Journal of Algebraic Combination 3 (1994), 77–111

Non-Cayley Vertex-Transitive Graphs of Order Twice the Product of Two Odd Primes

ALICE ANN MILLER AND CHERYL E. PRAEGER
Department of Mathematics, University of Western Australia, Nedlands, WA 6009, Australia.

Received November 16, 1992; Revised June 22, 1993

Abstract. For a positive integer n, does there exist a vertex-transitive graph Γ on n vertices which is not a Cayley graph, or, equivalently, a graph Γ on n vertices such that Aut Γ is transitive on vertices but none of its subgroups are regular on vertices? Previous work (by Alspach and Parsons, Frucht, Graver and Watkins, Marušič and Scapellato, and McKay and the second author) has produced answers to this question if n is prime, or divisible by the square of some prime, or if n is the product of two distinct primes. In this paper we consider the simplest unresolved case for even integers, namely for integers of the form $n = 2pq$, where $2 < q < p$, and p and q are primes. We give a new construction of an infinite family of vertex-transitive graphs on $2pq$ vertices which are not Cayley graphs in the case where $p \equiv 1 \pmod q$. Further, if $p \not\equiv 1 \pmod q$, $p \equiv q \equiv 3 \pmod 4$, and if every vertex-transitive graph of order pq is a Cayley graph, then it is shown that, either $2pq = 66$, or every vertex-transitive graph of order $2pq$ admitting a transitive imprimitive group of automorphisms is a Cayley graph.

Keywords: finite vertex-transitive graph, automorphism group of graph, non-Cayley graph, imprimitive permutation group

1. Introduction

In [22] Marušič asked: For which positive integers n does there exist a vertex-transitive graph on n vertices which is not a Cayley graph? The problem of determining such numbers was investigated by Marušič [22] when n is a prime power, and many constructions of families of non-Cayley, vertex-transitive graphs can be found in the literature, for example see [1, 10, 19, 23, 25, 32]. Constructions and partial solutions to the problem were summarized and extended in [19]. For even integers $n \geq 14$ it was shown in [19, Theorem 2(c)] that there is a non-Cayley vertex-transitive graph of order n except possibly if $n = 2p_1p_2 \cdots p_r$ where the p_i are distinct primes congruent to 3 modulo 4, $r \geq 1$. If $r = 1$ there is no such graph, see [2]. This paper considers the problem for the next case, $n = 2p_1p_2$, where $2 < p_1 < p_2$. We shall give a construction of a non-Cayley vertex-transitive graph on $2p_1p_2$ vertices in the case where $p_2 \equiv 1 \pmod{p_1}$. Further if $p_2 \not\equiv 1 \pmod{p_1}$, $p_1 \equiv p_2 \equiv 3 \pmod 4$, and if every vertex-transitive graph on p_1p_2 vertices is a Cayley graph then we shall show that either $2p_1p_2 = 66$, or every graph on $2p_1p_2$ vertices which admits a transitive imprimitive group of automorphisms is a Cayley graph.

A *graph* $\Gamma = (V, E)$ consists of a set V of *vertices* and a set E of unordered pairs from V called *edges*. The cardinality of V is called the *order* of Γ. The *automorphism group* Aut Γ of Γ is the subgroup of all permutations of V which preserve the edge-set E, and Γ is said to be *vertex-transitive* if Aut Γ is transitive on V. For group G and a subset X of G such that $1_G \notin X$ and $X^{-1} = X$, where $X^{-1} = \{x^{-1} | x \in X\}$, the *Cayley graph* $\mathrm{Cay}(G, X)$ of G relative to X is the graph with vertex set G such that two vertices $g, h \in G$ are *adjacent*, that is $\{g, h\}$ is an edge, if and only if $gh^{-1} \in X$. The group G acting by right multiplication is then a subgroup of the automorphism group of $\mathrm{Cay}(G, X)$, and as G is *regular* on vertices (that is G is transitive and only the identity fixes a vertex) $\mathrm{Cay}(G, X)$ is a vertex-transitive graph. Thus all Cayley graphs are vertex-transitive. Conversely, every vertex-transitive graph Γ for which Aut Γ has a subgroup G which is regular on vertices is isomorphic to a Cayley graph for G. However there are vertex-transitive graphs which are not Cayley graphs. We will call such graphs *non-Cayley vertex-transitive graphs*, and these are the subject of this paper. The order of a non-Cayley, vertex-transitive graph will be called a *non-Cayley number*. Let NC denote the set of non-Cayley numbers.

An important, but elementary, fact about non-Cayley numbers is that, for every non-Cayley number n and every positive integer k, kn is also a non-Cayley number, for the union of k vertex disjoint copies of a non-Cayley, vertex-transitive graph of order n is a non-Cayley, vertex transitive graph of order kn. Thus the important numbers n to examine turn out to be those with few prime factors. We have the following information about non-Cayley numbers which are relevant to our investigations of even numbers, where p and q are distinct odd primes, $p > q$.

(a) [2, 10], $2p \in NC$ if and only if $p \equiv 1 \pmod 4$.
(b) [19, Theorem 5], $2p^2 \in NC$.
(c) [19, Theorem 3], $4p \in NC$ if $p \geq 5$.
(d) [17, 21, 27], for $n \leq 24$, n even, $n \in NC$ if and only if n is one of 10, 16, 18, 20, 24.
(e) [1, 24, 25, 26] or see [20], $pq \in NC$ for $q < p$ if and only if one of the following holds:
  (i) q^2 divides $p - 1$,
  (ii) $p = 2q - 1 > 3$ or $p = (q^2 + 1)/2$.
  (iii) $p = 2^t + 1$ and q divides $2^t - 1$, or $q = 2^{t-1} - 1$.
  (iv) $p = 2^t - 1$, $q = 2^{t-1} + 1$.
  (v) $(p, q) = (7, 5)$ or $(11, 7)$.

From results (a)–(e) we see that membership of an even number n in NC can be determined unless $n = 2p_1p_2 \cdots p_r$ where $p_1, p_2, \ldots, p_r$ are distinct primes congruent to 3 modulo 4 and $r \geq 2$ and where none of the conditions (i)–(v) of (e) hold for any pair of primes $p, q \in \{p_1, p_2, \ldots, p_r\}$.

In this paper we investigate the first open case, namely $n = 2pq$ with p, q distinct primes, $p \equiv q \equiv 3 (\mathrm{mod}\ 4)$. We give (Construction 2.1) a construction of an infinite family of vertex-transitive non-Cayley graphs of order $2pq$ where q divides $p - 1$. Thus we have:

THEOREM 1. *If $2 < q < p$ and p, q are primes such that $p \equiv 1$ (mod q), then $2pq \in NC$.*

Then we analyze vertex-transitive graphs of order $2pq$ such that $2 < q < p$, $pq \notin NC$, $p \not\equiv 1$ (mod q), $p \equiv q \equiv 3(\mathrm{mod}\ 4)$. We confine ourselves to examining graphs $\Gamma = (V, E)$ for which Aut Γ has a subgroup H which is transitive and imprimitive on V. (A transitive permutation group H on V is said to be *imprimitive* on V if there is a partition $\Sigma = \{B_1, B_2, \dots, B_r\}$ of V with $1 < |\Sigma| < |V|$ such that, for each $h \in H$ and each $B_i \in \Sigma$, the image B_i^h also lies in Σ; such a partition Σ is said to be H-invariant. If there is no such partition for a transitive group H then H is said to be *primitive* on V.) Our reasons for this restriction are two-fold. The set of numbers n for which there exists a vertex-primitive non-Cayley graph has zero density in the set of all positive integers. This can be easily derived from the result of Cameron, Neumann, and Teague [5] that the set of numbers n for which there is a primitive permutation group on n points, different from A_n and S_n, has zero density in the set of all positive integers. (Note that the only graphs of order n admitting A_n or S_n as a group of automorphisms are the *complete graph* K_n and the *empty graph* $n.K_1$, both of which are Cayley graphs.) Thus the case where there is a vertex-imprimitive group of automorphisms is the heart of the problem. The other reason for omitting the primitive case here is that it will be treated by Greg Gamble as an application of his, as yet unfinished, classification of primitive permutation groups of degree kp, $k < 2p$, p a prime.

THEOREM 2. *Let p and q be primes such that $2 < q < p$, $p \equiv q \equiv 3$(mod 4), $p \not\equiv 1$ (mod q), and $pq \notin NC$. Let Γ be a vertex-transitive graph of order $2pq$ which admits some transitive imprimitive group of automorphisms. Then either Γ is a Cayley graph or $p = 11$, $q = 3$.*

Notation

A transitive permutation group G acting on a set V induces a natural action on $V \times V$ given by

$$(\alpha, \beta)^g := (\alpha^g, \beta^g)$$

for all $\alpha, \beta \in V$ and $g \in G$. The G-orbits in $V \times V$ are called *orbitals* of G. In particular $\Delta_0 = \{(\alpha, \alpha) | \alpha \in V\}$ is an orbital, called the *trivial orbital* and all other orbitals are said to be *nontrivial*. For $\alpha \in V$, the G_α-orbits in V are called *suborbits* of G, and they are precisely the sets $\Delta(\alpha) := \{\beta | (\alpha, \beta) \in \Delta\}$

where Δ is an orbital. For each orbital Δ, the set $\Delta^* := \{(\beta, \alpha) | (\alpha, \beta) \in \Delta\}$ is also an orbital and is called the orbital *paired* with Δ; if $\Delta^* = \Delta$ then Δ is said to be *self-paired*. Similarly $\Delta^*(\alpha)$ is called the G_α-orbit paired with $\Delta(\alpha)$ and if $\Delta^*(\alpha) = \Delta(\alpha)$ (which is equivalent to $\Delta^* = \Delta$) then $\Delta(\alpha)$ is said to be self-paired.

Let Θ be a union of orbitals which is self-paired (that is $\Delta \subseteq \Theta$ implies $\Delta^* \subseteq \Theta$) and such that $\Delta_0 \not\subseteq \Theta$. The *generalized orbital graph* corresponding to Θ is defined as the graph $\Gamma^{(\Theta)}$ with vertex set V such that $\{\alpha, \beta\}$ is an edge if and only if $(\alpha, \beta) \in \Theta$. The fact that Θ is self-paired ensures that the adjacency relation is symmetric, and the fact that $\Delta_0 \not\subseteq \Theta$ ensures that there are no loops. Clearly G is a subgroup of automorphisms of $\Gamma^{(\Theta)}$ which is vertex-transitive. Conversely, it is not hard to see that every graph admitting a vertex-transitive group G of automorphisms is a generalized orbital graph for G corresponding to some self-paired union of orbitals. If Θ consists of a single self-paired orbital then $\Gamma^{(\Theta)}$ is called an *orbital graph*.

For a connected graph $\Gamma = (V, E)$, a vertex $\alpha \in V$, and a positive integer i, the set of vertices at distance i from α is denoted by $\Gamma_i(\alpha)$. (Here the *distance* between two vertices is the length of the shortest path between them.) If Σ is a partition of V then the *quotient graph* Γ_Σ is defined as the graph with vertex set Σ such that $\{B, B'\}$ is an edge, where $B, B' \in \Sigma$, if and only if, for some $\alpha \in B$ and $\alpha' \in B'$, $\{\alpha, \alpha'\} \in E$. For a subset B of V the *induced subgraph* $\overline{B}$ is the graph with vertex set B and edge set $\{\{\alpha, \beta\} \in E | \alpha, \beta \in B\}$. In particular if $G \leq \mathrm{Aut}\Gamma$, G is vertex-transitive, and Σ is a G-invariant partition of V, then the induced subgraph $\overline{B}$, for $B \in \Sigma$, is independent of the choice of B; the two graphs, Γ_Σ and $\overline{B}$ will be analyzed in detail whenever such a pair G, Σ arises. Two disjoint nonempty subsets U, W of V are said to be *trivially joined* if either, for all $\alpha \in U$, $\Gamma_1(\alpha) \supseteq W$, or for all $\alpha \in U$, $\Gamma_1(\alpha) \cap W = \emptyset$.

