) with intransitive normal subgroup \( M \). By the minimality of \( G \) it follows that \( G = \langle M, x \rangle \).

We shall prove that \( M \cong T \), that is, that \( a = 1 \). Let \( B \in \Sigma \), and note that \( M \) is transitive on \( B \). Since \( |B| = pq \), we have that \( pq \) divides \( |T| \). If the group \( M^B \) induced by \( M \) on \( B \) was not quasiprimitive then \( T \) would be a composition factor of a transitive permutation group of degree \( p \) and also a composition factor of a transitive permutation group of degree \( q \). Without loss of generality suppose that \( q < p \). Then we have a contradiction, since \( q \) is the largest prime which divides the order of a transitive permutation group of degree \( q \). Hence \( M^B \) is quasiprimitive of degree \( pq \). By the O'Nan–Scott theorem for quasiprimitive groups [22], \( M^B \) is almost simple, and hence \( M^B \cong T \). If \( a > 1 \) then the pointwise stabilizer \( M_{(B)} \) of \( B \in \Sigma \) in \( M \) is nontrivial. Moreover, \( \text{fix}_x M_{(B)} \) is a block of imprimitivity for \( G \) in \( V \) and is a union of complete blocks of \( \Sigma \) (since \( M_{(B)} \) is normal in \( M \)). Since \( G \) is primitive on \( \Sigma \), it follows that \( \text{fix}_x M_{(B)} = B \) and hence that \( M_{(B)} \) is transitive on each block of \( \Sigma \setminus \{B\} \). It follows from, for example, [10, Lemmas 3.3 and 3.4] that \( \Gamma \cong \Gamma_s[B] \) and hence that \( \Gamma \) is a Cayley graph, which is a contradiction. Hence \( a = 1 \) and \( M = T \).

Suppose that \( M^B \) is not one of the groups listed in Theorem 3.4. Then, by Theorems 3.4 and 3.5, \( M \) has a proper subgroup \( H \) which is transitive on \( B \) and is such that all the subgroups of \( M \) isomorphic to \( H \) form a single \( M \)-conjugacy class. Thus we have \( G = MN_G(H) \), and so \( N_G(H) \) is transitive on \( V \) with an intransitive normal subgroup \( H \), contradicting the minimality of \( G \). Hence \( M^B \) is one of the groups listed in Theorem 3.4.

Suppose that \( C := C_{c_x}(M) \neq 1 \). Then \( C \) is a normal \( r \)-subgroup of \( G \) and hence the \( C \)-orbits have length a power of \( r \) dividing \( pqr \), that is, the \( C \)-orbits have length \( r \). It follows that \( C \) is elementary abelian and, as \( C \) is also cyclic, \( |C| = r \). By the minimality of \( G \) we have that \( G = M \times C \), and hence that \( M = K \). Since \( G = \langle M, x \rangle \), it follows also that \( C = \langle x \rangle \cong \mathbb{Z}_r \). Now, by examining all the quasiprimitive groups of degree \( pq \), which are listed in the results in Section 3 we see that \( M \) has up to equivalence at most two transitive permutation representations of degree \( pq \), and the sub-set of blocks of \( \Sigma \) on which the action of \( M \) is equivalent to its action on \( B \) forms a block of imprimitivity for the action of \( G \) on \( \Sigma \). Since \( G \) is primitive on \( \Sigma \) it follows that the action of \( M \) on each block of \( \Sigma \) is equivalent to its action on \( B \). In particular \( M_x \) fixes exactly one point of each block of \( \Sigma \).

Suppose that \( M = \text{PSU}(3, 2^a) \). Then \( M_x \) fixes one point of each of the blocks of \( \Sigma \) and is transitive on the \( pq - 1 \) remaining points of each of these blocks. In the symmetric group \( \text{Sym} V \), the overgroup \( S_{pq} \times C \) of \( M \times C \) has the same suborbits as \( M \times C \) in \( V \), and hence \( S_{pq} \times C \leq \text{Aut} \Gamma \). Since \( S_{pq} \times C \) contains a regular subgroup, \( \Gamma \) is a Cayley graph, which is a contradiction.
Hence $M = \text{PSL}(n, s)$, $p = (s^n - 1)/(s - 1)$, and $n \geq 3$. By Theorem 3.4, $M^s$ has a block $D$ of imprimitivity of length $q$ containing $x$, and $M_s$ is transitive on $B \setminus D$. Let $\Sigma = \{B_1 = B, \ldots, B_\ell\}$, let $x_i$ be the point of $B_i$ fixed by $M_s$, and let $D_i$ be the block of length $q$ in $B_i$ containing $x_i$. Then, for each $i$, $G_s = M_s$ fixes $D_i$ setwise and is transitive on $B_i \setminus D_i$. Hence, for each $i$, $H := M_D$ is equal to $M_D$, the setwise stabiliser in $M$ of $D_i$. Also, since $H$ is transitive on each of the $D_i$, each $H$-orbit in $V := D_1 \cup \cdots \cup D_\ell$ is trivially joined to each of the $B_i \setminus D_i$. It follows from [21, Lemma 3.3] that $\text{Aut} \, H$ contains the group $H^{(E)}$, which is defined as the permutation group on $V$ inducing on $E$ the same permutation group that $H$ does and fixing $V \setminus E$ pointwise. Let $y \in M$ be an element of order $p$, and let $h \in H^{(E)}$ be an element of order $q$. Then, for $j = 0, 1, \ldots, p - 1$, $h_j := y^{-j}hy$ has order $q$, and $\langle h_j \rangle$ is transitive on $D_i^{(y)}$ and fixes $B_i \setminus D_i^{(y)}$ pointwise for each $i$. Moreover, $h_j^q = h_{j+1}$ for $0 \leq j < p - 2$ and $h_j^{q+1} = h_0$. Hence $h' := h_0h_1 \cdots h_{p-1}$ is centralised by $y$ and by $C = \langle x \rangle$ and has $pr$ orbits of length $q$. Thus $\langle h', y, x \rangle$ is regular on $V$, and so $\Gamma$ is a Cayley graph, which is a contradiction.

Hence $C_{\langle y \rangle}(M) = 1$ and so $G \leq \text{Aut} \, M$ and $r$ divides $|\text{Out} \, M|$. If $M = \text{PSL}(3, 2^a)$ with $p = 2^{2a} - 2^a + 1$ and $q = 2^a + 1 > 3$, then $|\text{Out} \, M|$ divides $2a \cdot \gcd(3, 2^a + 1) = 2a$. However, in order for $q = 2^a + 1$ to be prime, $a$ must be a power of 2. Hence $|\text{Out} \, M|$ has no odd prime divisor. Similarly, $|\text{Out} \, \text{PSL}(3, 5)| = 2$ which has no odd prime divisor. Thus $M = \text{PSL}(n, s)$, $p = (s^n - 1)/(s - 1)$, $n \geq 3$, and $q$ divides $s - 1$. Since $p$ is prime, $s$ and $n$ must be prime also. Hence $|\text{Out} \, M| = 2\gcd(n, s - 1)$, and so $r = n$ and $r$ divides $s - 1$. However this means that $p = s^{s-1} + \cdots + s + 1 \equiv 1 + \cdots + 1 + 1 = n \equiv 0 \pmod{r}$, and hence that $p = r$, which is a contradiction.

REFERENCES