The *lexicographic product* $\Gamma_1[\Gamma_2]$ of $\Gamma_2 = (V_2, E_2)$ by $\Gamma_1 = (V_1, E_1)$ has vertex set $V_1 \times V_2$ and $\{(x_1, x_2), (y_1, y_2)\}$ is an edge if and only if either $(x_1, y_1) \in E_1$, or $x_1 = y_1$ and $(x_2, y_2) \in E_2$. Since Aut $\Gamma_1[\Gamma_2]$ contains the wreath product Aut Γ_2 *wr* Aut Γ_1, if Γ_1 and Γ_2 are both Cayley graphs it follows that $\Gamma_1[\Gamma_2]$ is also a Cayley graph.

For a group G, the *socle* soc G of G is the product of the minimal normal subgroups of G. If G is a group of permutations of a set V then $\mathrm{fix}_V G = \{\alpha \in V | \alpha^g = \alpha \text{ for all } g \in G\}$ is the set of *fixed points* of G in V.

2. Non-Cayley graphs of order 2*pq*

In this section we give constructions of two families of non-Cayley vertex-transitive graphs of order $2pq$.

The first construction gives a non-Cayley vertex-transitive graph of order $2pq$ where p and q are odd primes and q divides $p-1$.

Construction 2.1. The graphs $A(p,q)$, where p and q are odd primes and q divides $p-1$. Consider the following group G of order $4p^2q$: $G = \langle a, b, c, x\rangle$ where $a^p = b^p = c^q = x^4 = [a, b] = 1$, and also $a^x = b$, $b^x = a^{-1}$, $c^x = c^{-1}$, $a^c = a^\varepsilon$ and $b^c = b^{\varepsilon^{-1}}$ where $1 < \varepsilon \leq p-1$, and $\varepsilon^q \equiv 1 (\text{mod } p)$. Let $H = \langle b, x^2\rangle$ and let $V = [G : H]$, the set of right cosets of H in G with G acting by right multiplication. Let $A(p, q)$ be the graph with vertex set V and with edges $\{H_y, H_z\}$ such that $yz^{-1} \in (HaH) \cup (HcH) \cup (Hc^{-1}H) \cup (HxH)$.

We shall show in Proposition 2.1 that $A(p, q)$ is a vertex-transitive non-Cayley graph of order $2pq$ and valency $p+4$ such that $\text{Aut}A(p,q)$ contains G as a subgroup of index dividing 8. Before proving this we discuss in more detail the action of G on V. Let $\alpha = H \in V$ so that $G_\alpha = H$. There is a one-to-one correspondence between the set V of points and the right transversal $T = \langle a, c\rangle \cup \langle a, c\rangle x$ of G_α in G, such that $\alpha = 1$ and an element $g \in G$ maps $t \in T$ to $t' \in T$, where $Ht' = Htg$. The actions of the generators a, b, c, x, and the element x^2 on V identified with T are given as follows: (note that $xa = b^{-1}x$ and $xb = ax$, and $ca = a^{\varepsilon^{-1}}c$).

$$\begin{aligned}
a &: a^ic^j \to a^{i+\varepsilon^{-j}}c^j, & &: a^ic^jx \to a^ic^jx\\
b &: a^ic^j \to a^ic^j, & &: a^ic^jx \to a^{i+\varepsilon^{-j}}c^jx\\
c &: a^ic^j \to a^ic^{j+1}, & &: a^ic^jx \to a^ic^{j-1}x\\
x &: a^ic^j \to a^ic^jx, & &: a^ic^jx \to a^{-i}c^j\\
x^2 &: a^ic^j \to a^{-i}c^j, & &: a^ic^jx \to a^{-i}c^jx.
\end{aligned}$$

The set of orbits of the normal subgroup $L = \langle a, b\rangle$ of G is a block system for G. It consists of $2q$ blocks of size p, namely $B_j = (c^j)^L = \{a^ic^j | i \in Z_p\}$, $j \in Z_q$ and $C_j = (c^jx)^L = \{a^ic^jx | i \in Z_p\}$, $j \in Z_q$. Let us denote this block system by $\Sigma = \Sigma_1 \cup \Sigma_2$, where $\Sigma_1 = \{B_i | i \in Z_q\}$ and $\Sigma_2 = \{C_i | i \in Z_q\}$. In addition, G preserves the block system $\Delta = \{D_1, D_2\}$ where $D_1 = \cup_{i\in Z_q} B_i$ and $D_2 = \cup_{i \in Z_q} C_i$.

Now $(a^i)^{G_\alpha} = \{a^i, a^{-i}\}$ for all $i \in Z_p$, and so the G_α-orbits in B_0 are $\Delta_{\pm i,0}(\alpha) = \{a^i, a^{-i}\}$, for $i \in Z_p$. Since a^{-i} sends the pair $(1, a^i)$ to $(a^{-i}, 1)$ it follows that the orbits $\Delta_{\pm i,0}(\alpha)$ are self-paired. Also, since $c^{-j}a^{-i} : (1, a^ic^j) \to (c^{-j}a^{-i}, 1) = (a^{-i\varepsilon^j}c^{-j}, 1)$, while $\{a^ic^j\}^{G_\alpha} = \{a^ic^j, a^{-i}c^j\}$, the G_α-orbit $\Delta_{\pm i,j}(\alpha) = \{a^ic^j, a^{-i}c^j\}$ in B_j is paired to the G_α-orbit $\Delta_{\pm i\varepsilon^j,-j}(\alpha) = \{a^{-i\varepsilon^j}c^{-j}, a^{i\varepsilon^j}c^{-j}\}$ in B_{-j}. Furthermore $x^{-1}c^{-j}a^{-i}$ maps $(1, a^ic^jx)$ to $(c^jx, 1)$ since $x^{-1}c^{-j}a^{-i} = x^2b^{i\varepsilon^j}c^jx$ is in the same G_α-coset as c^jx. Nothing that

$$(a^ic^jx)^{G_\alpha} = \{a^{\pm i + t\varepsilon^{-j}}c^jx \mid t \in Z_p\} = C_j$$

for all $i \in Z_p$, $j \in Z_q$, each C_j is a self-paired G_α-orbit.

Thus $A(p, q)$ is the generalized orbital graph (as defined in Section 1) associated with the G_α-orbits containing the points a, c, c^{-1}, and x and so has valency

$|\Delta_{\pm1,0}(\alpha)| + |\Delta_{0,1}(\alpha)| + |\Delta_{0,-1}(\alpha)| + |C_0| = p + 4$. Clearly $A(p, q)$ admits G as a vertex-transitive group of automorphisms, its edge-set is $\bigcup_{1\le j\le 3} E_j$ where $E_1 = \{1, a\}^G$, $E_2 = \{1, c\}^G \cup \{1, c^{-1}\}^G$, and $E_3 = \{1, x\}^G$. For any edge $e \in E(\Gamma)$ let us say that e is a *type j edge* if and only if $e \in E_j$.

PROPOSITION 2.1. *The graph $A(p, q)$ is a vertex-transitive non-Cayley graph of order $2pq$ and valency $p + 4$, and $|Aut A(p, q) : G|$ divides* 8.

Proof. Set $\Gamma = A(p, q)$ and $A = \mathrm{Aut}\,\Gamma$. All type 1 edges consist of a pair of points contained in some set B_j or some set C_j, for $j \in Z_q$. Every edge of this type lies on p triangles each of which contains two type 3 edges. Also all type 2 edges consist of a pair of points lying in different sets B_j and $B_{j'}$ or in different sets C_j and $C_{j'}$ where $0 \le j < j' < q$. All edges of this type lie in 0 triangles if $q > 3$ and in 1 triangle (consisting of three type 2 edges) if $q = 3$. Finally all type 3 edges consist of one point in a set B_j and one point in C_{-j}, for some $j \in Z_q$, and lie in 4 triangles each consisting of two type 3 edges and one edge of type 1. Since p, 0 (or 1), and 4 are all distinct, Aut Γ preserves the sets E_1, E_2, and E_3. Hence Aut Γ permutes the connected components of the graph Γ_J defined as the graph with the same vertex set as Γ and with edge set $\bigcup_{j\in J} E_j$ for each $J \subseteq \{1, 2, 3\}$. Taking $J = \{1\}$ we obtain that $\{B_1, \ldots, B_q, C_1, \ldots, C_q\}$ is preserved by A and taking $J = \{1, 2\}$, we find that $\{D_1, D_2\}$ is preserved by A.

Now A contains G, and hence A is transitive on V and $|A : A_\alpha| = 2pq$. For $1 \le j \le 3$, A_α fixes $\Gamma_1(\alpha) \cap E_j$ setwise and, since $x^2 \in A_\alpha$ and x^2 interchanges a and a^{-1}, $|A : A_{\alpha,a}| = 4pq$. In addition, as the subgraph induced on B_0 is a cycle of length p, $A_{\alpha,a}$ fixes B_0 pointwise. Since the only type 2 edges from α end in c and c^{-1}, $A_{\alpha,a}$ fixes setwise $\{c, c^{-1}\}$. So $|A_{\alpha,a} : A_{\alpha,a,c}| = 1$ or 2. Moreover, since each point of B_0 is joined to exactly one point of B_1 and one point of B_{q-1}, $A_{\alpha,a,c}$ fixes $B_1 \cup B_{q-1}$ pointwise and in fact $A_{\alpha,a,c}$ fixes D_1 pointwise. Further, since edges from points of B_i to points of D_2 go only to points of C_{-i}, $A_{\alpha,a,c}$ fixes each C_i setwise. Since $b \in A_{\alpha,a,c}$, $A_{\alpha,a,c}$ is transitive on C_0, so $|A_{\alpha,a,c} : A_{\alpha,a,c,x}| = p$. Arguing as above $A_{\alpha,a,c,x}$ fixes $\Gamma_1(x) \cap C_0$ and $\Gamma_1(x) \cap (C_1 \cup C_{q-1})$ (which are sets of size 2) setwise, and the stabilizer in $A_{\alpha,a,c,x}$ of a point of each of these sets fixes D_2 pointwise. Hence $|A_{\alpha,a,c,x}|$ divides 4. Thus $|A| = 4p^2q\delta$ where δ is 1, 2, 4, or 8.

Now $|G| = 4p^2q$ and so $\delta = |A : G| = 1, 2, 4$, or 8. Let A^+ be the subgroup of A fixing D_1 and D_2 setwise. Then $|A : A^+| = 2$, and $A = \langle A^+, x\rangle = A^+G$. So $|A^+ : A^+ \cap G| = |A : G| = \delta$. Now A^+ acts on the quotient graph $\hat{\Sigma}_i$ with vertex set Σ_i such that two elements of Σ_i are adjacent in $\hat{\Sigma}_i$ if there is at least one edge of Γ having a point in each of those elements. Since $\hat{\Sigma}_i$ is a cycle of length q, Aut $\hat{\Sigma}_i \simeq D_{2q}$. Let $K_i = A^+_{(\Sigma_i)}$ (the subgroup fixing each element of Σ_i setwise) and let $P = \langle a, b\rangle$. Then $P \subseteq K_1 \cap K_2$ (as $|A^+/(K_1 \cap K_2)|$ divides $4q^2$). Moreover $K_1 \cap K_2 = A_{(\Sigma)}$ and $K_1 \cap K_2 \lesssim \prod_{i\in Z_q}(K_1 \cap K_2)^{B_i} \times \prod_{i\in Z_q}(K_1 \cap K_2)^{C_i} \le D_{2p}^{2q}$. It follows that P, which is a Sylow p-subgroup of A (since p^3 does not divide $|A|$), is normal in $K_1 \cap K_2$. Hence P is a characteristic subgroup of $K_1 \cap K_2$ and therefore P is a normal subgroup of A.

Suppose that A has a subgroup R which is regular on vertices. Then $|R| = 2pq$. So R contains a Sylow q-subgroup of A (since q^2 does not divide $|A|$). We may therefore assume that $c \in R$ (by replacing R by some conjugate if necessary). Moreover $|R \cap P| = p$ (since P is the unique Sylow p-subgroup of A). Since $R \cap P$ is transitive on each element of Σ, $R \cap P = \langle ab^i \rangle$ for some $i \not\equiv 0$ (mod p). Now $(ab^i)^c \in \langle ab^i \rangle$, since $R \cap P$ is normal in R. But $(ab^i)^c = a^c(b^c)^i = a^\varepsilon b^{\varepsilon^{-1} i}$ and hence $(ab^i)^c = (ab^i)^\varepsilon$ so $b^{\varepsilon^{-1} i} = b^{i\varepsilon}$. Hence $b^{i(\varepsilon - \varepsilon^{-1})} = 1$ and so $\varepsilon \equiv \varepsilon^{-1}$ (mod p). Thus $\varepsilon^2 \equiv 1$ (mod p) which is a contradiction since ε has order q modulo p. Hence A has no regular subgroup and Γ is a non-Cayley graph. □

The next construction produces a non-Cayley vertex-transitive graph of order $r(r+1)/2$ for each odd prime power $r \geq 7$; the order is of the form $2pq$ with p and q distinct odd primes if and only if $p = r = 4q - 1$.

Construction 2.2. The graphs Ext(r) constructed from a conic in the projective plane $PG_2(r)$, for r an odd prime power. Let C be a conic in $PG_2(r)$, that is C is a maximal subset of $PG_2(r)$, no three points collinear. Then $|C| = r + 1$. Points not on C lie on either 2 or 0 tangents to C; those points lying on 2 tangents to C are called *external points* to C. There are $r(r+1)/2$ external points. For an external point P let A and B be the two points of C such that the lines PA and PB are tangents to C, and let $P^\perp$ denote the line AB. Then $P^\perp$ contains exactly $(r-1)/2$ external points since there are $r - 1$ tangent lines which meet $P^\perp$ in points different from A, B, and each of these (external) points lies on two such tangent lines. It follows from the above discussion that, if Q is a point on $P^\perp$, then P lies on $Q^\perp$ also.

Define a graph $Ext(r)$ with vertex set the set of external points to C, such that a pair $\{P, Q\}$ of external points is an edge if and only if Q lies on $P^\perp$ (or equivalently P lies on $Q^\perp$).

PROPOSITION 2.2. *Let r be a power of an odd prime.*

(a) *The (isomorphism class of the) graph $Ext(r)$ is independent of the choice of C.*
(b) *$Ext(r)$ is a vertex-transitive graph of order $r(r+1)/2$ and valency $(r-1)/2$. Further $Ext(3) \cong 3K_2$, $Ext(5) \cong 5C_3$, and, for $r \geq 7$, the graph $Ext(r)$ is connected, and $Aut(Ext(r)) \cong P\Gamma L(2, r)$ is primitive on vertices, transitive on ordered pairs of adjacent vertices, and has no subgroup regular on vertices.*
(c) *For $r \geq 7$, the group $PSL(2, r)$ is the unique subgroup of $Aut(Ext(r))$ which is minimal transitive on vertices; it is imprimitive on vertices if and only if $r = 7$, 9, or 11.*
(d) *The order $r(r+1)/2$ of $Ext(r)$ is equal to $2pq$, where $2 < q < p$ and p and q are primes, if and only if $p = 4q - 1 = r$.*

Proof. Since $PGL(3, r)$ is transitive on the set of all conics in $PG(2, r)$, graphs constructed as above with respect to different conics are isomorphic. Clearly $Ext(r)$ has order $r(r+1)/2$ and valency $(r-1)/2$. Let $\Gamma = Ext(r)$ and $A = \mathrm{Aut}\,\Gamma$. By construction the stabilizer of C in $P\Gamma L(3, r)$, namely $P\Gamma L(2, r)$, is contained in A and $PGL(2, r)$ is transitive on the external points to C. Hence Γ is vertex-transitive. For $r = 3$, Γ has valency 1 so $\Gamma \cong 3K_2$. For $r = 5$, Γ has order 15 and valency 2 so $\Gamma \cong sC_t$ where $st = 15$; the group $PGL(2, 5) \cong S_5$ must therefore permute the s connected components of Γ, each of which has size at least 3, and it follows that $\Gamma \cong 5C_3$.

Now let $r \geq 7$. Then the stabilizer in $PGL(2, r)$ of an external point P, namely $D_{2(r-1)}$, is maximal in $PGL(2, r)$, so $PGL(2, r)$, and hence A, is primitive on vertices. In particular Γ is connected. Also, as $D_{2(r-1)}$ is transitive on the external points on $P^{\perp}$, it follows that $PGL(2, r)$, and hence A, is transitive on ordered pairs of adjacent vertices of Γ. It follows from [15] that $P\Gamma L(2, r)$ is a maximal subgroup of $A_{r(r+1)/2}.P\Gamma L(2, r)$ and hence $A = P\Gamma L(2, r)$. Then by [9], A has no subgroup regular on vertices.

Suppose that $r \geq 7$ and that $G \leq A$ is minimal transitive on vertices. Then $r(r + 1)/2$ divides $|G|$ and it follows that $G = PSL(2, r)$. Then the stabilizer in G of an external point P is D_{r-1}, which is maximal in G (by [9]) unless r is 7, 9, or 11 (when D_{r-1} is contained in S_4, S_4, or A_5 respectively). If $r(r + 1)/2 = 2pq$ then $pq = r(r+1)/4$ and, since r is odd, 4 divides $r+1$. Thus $p = r$, $q = (r+1)/4$ and (d) follows. □

We thank Andries Brouwer for drawing to our attention the construction of $Ext(r)$. We note that $Ext(7)$ is the Coxeter graph, see [3, p. 382]. This construction gives a family of vertex-transitive, non-Cayley graphs of order $2pq$ where $p = 4q - 1$. From Proposition 2.2 it follows that the only graph in this family which has order $2pq$ ($2 < q < p$, q and p primes) and admits a transitive imprimitive group of automorphisms is $Ext(11)$ of order 66. Using the computer packages CAYLEY [6], GAP [28], Nauty [18] and GRAPE [29], we investigated the graph $Ext(11)$ and showed that it has the distance diagram (see [3, 2.9]) depicted in Figure 1. Here each circle represents an orbit of the subgroup H of automorphisms of $Ext(11)$ fixing a given vertex. The size of an H-orbit Δ is written in the corresponding circle $C(\Delta)$. For a vertex $\delta \in \Delta$ and an H-orbit Δ' (which may or may not be equal to Δ) the number n of vertices of Δ' adjacent to δ is independent of the choice of δ in Δ; this number n is indicated in Figure 1 by a directed edge from $C(\Delta)$ to $C(\Delta')$ labeled n.

There is an alternative construction of $Ext(11)$ obtained from the $2-(11, 5, 2)$ design, which was pointed out to us by A.A. Ivanov. The action in this case is on antiflags (that is nonincident point-line pairs) of the design.

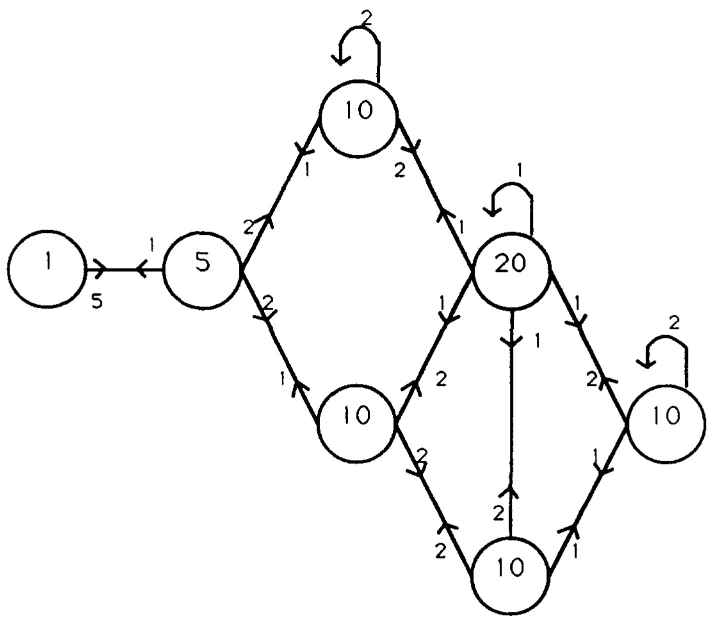

Fig. 1. Distance diagram.

3. Some minimal transitive groups and their graphs

In our analysis of this problem we had to deal with several families of minimal transitive permutation groups of degree $2pq$. One such family led to Construction 2.1 of a family of non-Cayley vertex-transitive graphs. Two other similar families arose, and for them all related generalized orbital graphs turned out to be Cayley graphs. The results of analyzing these groups will be required at several places in our proof and so we give the analyses here. The basic strategy in showing that the graphs are Cayley graphs is to prove that they have additional automorphisms to those in the given group G. The smallest members of the families of minimal transitive permutation groups arising in connection with Construction 2.1, and Propositions 3.1 and 3.2 below, were examined using GAP and GRAPE [28, 29]. This gave us the insights necessary to construct both the non-Cayley graphs of Construction 2.1, and the extra automorphisms of Propositions 3.1 and 3.2. The following result gives conditions under which the existence of such extra automorphisms may be inferred. It may be regarded as a generalization of Wielandt's dissection theorem [33, Theorem 6.5].

LEMMA 3.1. *Let $\Gamma = (V, E)$ be a finite graph, and let $\{U, W_1, \ldots, W_t\}$ be a partition of V, where $t \geq 1$. Let H be a subgroup of Aut Γ which fixes each of $U, W_1, \ldots, W_t$ setwise, and such that, for each H-orbit $U' \subseteq U$, U' is trivially joined to each of $W_1, W_2, \ldots, W_t$. Then H^U (the group which fixes $V \backslash U$ pointwise and which induces the same permutation group of U as H does) is a subgroup of AutΓ.*

Proof. Consider three types of edges in Γ; those that lie within U, those that lie outside U, and those that have one point inside U and one point outside U. An edge of the first type is sent to an edge of the same type by H^U since $H \leq$ Aut Γ and H fixes U setwise. An edge of the second type is fixed by H^U as H^U fixes all points not in U. Finally let e be an edge of the third type. Then e is an edge of the form $\{v, v'\}$ where $v \in U$ and $v' \in W_i$ for some $0 < i \leq t$. Since v^H and W_i are trivially joined, $\{v, v'\}^h$ is an edge for all $h \in H^U$. Hence $H^U \leq$ Aut Γ. □

We assume throughout the remainder of this section that p and q are distinct odd primes.

PROPOSITION 3.1. *Suppose that Γ is a graph of order $2pq$ admitting the following group G as a vertex-transitive group of automorphisms: $G = \langle a, b, c, x\rangle$ where $a^q = b^q = c^p = x^4 = [a, b] = [a, c] = [b, c] = 1$, and also $a^x = b$, $b^x = a^{-1}$, $c^x = c^\delta$ for $\delta = +1$ or -1. Suppose that the action of G is such that, for some $\alpha \in V$, $G_\alpha = \langle b, x^2\rangle$. Then Γ is a Cayley graph.*

Proof. As in Construction 2.1 we may identify the set of points V with the right transversal $T = \langle a, c\rangle \cup \langle a, c\rangle x$ of G_α in G such that $\alpha = 1$, and the actions of the generators a, b, c, x, and the element x^2 on the points are given as follows: (note that $xa = b^{-1}x$ and $xb = ax$)

$$\begin{aligned}
a &: a^ic^j \to a^{i+1}c^j, && : a^ic^jx \to a^ic^jx\\
b &: a^ic^j \to a^ic^j, && : a^ic^jx \to a^{i+1}c^jx\\
c &: a^ic^j \to a^ic^{j+1}, && : a^ic^jx \to a^ic^{j+\delta}x\\
x &: a^ic^j \to a^ic^jx, && : a^ic^jx \to a^{-i}c^j\\
x^2 &: a^ic^j \to a^{-i}c^j, && : a^ic^jx \to a^{-i}c^jx.
\end{aligned}$$

The set of orbits of the normal subgroup $L = \langle a, b\rangle$ of G is a block system for $G : \Sigma = B_0^G$ where $B_0 = \alpha^L$. It consists of $2p$ blocks of size q, namely $B_j = (c^j)^L = \{a^ic^j | i \in Z_q\}$, and $C_j = (c^jx)^L = \{a^ic^jx | i \in Z_q\}$, for $j \in Z_p$.

The G_α-orbits in B_0 are $\Delta_{\pm i,0}(\alpha) = (a^i)^{G_\alpha} = \{a^i, a^{-i}\}$, for $i \in Z_q$. Since

a^{-i} sends the pair $(1, a^i)$ to $(a^{-i}, 1)$, these orbits are self-paired. Also, since $c^{-j}a^{-i} : (1, a^ic^j) \to (c^{-j}a^{-i}, 1) = (a^{-i}c^{-j}, 1)$, the G_α-orbit $\Delta_{\pm i,j}(\alpha) = \{a^ic^j\}^{G_\alpha} = \{a^ic^j, a^{-i}c^j\}$ in B_j is paired to the G_α-orbit $\Delta_{\pm i,-j}(\alpha) = \{a^{-i}c^{-j}, a^ic^{-j}\}$ in B_{-j}. Furthermore $x^{-1}c^{-j}a^{-i}$ maps $(1, a^ic^jx)$ to $(c^{-j\delta}x, 1)$ since $x^{-1}c^{-j}a^{-i} = x^2b^ic^{-j\delta}x$ is in the same G_α-coset as $c^{-j\delta}x$. Hence the G_α-orbit $(a^ic^jx)^{G_\alpha} = \{a^{\pm i+t}c^jx \mid t \in Z_q\} = C_j$ is paired with the G_α-orbit $C_{-\delta j}$ for each $j \in Z_p$.

Any graph Γ with vertex set V admitting G is a generalized orbital graph for G and the set $\Gamma(\alpha)$ is a union of G_α-orbits in $V\backslash\{\alpha\}$ closed under pairing. Hence

$$\Gamma(\alpha) = \bigcup_{j\in Z_p}\left(\bigcup_{i\in I_j}\Delta_{\pm i,j}(\alpha)\right)\bigcup_{j\in J}C_j$$

for some $I_j \subseteq Z_q$, for $j \in Z_p$, and for some $J \subseteq Z_p$, where $0 \notin I_0$ (since there are no loops in Γ), $I_j = -I_j = \{i|i \in I_j\} = I_{-j}$, for all $j \in Z_p$, and $J = -J$ (since Γ is undirected).

Now we apply Lemma 3.1 to the partition $\{U = \cup_{i\in Z_p}B_i, C_0, C_1, \dots, C_{p-1}\}$ and the group $H = \langle x^2\rangle$. The H-orbits in U are the sets $\{a^ic^j, a^{-i}c^j\}$ for $i, j \in Z_q$. Suppose there is an edge e from a^ic^j to a point $a^{i'}c^{j'}x$ in $C_{j'}$. Then $e^{c^{-j}a^{-i}} = \{1, a^{i'}c^{j'-j\delta}x\}$ is also an edge, that is $j' - j\delta \in J$. It follows that $e'' = \{1, a^{i''}c^{j'-j\delta}x\}$ is an edge and hence that $(e'')^{a^{\pm i}c^j} = \{a^{\pm i}c^j, a^{i''}c^{j'}x\}$ is an edge for all $i'' \in Z_q$. It follows that each H-orbit $\{a^ic^j, a^{-i}c^j\}$ in U is trivially joined to each $C_{j'}$. By Lemma 3.1, $\sigma = (x^2)^U \in \mathrm{Aut}\,\Gamma$. By considering the actions of a^σ, b^σ, c^σ, and x^σ on V, $a^\sigma = a^{-1}$, $b^\sigma = b$, $c^\sigma = c$, and $x^\sigma = x^{-1}$. It is straightforward to check that $x\sigma$ is an involution and $\langle ab, c, x\sigma\rangle$ is regular on V, so Γ is a Cayley graph. □

PROPOSITION 3.2. *Suppose that Γ is a graph of order $2pq$ admitting the following group G (of order 2^apq) as a vertex-transitive group of automorphisms: $G = \langle x_1, x_2, \dots, x_a, y\rangle$ where $y^{pq} = x_i^2 = 1$ for $i = 1, \dots, a$; and where $[x_i, x_j] = 1$, $i \neq j$. If y normalizes $S = \langle x_1, x_2, \dots, x_a\rangle \cong Z_2^a$ but y normalizes no proper nontrivial subgroup of S, then Γ is a Cayley graph.*

Proof. As G acts transitively on the set V of $2pq$ vertices we may assume the $G_\alpha = \langle x_2, x_3, \dots, x_a\rangle = H$ for some vertex $\alpha \in V$. As in Construction 2.1, there is a one-to-one correspondence between V and the right transversal $T = \langle y\rangle \cup x_1\langle y\rangle$ of H in G, such that $\alpha = 1$ and the action of G on the points is equivalent to the action of G by right multiplication on the set of right cosets $\{Ht \mid t \in T\}$. Since $S = \langle x_1, \dots, x_a\rangle$ is a normal subgroup of G, for each $x \in S$ we have $y^jx \in y^jS = Sy^j$. Hence $y^jx = x_1^{\varepsilon_1}x_2^{\varepsilon_2}\cdots x_a^{\varepsilon_a}y^j \in Hx_1^{\varepsilon_1}y^j$ for some $\varepsilon_1, \varepsilon_2, \dots, \varepsilon_a \in Z_2$ depending on x and on j. So the actions of the generators x_k (for $1 \leq k \leq a$), and y on the points are given as follows:

$$x_k : y^j \to x_1^{\varepsilon(j,k)y^j}, \quad x_1 y^j \to x_1^{\varepsilon(j,k)+1} y^j$$
$$y : y^j \to y^{j+1}, \qquad x_1 y^j \to x_1 y^{j+1}$$

Consider the pair of points $C_j = \{y^j, x_1 y^j\}$. An element of G has the form xy^s where $x \in S = Z_2^a$ and $0 \leq s \leq pq - 1$. Every element of S either swaps the points y^j and $x_1 y^j$ or fixes them. Therefore $\{y^j, x_1 y^j\}^{xy^s} = \{y^{j+s}, x_1 y^{j+s}\} = C_{j+s}$ (taking the subscript modulo pq), and hence $\Delta = \{C_j \mid 0 \leq j \leq pq-1\}$ is a system of blocks of imprimitivity for G. As in Proposition 3.1, the graph Γ admitting G on the set of points V is determined by $\Gamma(\alpha)$, a union of G_α-orbits closed under pairing.

Suppose that j is such that $1 \leq j \leq pq - 1$ and $y^j \notin N_G(H)$. Then there are elements h_1 and h_2 in H such that $\hat{h}_1 := y^j h_1 y^{-j} \notin H$ and $\hat{h}_2 := y^{-j} h_2 y^j \notin H$. Since S is normal in G, $\hat{h}_1, \hat{h}_2 \in S \backslash H$.

Consider the pair of blocks $C_j = \{y^j, x_1 y^j\}$ and $C_{j'} = \{y^{j'}, x_1 y^{j'}\}$ and suppose that $y^{j'-j}$ does not normalize H. Then $C_j \neq C_{j'}$. Now suppose that there is an edge between C_j and $C_{j'}$, say $\{x_1^{\delta_1} y^j, x_1^{\delta_2} y^{j'}\} \in E$ for some $\delta_1 = 0$ or 1 and $\delta_2 = 0$ or 1. Now from the above, since $y^{j'-j}$ does not normalize H, there exist elements $h_1, h_2 \in H$ and $\hat{h}_1, \hat{h}_2 \in S \backslash H$ such that $y^{j'-j}\hat{h}_2 = h_2 y^{j'-j}$ and $\hat{h}_1 y^{j'-j} = y^{j'-j} h_1$. Hence $\{x_1^{\delta_1} y^j, x_1^{\delta_2} y^{j'}\}^{y^{-j}\hat{h}_2 y^j} = \{x_1^{\delta_1}, x_1^{\delta_2} y^{j'-j}\}^{\hat{h}_2 y^j} = \{x_1^{\delta_1+1}, x_1^{\delta_2} h_2 y^{j'-j}\}^{y^j}$ (since $\hat{h}_2$ does not fix $\alpha = 1$ or x_1) $= \{x_1^{\delta_1+1} y^j, x_1^{\delta_2} y^{j'}\} \in E$. Similarly $\{x_1^{\delta_1+\varepsilon} y^j, x_1^{\delta_2} y^{j'}\}^{y^{-j} h_1 y^j} = \{x_1^{\delta_1+\varepsilon} y^j, x_1^{\delta_2+1} y^{j'}\} \in E$, for $\varepsilon = 0$ or 1. It follows that C_j and $C_{j'}$ are trivially joined whenever $y^{j'-j}$ does not normalize H.

Suppose that, for all $1 \leq j \leq pq - 1$, y^j does not normalize H. Then every pair of distinct blocks are trivially joined. It follows that Γ is the lexicographic product $\Gamma_\Delta[\overline{C}_j]$, which is a Cayley graph since both the quotient Γ_Δ and $\overline{C}_j$ admit regular groups of automorphisms.

Suppose on the other hand that, for some j where $1 \leq j \leq pq-1$, y^j normalizes H. Since H is not normal in G, H is not normalized by y^k for any k coprime to pq. It follows that y^j has order p or q. We may assume, without loss of generality, that y^j has order q and we may take $j = p$. Then, since y does not normalize H, no element of $\langle y \rangle$ of order p normalizes H. Now $H < \langle S, y^p \rangle < G$. Define D_0 to be the $\langle S, y^p \rangle$-orbit containing $\alpha = 1$. Then D_0 is a block of imprimitivity for G in V of size $2q$, and is the union of the q blocks C_{rp} for $0 \leq r < q$. Also, for $i = 1, 2, \ldots p - 1$, set $D_i = D_0^{y^i}$. Then D_i is the union of the q blocks C_{rp+i}, for $0 \leq r < q$. For all $0 < i < p$, and $0 \leq k, l < q$, $y^{(lp+i)-kp}$ has order divisible by p and so does not normalize H. Hence C_{kp} and C_{lp+i} are trivially joined, that is every S-orbit in D_0 is trivially joined to each C_{lp+i} for $0 < i < p$ and $0 \leq l < q$. By Lemma 3.1 applied to the partition $\{U = D_0, C_{lp+i},$ for $0 < i < p$, $0 \leq l < q\}$ and the group S, it follows that $S^{D_0} \leq \operatorname{Aut} \Gamma$.

Now H fixes C_0 pointwise and, as y^p normalizes H, y^p permutes the points fixed by H amongst themselves. Hence H fixes D_0 pointwise and therefore S^{D_0} has order 2. It follows that $S^{D_i} = \langle \zeta_i \rangle \simeq Z_2$, and is contained in $\operatorname{Aut} \Gamma$, for $i = 0, 1, \dots p-1$. Hence Aut $\Gamma \geq \prod_{i=0}^{p-1} S^{D_i} = Z_2^p$. Now $\zeta_i^y = \zeta_{i+1}$ for $i = 0, 1, \dots p-1$, and $\zeta_{p-1}^y = \zeta_0$. Hence $(\zeta_0\zeta_1 \cdots \zeta_{p-1})^y = (\zeta_0\zeta_1 \cdots \zeta_{p-1})$ and it follows that $\langle \zeta_0\zeta_1 \cdots \zeta_{p-1}, y\rangle$ is regular on V. Hence Γ is a Cayley graph. □

4. Permutation groups related to primitive groups of degrees p or pq

In this section we prove some technical results which are needed in the proof of Theorem 2.

LEMMA 4.1. *Suppose that p and q are distinct primes such that $p \equiv q \equiv 3 (mod\ 4), p \not\equiv 1 (mod\ q)$ and $q \not\equiv 1 (mod\ p)$, and such that $pq \notin NC$. Then if G is a primitive group of degree pq and G has socle T, G is 2-transitive and one of the following holds:*

(i) $T = A_{pq}$.
(ii) *$T = PSL_m(r)$ on the points or hyperplanes of the projective space $PG_{m-1}(r)$, $pq = (r^m - 1)/(r - 1)$, where m is prime or the square of a prime, and $(m, r) \neq (2, 2), (2, 3)$.*

Proof. Suppose, without loss of generality, that $p > q$. The primitive groups of degree kp, p a prime and $k < p$, were classified by Liebeck and Saxl in [16]. (Those groups which are primitive but not 2-transitive of degree qp, p a prime greater than q, were extracted from the lists in [16] and then listed in [26, table IV] and [31, Lemma 2.1] (where $q > 3$ and $q = 3$ respectively).) There are no examples with $p \equiv q \equiv 3$ (mod 4), $p \not\equiv 1$ (mod q) and $pq \notin$ NC. Hence G is 2-transitive and T is therefore one of those groups listed in [4, Theorem 5.3].

Suppose that $PSU_3(r) \leq G \leq P\Gamma U_3(r)$ with $pq = r^3 + 1$. Then, since $p > q$, $q = r + 1$ and $p = r^2 - r + 1$. Since $q \equiv 3 (\text{mod } 4)$, it follows that $r \equiv 2 (\text{mod } 4)$ and so, since r is a prime power, $r = 2$. But then $p = q = 3$, which is a contradiction.

It now follows from [4, Theorem 5.3] that the only examples of degree pq, where $p \equiv q \equiv 3 (\text{mod } 4)$ are as in (i) or (ii) above, and we need to obtain the restrictions on m and r in case (ii). Certainly $(m, r) \neq (2, 2)$or $(2, 3)$.

If m_1 divides m, then $(r^{m_1}-1)/(r-1)$ divides $(r^m-1)/(r-1)$. If m were divisible by two distinct primes m_1 and m_2 say, then $(r^{m_1} - 1)/(r - 1).(r^{m_2} - 1)/(r - 1)$ would be a proper divisor of $(r^m - 1)/(r - 1)$ which is not possible. So $m = m_1^a$ for some prime m_1. If $a \geq 3$ then $(r^{m_1^2} - 1)/(r^{m_1} - 1).(r^{m_1} - 1)/(r - 1)$ would be a proper divisor of $(r^m - 1)/(r - 1)$. Hence $a \leq 2$. □

LEMMA 4.2. *Suppose that p and q are primes such that $p \equiv q \equiv 3$ (mod 4), $p \not\equiv 1$ (mod q) and $q \not\equiv 1$ (mod p), and such that $pq \notin NC$. Suppose also that $G \leq Sym(V)$ is transitive with $|V| = p$ and G has socle T.*

(a) *If q divides the order of G then T is nonabelian.*

(b) *If T is nonabelian then T is one of the following groups:*
  (i) A_p,
  (ii) $PSL_m(r)$ *where* $p = (r^m - 1)/(r - 1)$,
  (iii) $PSL_2(11)$ *or* M_{11} *with* $p = 11$, *or*
  (iv) M_{23} *with* $p = 23$.

(c) *Suppose that T is nonabelian. If G_x, where $x \in V$, has a subgroup H of index 2 and no proper subgroup of G is transitive on the coset space $[G : H]$, then $T = M_{11}$ with $p = 11$, or $PSL_m(r)$ where $p = (r^m - 1)/(r - 1)$.*

(d) *If G_x, where $x \in V$, has a subgroup of index q, or G_x has a subgroup H of index 2, which in turn has a subgroup of index q, then $T = PSL_m(r)$ and $p = (r^m - 1)/(r - 1)$.*

Proof.

(a) If T is abelian then $G \leq Z_p.Z_{p-1}$ and, since q divides the order of G, q divides $p - 1$, which is a contradiction. Hence T is nonabelian.

(b) If T is nonabelian then, by [13], T is one of the groups listed in (b).

(c) If $G \cong S_p$, then $G_x \cong S_{p-1}$ and $H \cong A_{p-1}$. Let $R = Z_p.Z_{p-1} \leq G$. Then $R_x = Z_{p-1}$ is not a subgroup of A_{p-1} and so R is transitive on $[G : H]$ which is a contradiction. If $G = A_p$, $PSL_2(11)$ or M_{23} then $G_x = A_{p-1}$, A_5 or M_{22}, none of which has a subgroup of index 2. Hence by (b), G is either M_{11}, with $p = 11$, or $PSL_m(r) \leq G \leq P\Gamma L_m(r)$ with $p = (r^m - 1)/(r - 1)$.

(d) Since q divides $|G|$, T is nonabelian by (a) and T is one of the groups listed in (b). As pq divides $|G|$ and $p \equiv q \equiv 3 \pmod 4$, $p \neq q$, it follows that $p \geq 7$. Suppose that G_x has a subgroup of index q. If $G = A_p$ or S_p, M_{11}, $PSL_2(11)$ or M_{23} then G_x has no subgroup of index q unless $G = PSL_2(11)$ and $q = 5$ in which case $q \not\equiv 3 \pmod 4$. Hence $T = PSL_m(r)$. Suppose instead that G_x has a subgroup H of index 2 such that H has a subgroup of index q. If $G = A_p$, $PSL_2(11)$ or M_{23} then G_x has no subgroup of index 2. If $G = S_p$ or M_{11} then the subgroup of G_x of index 2 has no subgroup of index q. Hence $T = PSL_m(r)$. □

LEMMA 4.3. *Suppose that p and q are primes such that $p \equiv q \equiv 3 \pmod 4$. Let $p = (r^m - 1)/(r - 1)$ with r a power of a prime r_0 and $m \geq 2$.*

(a) *Then m is prime and $r = r_0^{m^c}$ for some $c \geq 0$. Further, either $p = r + 1 = 3$, or $m \geq 3$.*

(b) *If there is a subgroup $G \leq S_{2p}$ such that pq divides $|G|$, then $m \geq 3$, and if $m = 3$ then $r \equiv 1 \pmod 4$.*

(c) *If G is as in (b) and is a subgroup of $P\Gamma L_m(r)$ wr S_2 or S_2 wr $P\Gamma L_m(r)$ acting imprimitively of degree $2p$, then the group $PSL_{m-1}(r)$ is a nonabelian simple group and has no subgroup of index q.*

Proof.

(a) For any divisor $a > 1$ of $m, (r^a - 1)/(r - 1) > 1$ divides p whence $p = (r^a - 1)/(r - 1)$ and $a = m$. Thus m is prime. Suppose that $r = r_0^{sb}$ where m does not divide s and $b \geq 1$, $s \geq 1$. Then $r_0^{bm} - 1$ divides $r^m - 1 = r_0^{sbm} - 1$ and the greatest common divisor of $r_0^{bm} - 1$ and $r - 1$ is equal to $r_0^{(bm, bs)} - 1$ which equals $r_0^b - 1$. Thus $(r_0^{bm} - 1)/(r_0^b - 1) > 1$ divides p, whence $(r_0^{bm} - 1)/(r_0^b - 1) = p$. But $2r_0^{b(m-1)} > (r_0^{bm} - 1)/(r_0^b - 1) = (r^m - 1)/(r - 1) > r^{m-1} = r_0^{bs(m-1)}$ so $b(m-1) \geq bs(m-1)$, that is $s = 1$. Hence $r = r_0^{m^c}$, for some $c \geq 0$. If $m = 2$ then $p = r + 1 \equiv 3 \pmod 4$, so $r = 2$, $p = 3$.

(b) If $m = 2$ then, by (a), $G \leq S_6$. But $|G|$ is not divisible by any $q \neq p$ with $q \equiv 3 \pmod 4$. Hence $m \geq 3$. If $m = 3$ then $p = 1 + r + r^2 \equiv 3 \pmod 4$ so $r(r + 1) \equiv 2 \pmod 4$. So either $r = 2$ or $r \equiv 1 \pmod 4$. However if $r = 2$ then $p = 7$ and the only odd prime $q \neq 7$ dividing $|G|$ is $q = 3$ which contradicts the fact that $p \not\equiv 1 \pmod q$.

(c) By (b) it follows that $PSL_{m-1}(r)$ is a nonabelian simple group. Suppose that $PSL_{m-1}(r)$ has a subgroup of index q. Since q divides $|PSL_{m-1}(r)|$, $q \leq (r^{m-1} - 1)/(r - 1)$. If $PSL_{m-1}(r)$ has minimal degree (that is minimum index of a proper subgroup) $(r^{m-1} - 1)/(r - 1)$ then $q = (r^{m-1} - 1)/(r - 1)$. As in the proof of (a), $m - 1$ is prime and, as m is also prime, $m = 3$. Hence $q = r + 1 \equiv 3 \pmod 4$, whence $r \equiv 2 \pmod 4$, contradicting (b). Thus the minimal degree of $PSL_{m-1}(r)$ is less than $(r^{m-1} - 1)/(r - 1)$ whence $(m - 1, r) = (2, 5), (2, 7), (2, 9), (2, 11)$, or $(4, 2)$ (see [8], [9] or [11]). Moreover since $PSL_{m-1}(r)$ has a subgroup of odd prime index $q \equiv 3 \pmod 4$, $q < (r^{m-1} - 1)/(r - 1)$, $(m - 1, r)$ is $(2, 7)$ or $(2, 11)$. In either case $p = 1 + r + r^2$ is not prime. Hence $PSL_{m-1}(r)$ has no subgroup of index q. □

LEMMA 4.4. *Let $m \geq 3$, and $k = (r^m - 1)/(r - 1)$ for some prime power r, and suppose that the group $G = PSL_m(r)$ acts imprimitively on a set V of points where $|V| = tk$ for some $t > 1$. Suppose that G has a set $\Sigma = \{B_1, B_2, \dots, B_k\}$ of k blocks of size t, which G permutes as the 1-spaces of an m-dimensional vector space $V_m(r)$ over $GF(r)$, and suppose that $G_\alpha \geq [Z_r^{m-1}].SL_{m-1}(r)$, for $\alpha \in B \in \Sigma$. Then G_α is transitive on $V \backslash B$.*

Proof. We may choose $B = \langle e_1 \rangle$ where $e_1 = (1, 0, \dots, 0)$. Consider $H = SL_m(r)$, the preimage of G in $GL_m(r)$, and for $A \in H$ let $\overline{A}$ denote the corresponding element of G. Then A fixes B (or $\overline{A} \in G_B$) if and only if

$$A = \begin{bmatrix} a_1 & \underline{0} \\ \underline{a}_2 & A_1 \end{bmatrix}$$

where $a_1 \det A_1 = 1$. Since, for $\alpha \in B$, $G_\alpha \geq [Z_r^{m-1}].SL_{m-1}(r)$, the preimage H_α of G_α in H contains all matrices of the form

$$\begin{bmatrix} 1 & \underline{0} \\ \underline{a}_2 & A_1 \end{bmatrix}$$

with det $A_1 = 1$. It follows that, for $\overline{A} \in G_B$, $\overline{A} \in G_\alpha$ if and only if

$$A = \begin{bmatrix} a_1 & \underline{0} \\ \underline{a}_2 & A_1 \end{bmatrix}$$

with a_1 belonging to the subgroup L of order $(r-1)/t$ of the multiplicative group of $GF(r)$. Clearly G_α is transitive on $\Sigma \backslash \{B\}$ and, for $B' = \langle e_2 \rangle$ where $e_2 = (0, 1, \ldots, 0)$, the preimage of $G_{\alpha, B'}$ in H contains all matrices of the form

$$\begin{bmatrix} a_1 & 0 & \underline{0} \\ a_2 & a_3 & \underline{0} \\ \underline{a}_4 & \underline{a}_5 & A_1 \end{bmatrix}$$

where $a_1 \in L$ and $a_1 a_3 \det A_1 = 1$. It follows that $G_{\alpha, B'}$ is transitive on B' and hence G_α is transitive on $V \backslash B$. □

5. Proof of Theorem 2: A preliminary analysis.

In this section we begin the proof of Theorem 2. Let $\Gamma = (V, E)$ be a vertex-transitive non-Cayley graph of order $2pq$, where p and q are distinct odd primes, and p, q are such that all vertex-transitive graphs of order pq are Cayley graphs. It will be convenient in the proof to allow either of q, p to be the larger prime so we shall assume

$$p \equiv q \equiv 3 (\text{mod } 4), \quad p \not\equiv 1 (\text{mod } q) \text{ and } q \not\equiv 1 (\text{mod } p).$$

Suppose that there is a subgroup G of Aut Γ which is transitive and imprimitive on V. We may assume that G is *minimal transitive* on V, that is, that every proper subgroup of G is intransitive on V. Then there is a G-invariant partition $\Sigma = \{B_1, B_2, \ldots, B_r\}$ of V with $1 < |\Sigma| < 2pq$. Choose Σ such that the only proper refinement of Σ which is G-invariant is the trivial partition with $2pq$ parts of size 1. A consequence of this is that the setwise stabilizer G_B of a block $B \in \Sigma$ is primitive on B. This is true since G_B must be transitive on B and, if $\{C^g | g \in G_B\}$ is a G_B-invariant partition of B with $1 < |C| < |B|$ then $\{C^g | g \in G\}$ would be a G-invariant partition of V which is a proper refinement of Σ.

Associated with Σ are (up to isomorphism) two graphs smaller than Γ, namely the quotient graph Γ_Σ and the induced subgraph $\overline{B}$, as defined in Section 1. First we show that Γ is not a lexicographic product $\Gamma_\Sigma[\overline{B}]$ of $\overline{B}$ by Γ_Σ.

LEMMA 5.1. *The graph Γ is not isomorphic to the lexicographic product $\Gamma_\Sigma[\overline{B}]$ of the subgraph $\overline{B}$ induced on $B \in \Sigma$ by the quotient graph Γ_Σ.*

Proof. Suppose that $\Gamma \cong \Gamma_\Sigma[\overline{B}]$. Since both $|B|$ and $|\Sigma|$ are proper divisors of $2pq$, $\overline{B}$ and Γ_Σ are Cayley graphs by our assumptions about p and q, and hence Γ is a Cayley graph, which is a contradiction. □

This lemma has certain consequences for the structure of G. Let $K = G_{(\Sigma)}$ be the subgroup of G fixing each block of Σ setwise, and for $B \in \Sigma$ let $K_{(B)}$ denote the subgroup of K fixing B pointwise. The *complementary graph* Γ^c of Γ is the graph with vertex-set V such that $\{\alpha, \beta\}$ is an edge of Γ^c if and only if $\{\alpha, \beta\} \notin E$.

LEMMA 5.2.

(a) *If $K \neq 1$ then K is transitive on each block of Σ. The group $K_{(B)}$ fixes pointwise s blocks of Σ, where $s \geq 2$ and s divides $|\Sigma|$, and is transitive on the remaining blocks, if any, of Σ.*
(b) *The complementary graph Γ^c is connected.*

One consequence of part (b), since Aut Γ^c = Aut Γ, is that we may replace Γ by Γ^c whenever it is helpful for the proof.

Proof.

(a) Suppose that $K \neq 1$. Then the set of K-orbits is a G-invariant partition of V which is a refinement of Σ. Since Σ has no proper nontrivial G-invariant refinements, K is transitive on B. If $|B|$ is prime then K is primitive on each $B \in \Sigma$. On the other hand, if $|B|$ is not prime then r is prime. It follows from the minimality of G that $G/K \cong Z_r$. Hence, for each $C \in \Sigma$, $G_C = K$ is primitive on C. If $K_{(B)} = 1$ then the rest of part (a) follows so assume that $K_{(B)} \neq 1$ and let $C \in \Sigma\backslash\{B\}$ be a block on which $K_{(B)}$ acts nontrivially. Then, since $K_{(B)}^C$ is normal in the primitive group K^C, $K_{(B)}$ must be transitive on C. So $K_{(B)}$ fixes pointwise s, say, blocks of Σ and is transitive on the remaining blocks of Σ.
It is straightforward to show that the set F of fixed points of $K_{(B)}$ in V is a block of imprimitivity for G in V, and hence that s divides $|\Sigma|$. If $s = 1$ then $K_{(B)}$ is transitive on each block of $\Sigma\backslash\{B\}$. If $\{B, C\}$ is an edge of the quotient graph Γ_Σ then for some $\alpha \in B$, $\beta \in C$, $\{\alpha, \beta\} \in E$. It follows that for all $g \in K_{(B)}$, $\{\alpha, \beta\}^g = \{\alpha, \beta^g\} \in E$ and consequently that α is joined to every point of C. Similarly, $K_{(C)}$ is transitive on B and hence β is joined to every point of B. It follows that Γ is isomorphic to $\Gamma_\Sigma[\overline{B}]$, contradicting Lemma 5.1. Hence $s \geq 2$.
(b) If Γ^c is not connected then it has t connected components of size u say where $tu = 2pq$, $t > 1$, $u > 1$ (since Γ being a non-Cayley graph is not K_{2pq}). Thus, since u is a proper divisor of $2pq$, a connected component C of Γ^C

is a Cayley graph. Thus, since Aut Γ = Aut Γ^c contains Aut $C\,wr\,S_t$, Γ is also a Cayley graph, which is a contradiction. □

This completes the preliminary analysis. Following a sensible suggestion of one of our referees, we give here a summary of the notation introduced in this section (and in section 1) which will be used in the remainder of this section and in the next three sections.

System of blocks of imprimitivity:	$\Sigma = \{B_1, \ldots B_r\}$
Permutation group induced by G on Σ:	G^Σ
Setwise stabilizer of $B \in \Sigma$ in G:	G_B
Subgroup of G fixing each B_i setwise:	$K = G_{(\Sigma)} = \cap_{1\le i\le r} G_{B_i}$
Permutation group induced by G_B, K on $B \in \Sigma$:	G_B^B, K^B
Stabilizer of $\alpha \in V$ in G:	G_α
Pointwise stabilizer of $B \in \Sigma$ in G, K:	$G_{(B)}$, $K_{(B)}$
Subgraph induced on B:	$\overline{B}$
Set of vertices adjacent to α:	$\Gamma_1(\alpha)$
Quotient graph of Γ modulo Σ:	Γ_Σ
Complementary graph of Γ:	Γ^c
Lexicographic product of Γ_2 by Γ_1:	$\Gamma_1[\Gamma_2]$
Set of points of V fixed by $H \le G$ or $g \in G$:	$\mathrm{fix}_V(H)$ or $\mathrm{fix}_V(g)$
Socle of a group H:	$\mathrm{soc}(H)$

In the remainder of this section we deal with the simplest case where $|\Sigma| = 2$. Clearly we may assume in this case that $q < p$, and we write $\Sigma = \{B, C\}$.

PROPOSITION 5.1. *There are no examples with* $|\Sigma| = 2$.

We prove Proposition 5.1 essentially by a sequence of lemmas. Let $\alpha \in B$. Since Γ is connected, $\Gamma_1(\alpha) \cap C$ is nonempty; let $\beta \in \Gamma_1(\alpha) \cap C$.

LEMMA 5.3. *If* $\alpha \in B$ *then* K_α *has at least two orbits in* C.

Proof. The set $\Gamma_1(\alpha) \cap C$ is nonempty, and by Lemma 5.1 is a proper subset of C. Since it is fixed setwise by K_α it follows that K_α has at least two orbits in C. □

LEMMA 5.4. *The group* K *is not 2-transitive on* B.

Proof. Suppose that K is 2-transitive on B and hence on C. By Lemma 5.3, K_α is intransitive on C, and, since the number of K_α-orbits in C is equal to the inner product of the permutation characters for K on B and on C, it follows that K_α has exactly two orbits in C and $\Gamma_1(\alpha)\cap C$ is one of them. Moreover, K_α is transitive on $B\backslash\{\alpha\}$ and so α is joined to all or none of the points of $B\backslash\{\alpha\}$.

Replacing Γ by Γ^c if necessary (as we may by Lemma 5.2) we may assume that α is joined to no points of B, so $\Gamma_1(\alpha) \subseteq C$. If the actions of K on B and C are equivalent then K_α fixes a point α' in C and is transitive on $C\backslash\{\alpha'\}$. Since Γ is connected, $\Gamma_1(\alpha) \neq \{\alpha'\}$, and so $\Gamma_1(\alpha) = C\backslash\{\alpha\}$ and Γ is isomorphic to the complete bipartite graph $K_{pq,pq}$ with the edges of a matching removed. However in that case Aut $\Gamma = S_{pq} \times Z_2$ contains a subgroup $Z_{pq} \times Z_2$ regular on V which is a contradiction. It follows that the actions of K on B and C are inequivalent. The only 2-transitive groups of degree pq with two inequivalent 2-transitive representations of degree pq, $p \equiv q \equiv 3 (\mathrm{mod}\ 4)$, are the projective groups $PSL_n(r) \leq K \leq P\Gamma L_n(r)$, $pq = (r^n - 1)/(r - 1)$, $n \geq 3$. Here B can be identified with the points and C with the hyperplanes of the projective geometry $PG_{n-1}(r)$. Moreover for a hyperplane β, $\Gamma_1(\beta)$ is either the set of points incident with β or the set of points not incident with β, as these are the two orbits of K_β in B. In either case Aut $\Gamma \geq$ Aut $PSL_n(r)$ and hence Aut Γ contains a subgroup R regular on V; for example R can be taken as a cyclic subgroup of $PGL_n(r)$ of order $(r^n - 1)/(r - 1)$ (a so-called Singer cycle) acting regularly on the points and hyperplanes of $PG_{n-1}(r)$ extended by a polarity interchanging points and hyperplanes. Hence K is not 2-transitive on B or C. □

Completion of Proof of Proposition 5.1. Now $K = G_B$ and so K^B is primitive of degree pq. Also $K_{(B)} = 1$ by Lemma 5.2 and hence $K \simeq K^B$. By Lemma 5.4, K is not 2-transitive on B. By Lemma 4.1 there are no primitive groups of degree pq satisfying these conditions, which is a contradiction. □

Thus $|\Sigma| > 2$. We shall examine the cases where $|\Sigma|$ is an odd prime or the product of two primes in the next sections.

6. The case $|\Sigma| = q$

Next we treat the case where $|\Sigma|$ is equal to an odd prime. Without loss of generality we may assume that $\Sigma = \{B_1, B_2, \ldots, B_q\}$, with $|B_i| = 2p$, $1 \leq i \leq q$. Then for $B \in \Sigma$, G_B induces on B a primitive permutation group of degree $2p$ and it follows from [16] that, since $p \neq 5$, G_B is 2-transitive on B. Thus the subgraph induced on B is either the complete graph K_{2p} or the empty graph 2_pK_1. Replacing Γ by Γ^c if necessary we may assume that $\overline{B}$ is 2_pK_1, that is, $\overline{B}$ contains no edges.

LEMMA 6.1. *If* $|\Sigma| = q$ *then* $K = 1$.

Proof. Assume that $K \neq 1$. By the minimality of G, since $K \neq 1$, $G/K \cong Z_q$. Thus $G_B = K$, and by Lemma 5.2, $K_{(B)} = 1$. By the classification of finite 2-transitive groups (see [4]), K has at most two inequivalent 2-transitive representations of degree $2p$. Since the union of the blocks on which the representation of K is equivalent to its representation on B forms a block of imprimitivity for G, it follows that the actions of K on all blocks of Σ are equivalent. Thus K_α fixes exactly one point in each block of Σ, so $G_\alpha = K_\alpha$ has q fixed points and is transitive on $C\backslash\{\beta\}$ for each $C \in \Sigma$ where K_α fixes $\beta \in C$. The set F of q fixed points of K_α is (easily shown to be) a block of imprimitivity for G in V. Since Γ is connected there is an edge from α to some point in $V\backslash F$. Hence for some $C \in \Sigma\backslash\{B\}$, if $\{\beta\} = F \cap C$, we have $C\backslash\{\beta\} \subseteq \Gamma_1(\alpha)$. Now G is isomorphic to a subgroup of the largest subgroup of Sym V preserving both Σ and $\{F^g | g \in G\}$, namely $S_{2p} \times S_q$. Moreover the group $S_{2p} \times Z_p$ preserves all the G-orbits in $V \times V$ and hence Aut Γ contains $S_{2p} \times Z_q$, which contains a subgroup $Z_{2p} \times Z_q$ regular on V. This contradiction completes the proof. □

PROPOSITION 6.1. *If $|\Sigma| = q$ then $q = 11$, $p = 3$, $G = PSL_2(11)$ and there is at least one example of a vertex-transitive non-Cayley graph given in Construction 2.2.*

Proof. By Lemma 6.1, $K = 1$, so $G \lesssim S_q$. Let T denote the unique minimal normal subgroup of G. By Lemma 4.2, as p divides the order of G, T is nonabelian and is one of the groups listed in Lemma 4.2(b) (with p and q reversed). Since G_B must be 2-transitive of degree $2p$, $p \equiv 3 (\text{mod } 4)$, $q \not\equiv 1 (\text{mod } p)$, it follows that either $G = PSL_2(11)$ with $q = 11$, $p = 3$, or $PSL_m(r) \leq G \leq P\Gamma L_m(r)$ with $q = (r^m - 1)/(r - 1)$. By Proposition 2.2, *Ext*(11) is a vertex-transitive non-Cayley graph of order 66 admitting $G = PSL_2(11)$ (with this action on V) and hence we may assume that $PSL_m(r) \leq G \leq P\Gamma L_m(r)$. Now G is 2-transitive on Σ, so the quotient graph Γ_Σ is the complete graph K_q. For $B \in \Sigma$, G_B is therefore transitive on both B and $\Sigma\backslash\{B\}$. Let $\alpha \in B$ and $C \in \Sigma\backslash\{B\}$ be such that $\Gamma_1(\alpha) \cap C$ is nonempty. If $G_{\alpha,C}$ were transitive on C then $\Gamma(\alpha) \supseteq C$. As G is 2-transitive on Σ, for every block $C' \neq C$, $\Gamma_1(\alpha) \supset C'$ and hence $\Gamma \cong K_q[2pK_1]$ contradicting Lemma 5.1. Thus $G_{\alpha,C}$ has at least two orbits in C and $\Gamma_1(\alpha) \cap C$ is a proper subset of C.

Since q is prime, r and m are both prime. Now

$$G_B \geq (PSL_m(r))_B = Z_r^{m-1}.GL_{m-1}(r)$$

(or $Z_r.Z_{(r-1)/2}$ if $m = 2$). Since all 2-transitive groups of degree $2p$ have a nonabelian simple normal subgroup we must have $m \geq 3$, $(m, r) \neq (3, 2)$ or $(3, 3)$ and the only possibility for $|B| = 2p$, $p \equiv 3 (\text{mod } 4)$, is $2p = (r^{m-1} - 1)/(r - 1)$(since r is prime). Since m is an odd prime, $m - 1 = 2\hat{m} \geq 2$ and $2p = (r^{\hat{m}} + 1)(r^{\hat{m}} - 1)/(r - 1)$ which implies that $m = 3$, $q = 1 + r + r^2$ and $2p = r + 1$ so p divides $q - 1$ which is contradiction. □

7. The case $|\Sigma| = 2p$

Next we treat the case where $|\Sigma|$ is twice an odd prime, that is, without loss of generality, $\Sigma = \{B_1, B_2, \ldots B_{2p}\}$, with $|B_i| = q$, $1 \leq i \leq 2p$. This case is far more complicated than the previous two cases. The first substantial part of the analysis is the proof of the following proposition.

PROPOSITION 7.1. *If $|\Sigma| = 2p$ then we may assume that $K \neq 1$, that is we may, if necessary, replace G by a different minimal transitive subgroup of Aut Γ, preserving Σ, and acting unfaithfully on Σ, or replace p by q, q by p and Σ by a set of $2q$ blocks of size p so that the kernel is nontrivial.*

Before proving Proposition 7.1 we first obtain some detailed information in the case where G is faithful on Σ.

LEMMA 7.1. *If $K = 1$ then G^Σ is imprimitive.*

Proof. If $K = 1$ then $G \cong G^\Sigma \lesssim S_{2p}$. If G^Σ is primitive then G is a transitive primitive permutation group of degree $2p$ and so, since $p \equiv 3 (\mathrm{mod}\ 4)$, it follows from [16] that $G \cong A_{2p}$ or S_{2p}. So G_B is A_{2p-1} or S_{2p-1} which has no subgroup of index q. □

Thus, if $K = 1$, G^Σ either has 2 blocks of size p or p blocks of size 2. The next Lemma shows that in the former case Proposition 7.1 holds.

LEMMA 7.2. *Either Proposition 7.1 holds or $K = 1$ and G^Σ has a set of p blocks of size 2, and does not preserve a set of two blocks of size p.*

Proof. Suppose on the contrary that $K = 1$ and G^Σ has two blocks of size p. Then $G \cong G^\Sigma \leq S_p\, wr\, S_2$. Hence, in its action on V, G has two blocks, Δ_1 and Δ_2 say, of length pq. Now G has a subgroup H of index 2 that fixes Δ_1 and Δ_2 setwise, $H \lesssim S_p \times S_p$, and $\overline{H} := H^{\Delta_i} \lesssim S_p$ where H_i^Δ is transitive of degree qp. Let M be the socle of H and T the socle of $\overline{H}$. As M fixes Δ_1 and Δ_2 setwise it is either transitive on Δ_1 and Δ_2 or has $2q$ orbits in V of length p. In the latter case replacing Σ by the set of M-orbits would give a block system for G for which the kernel is nontrivial and Proposition 7.1 is true. Hence we may assume that M is transitive on Δ_1 and Δ_2. In particular $T \neq Z_p$ and so T is a nonabelian simple group. Now $M \lesssim T \times T$. If $M \cong T \times T$ then $M_{(\Delta_1)} \cong T$ is transitive on Δ_2 so $\Gamma \cong K_2[\Delta_1]$ which contradicts Lemma 5.1. Hence $M \cong T$. Let $B \in \Sigma$, $B \subseteq \Delta_1$. Now M_B is transitive on the q points of B and thus contains a subgroup of index q. Hence, by Lemma 4.2(d), $M \cong PSL_m(r)$ with $p = (r^m - 1)/(r - 1)$, and by Lemma 4.3, m is an odd prime, and $PSL_{m-1}(r)$ is a nonabelian simple group with no subgroup of index q.

Now $M_B = Z_r^{m-1}.GL_{m-1}(r)$ and for $\alpha \in B$, $|M_B : M_\alpha| = q$ is prime. Since $PSL_{m-1}(r)$ has no subgroup of index q, $M_\alpha \geq Z_r^{m-1}.SL_{m-1}(r)$ and so $M_B^B \cong Z_q \leq Z_{r-1}$, whence M_α fixes B pointwise. By Lemma 4.4, M_α is transitive on $\Delta_1 \backslash B$. Set $\Sigma_i = \{B' \in \Sigma | B' \subseteq \Delta_i\}$, for $i = 1, 2$. Suppose M acts similarly on Σ_1 and Σ_2. Then M_B fixes $B' \in \Sigma_2$. Now $M_B = M_{BB'} = Z_r^{m-1}GL_{m-1}(r)$

has a unique subgroup of index q containing $Z_r^{m-1}SL_{m-1}(r)$. Hence M_α fixes $B \cup B'$ pointwise and M_α is transitive on $\Delta_1\backslash B$ and on $\Delta_2\backslash B'$. Since for $\alpha' \in B'$, $M_\alpha = M_{\alpha'}$ is transitive on $\Delta_1\backslash B$ and $\Delta_2\backslash B'$, it follows that, for $\alpha_1 \in \Delta_1\backslash B$ and $\alpha_2 \in \Delta_2\backslash B'$, $(M_B)_{\alpha_i}$ is transitive on B and on B' for $i = 1, 2$. This implies that each of B and B' is trivially joined to each of $\Delta_1\backslash B$ and $\Delta_2\backslash B'$. By Lemma 3.1 applied to the partition $\{U = B \cup B', \Delta_1\backslash B, \Delta_2\backslash B'\}$ and the group M_B, we have $(M_B)^{B\cup B'} \leq \operatorname{Aut}\Gamma$. We have shown that $(M_B)^{B\cup B'} = \langle y\rangle \simeq Z_q$, and hence Aut Γ contains a subgroup Z_q^p fixing each block of Σ setwise. It follows that Aut Γ has a transitive subgroup of the form $Z_q^p.N_G(P)$ preserving Σ, where $P \leq M$ has order p. A minimal transitive subgroup of this group would either be unfaithful on Σ or would have a normal subgroup of order p with $2q$ orbits of length p. In either case Proposition 7.1 would hold.

Hence we may assume that M acts on Σ_1 and Σ_2 as on points and hyperplanes of $PG_{m-1}(r)$ respectively. Let $g \in G\backslash G \cap (S_p \times S_p)$ be a 2-element. By minimality, $G = \langle M, g\rangle$ and, as g interchanges Δ_1 and Δ_2, g interchanges points and hyperplanes of $PG_{m-1}(r)$ so $g \notin C_G(M)$. We may identify Σ_1 with the 1-spaces of an m-dimensional vector space $V_m(r)$ over $GF(r)$ in such a way that $B = \langle e_1\rangle$ where $e_1 = (1, 0, \ldots, 0)$. For $A \in SL_m(r)$, the preimage of M in $GL_m(r)$, let $\overline{A}$ denote the corresponding element of M. Then A fixes B (or $\overline{A} \in M_B$) if and only if

$$A = \begin{bmatrix} a_1 & \underline{0} \\ \underline{a}_2 & A_1 \end{bmatrix}$$

where $a_1 \det A_1 = 1$ (as B^A is the block identified with the 1-space generated by e_1A). Let us, for convenience, identify Σ_2 with the set of 1-spaces (generated by column vectors) in the dual space V^*. The image of a 1-space $\langle v^*\rangle$ of V^* under A is $\langle v^*\rangle^A = \langle A^{-1}v^*\rangle$. Now for $\overline{A} \in M_B$, $\overline{A} \in M_\alpha$ if and only if the (1, 1) entry a_1 in A belongs to the subgroup L of order $(r-1)/q$ of the multiplicative group of $GF(r)$. Note that

$$A^{-1} = \begin{bmatrix} a_1^{-1} & \underline{0} \\ \underline{a}_2' & A_1^{-1} \end{bmatrix}$$

where $a_1^{-1}\underline{a}_2 + A_1\underline{a}_2' = \underline{0}$, or equivalently $a_1\underline{a}_2' + A_1^{-1}\underline{a}_2 = 0$. Thus the image of $\langle x^*\rangle$ under A, where $x^* = [x_1, \underline{x}_2]^t = [x_1, x_2, \ldots, x_m]^t$, is $\langle A^{-1}x^*\rangle$ where

$$A^{-1}x^* = x_1 \begin{bmatrix} a_1^{-1} \\ \underline{a}_2' \end{bmatrix} + \begin{bmatrix} 0 \\ A_1^{-1}\underline{x}_2 \end{bmatrix}.$$

From this we see that the orbits of M_B and M_α on Σ_2 are the same, namely $\Sigma_{21} = \{\langle [0, \underline{x}_2]^t\rangle \mid \underline{x}_2 \neq \underline{0}\}$ and $\Sigma_{22} = \{\langle [x_1, \underline{x}_2]^t\rangle \mid x_1 \neq 0, \underline{x}_2 \neq \underline{0}\}$; $|\Sigma_{21}| = (r^{m-1} - 1)/(r-1)$, and $|\Sigma_{22}| = r^{m-1}$. Consider $B' = \langle [0, 1, 0, \ldots, 0]^t\rangle \in \Sigma_{21}$. Then $\overline{A} \in M_{B,B'}$ if and only if

$$A = \begin{bmatrix} a_1 & 0 & \underline{0} \\ a_{21} & a_2 & \underline{a}_4 \\ \underline{a}_3 & \underline{0} & A_2 \end{bmatrix}$$

where $a_1a_2\det A_2 = 1$. Since $m \geq 3$, $M_{\alpha,B'}$ is still transitive on B'. Hence M_α is transitive on $\bigcup\{B'|B' \in \Sigma_{21}\}$. Now let $B' \in \Sigma_{22}$, say $B' = \langle[1, \underline{0}]^t\rangle$. Then, for $A \in M_B$, $A \in M_{B,B'}$ if and only if $\underline{a}_2' = \underline{0}$, that is if and only if $\underline{a}_2 = \underline{0}$. If $A \in M_{\alpha,B'}$ then, in addition, $a_1^{-1} \in L$, and it follows that $M_{\alpha,B'}$ fixes B' pointwise. That is M_α has q orbits of length r^{m-1} in $\bigcup\{B'|B' \in \Sigma_{22}\}$.

We may identify the vertex set $V = \Delta_1 \cup \Delta_2$ as follows: $\Delta_1 = \{L\underline{v}|\underline{v} \in V_m(r)\backslash\{0\}\}, \Delta_2 = \{L\underline{v}^*|\underline{v}^* \in V_m(r)^*\backslash\{0\}\}$, where, for $A \in GL_m(r)$, A acts as follows: $(L\underline{v})^A = L(\underline{v}A)$, $(L\underline{v}^*)^A = L(A^{-1}\underline{v}^*)$. The 1-spaces $\langle\underline{v}^*\rangle$ in Σ_{22} are the ones for which $\underline{e}_1.\underline{v} \neq 0$ and the points in $B' = \langle\underline{v}^*\rangle$ are the sets $\xi^i L\underline{v}^*$, $0 \leq i < q$, where ξ is a primitive root of $GF(r)$. The q orbits of $M_{\alpha,B'}$ in $\bigcup\{B'|B' \in \Sigma_{22}\}$ are therefore the sets $\Delta_{2,j} = \{L\underline{w}^*|\underline{e}_1.\underline{w} \in \xi^j L\}$, $0 \leq j < q$. Since Γ is connected, for $\alpha \in B \subseteq \Delta_1$, $\Gamma_1(\alpha) \cap \Delta_2 \neq \emptyset$ and, since $\Gamma \neq K_2[\Delta_1]$ by Lemma 5.1, $\Gamma_1(\alpha) \not\supseteq \Delta_2$. By replacing Γ by Γ^c if necessary we may assume that $\Gamma_1(\alpha)\cap\Delta_2 \not\supseteq \bigcup\{B'|B' \in \Sigma_{21}\}$ and therefore $\Gamma_1(\alpha)\cap\Delta_2 = \bigcup_{j\in J}\Delta_{2,j}$ for some $\emptyset \neq J \subseteq [0, q-1]$. Also $\Gamma_1(\alpha)\cap\Delta_1$ may contain all or none of $\Delta_1\backslash B$ and may contain some points of $B\backslash\{\alpha\}$. Thus the edges of Γ are of at most three types. Those of type 1 are of the form $\{L\underline{v}, L\underline{w}^*\}$ where $\underline{v}.\underline{w} \in \bigcup_{j\in J}\xi^j L$; those of type 2, which exist if and only if $\Delta_1\backslash B \subseteq \Gamma_1(\alpha)$, are of the form $\{L\underline{v}, L\underline{w}\}$ where $\underline{v}$ and $\underline{w}$ are linearly independent in $V_m(r)$, and $\{L\underline{v}^*, L\underline{w}^*\}$ where $\underline{v}^*$ and $\underline{w}^*$ are linearly independent in $V_m(r)^*$; those of type 3, which may or may not exist are of the form $\{L\underline{v}, L\underline{w}\}$ where $\underline{v} = k\underline{w}$ for $k \in L_1$, and $\{L\underline{v}^*, L\underline{w}^*\}$, where $\underline{v}^* = k\underline{w}^*$ for $k \in L_2$ for some $L_1, L_2 \subseteq GF(r)^\#$ with $L_i = L_i^{-1}$ for $i = 1, 2$. The action of $GL_m(r)$ on V defined above preserves the set of edges and the kernel of this action is $L^* = \{lI|l \in L\}$. That is Aut $\Gamma \geq GL_m(r)/L^*$ and the normal subgroup $Z_{r-1}/L^* \simeq Z_q$ (the scalars modulo L^*) fixes each block of Σ setwise. Now since Aut Γ interchanges points and hyperplanes, it also contains the mapping σ given by $(L\underline{v})^\sigma = L\underline{v}^*$, $(L\underline{v}^*)^\sigma = L\underline{v}$ and σ normalizes a Singer cycle P and $P/L^* \simeq Z_{pq}$. Hence Aut Γ contains a regular subgroup, namely $P/L^*.\langle\sigma\rangle$, which is a contradiction. This completes the proof of Lemma 7.2. □

In order to complete the proof of Proposition 7.1 we must examine the case where $K = 1$ and G^Σ has p blocks of size 2.

LEMMA 7.3. *If $K = 1$ and G^Σ has p blocks of size 2 then G contains no nontrivial normal 2-subgroup.*

Proof. If $K = 1$ and G^Σ has p blocks of size 2, then $G \cong G^\Sigma \leq S_2 wr S_p$ and G has a set $\Delta = \{D_1, D_2, \ldots, D_p\}$ of p blocks of length $2q$ in V where, without loss of generality, $D_i = B_i \cup B_{i+p}$ for $1 \leq i \leq p$. Let $S = O_2(G)$ (the largest normal 2-subgroup of G). Then $S = G \cap S_2^p$ and $|S| \leq 2^p$. Suppose that $S \neq 1$. Then the S-orbits form a set $\Psi = \{C_1, C_2, \ldots, C_{pq}\}$ of pq blocks of imprimitivity for G of size 2. We may assume that $D_1 = C_1 \cup C_2 \cup \cdots \cup C_q$ and then, for $\alpha \in B_1$, S_α fixes $B_1 \cap C_i$ for $1 \leq i \leq q$. Hence S_α fixes B_1

pointwise and similarly fixes B_{p+1} pointwise. So fix $S_\alpha \supseteq D_1$. As fix S_α is a block for G, either $S_\alpha = 1$ and $|S| = 2$, or fix $S_\alpha = D_1$. Suppose temporarily that $|S| > 2$, so fix $S_\alpha = D_1$. Then $S_\alpha = S_{(D_1)}$ and the S-orbits and S_α-orbits in $V \backslash D_1$ are the same. It follows that, for each i, j with $1 \le i \le q$ and $q < j \le pq$, C_i and C_j are trivially joined, and hence by Lemma 3.1 applied to the partition $\{U = D_1, C_{q+1}, \ldots, C_{pq}\}$ and subgroup S, $S^{D_1} \le \operatorname{Aut} \Gamma$. Similarly, setting $S^{D_j} = \langle y_j \rangle \simeq Z_2$ for $1 \le j \le p$, $\operatorname{Aut} \Gamma \ge Y = \langle y_j, 1 \le j \le p \rangle = Z_2^p \ge S$. Suppose that P is a Sylow p-subgroup of G. If $N_G(P)$ has a subgroup $P.Q$ of order pq with 2 orbits of length pq, then $\operatorname{Aut} \Gamma \ge Y.PQ$ and clearly $y = y_1 y_2 \cdots y_p$ is centralized by PQ (since for any $g \in G$ with $D_i^g = D_j$, we have $y_i^g = y_j$, as $S^{D_i} = \langle y_i \rangle^{D_i}$). So $\langle y \rangle PQ$ is regular on V which is a contradiction. Similarly when G has such a subgroup PQ, and $|S| = 2$, then SPQ is regular on V, which again gives a contradiction. Hence G has no subgroup PQ of order pq with two orbits of length pq.

Now $G/S \cong G^\Sigma / S^\Sigma \lesssim S_p$. As G is minimal transitive on V and as G permutes the pq orbits of S of length 2, G/S is minimal transitive of degree pq and G/S is the subgroup of S_p induced on Δ. Now $(G/S)_D$ is a subgroup of G/S of index p where $D \in \Delta$, and $(G/S)_C$ is a subgroup of $(G/S)_D$ of index q, where $C \subsetneq D$, $C \in \Psi$. Let T be the minimal normal subgroup of G/S. Then by Lemma 4.2(d), $T = PSL_m(r)$ where $(r^m - 1)/(r - 1) = p$, and by Lemma 4.3, m is prime and $PSL_{m-1}(r)$ is a nonabelian simple group with no subgroup of index q. Let M be the subgroup of G containing S such that $M/S \cong T$. If $G \ne M$ then, by the minimality of G, M has q orbits of length $2p$ and $G = \langle M, g \rangle$ for some q-element g. But, if $P = Z_p \in Syl_p(M)$, then $S.N_G(P)$ is transitive on V contradicting the minimality of G. Hence $G = M$, so $G/S \cong T$ and either $|S| = 2$ or $Y = Z_2^p \le \operatorname{Aut} \Gamma$.

Now $G_{D_1} = S.(Z_r^{m-1}.GL_{m-1}(r))$. Since S interchanges B_1 and B_{p+1}, $G_{D_1} = SG_{B_1}$ and $|S : S \cap G_{B_1}| = 2$. So $G_{B_1}/(S \cap G_{B_1}) \cong Z_r^{m-1}.GL_{m-1}(r)$. As G_{B_1} is transitive on B_1 of degree q, and $PSL_{m-1}(r)$ has no subgroup of index q, it follows that $G_\alpha \ge (S \cap G_{B_1}).(Z_r^{m-1}.SL_{m-1}(r))$ and q divides $r - 1$. This means in particular that G_{D_1} is regular on D_1, and $G_{(D_1)} = G_\alpha$ is transitive on the $p - 1$ blocks of $\Delta \backslash \{D_1\}$. By Lemma 4.4, $G_{(D_1)D_2}$ is transitive on the set of q S-orbits contained in D_2. If $|S| > 2$ then $S_{(D_1)} \ne 1$ and $S_{(D_1)}$ is transitive on all S-orbits not in D_1 (since fix $S_\alpha = D_1$); but this means that G_α is transitive on $V \backslash D_1$, and so Γ is isomorphic to $\Gamma_\Delta[\overline{D}_1]$, contradicting Lemma 5.1.

Hence $|S| = 2$ and G_α, for $\alpha \in D_1$, has two orbits in $V \backslash D_1$, with α joined to exactly one of these orbits (again using Lemma 5.1 and the fact that Γ is connected). Let $C_1 = \{\alpha, \beta\}$, and $C_i = \{\alpha', \beta'\}$ be two S-orbits in D_1. Since G_α fixes D_1 pointwise, and since $S \cong Z_2$ intercharges the points in each S-orbit, and S interchanges the two G_α-orbits in $V \backslash D_1$, it follows that α' is joined to all points in one of the G_α-orbits in $V \backslash D_1$ and to no points in the other. We may assume that $\Gamma_1(\alpha) \backslash D_1 = \Gamma_1(\alpha') \backslash D_1$ and $\Gamma_1(\beta) \backslash D_1 = \Gamma_1(\beta') \backslash D_1$. Suppose now that $\{\alpha\} = C_1 \cap B_1$. We have shown that $G_\alpha = G_{(D_1)}$ is a normal subgroup of

G_{B_1} of index q so G_{B_1} permutes the G_α-orbits amongst themselves. However, since $|G_{B_1} : G_\alpha| = q$ is odd, G_{B_1} must fix setwise the two G_α-orbits in $V\backslash D_1$. As G_{B_1} is transitive on B_1, all points of B_1 are joined to the same G_α-orbits in $V\backslash D_1$ and all points of B_{p+1} are joined to the other G_α-orbit in $V\backslash D_1$. Hence each of B_1 and B_{p+1} is trivially joined to each of $\Gamma_1(\alpha)\backslash D_1$, $\Gamma_1(\beta)\backslash D_1$, the two G_α-orbits in $V\backslash D_1$. By Lemma 3.1 applied to the partition $\{U = D_1, \Gamma_1(\alpha)\backslash D_1, \Gamma_1(\beta)\backslash D_1\}$ and the subgroup G_{B_1}, we have $G_{B_1}^{B_1} < \mathrm{Aut}\,\Gamma$. Now $G_{B_1}^{B_1}$ is a cyclic group of order q, say $\langle y\rangle$. It follows that Aut Γ contains $Y = \langle y^g | g \in G\rangle \cong (Z_q)^p$ with one copy of Z_q acting on each of the D_i, for $i = 1$ to p. Moreover S^{D_1}, and hence S centralizes y, so S centralizes Y. Let $X \cong Z_p \leq G$. Then X acts regularly on $\{D_1, D_2, \ldots, D_p\}$; X acting on Y normalizes a subgroup $Q \cong Z_q$, and $(S \times Q).X$ is regular on V, which is a contradiction. Hence $S = 1$. This completes the proof of Lemma 7.3. □

Proof of Proposition 7.1. By Lemmas 7.1, 7.2, and 7.3, if $K = 1$ then G^Σ has p blocks of size 2 and contains no nontrivial normal 2-group. Thus $G \cong G^\Sigma \lesssim S_p$ and G has a set Δ of p blocks, $\{D_1, D_2, \ldots, D_p\}$ say, of length $2q$ in V where, without loss of generality, $D_i = B_i \cup B_{i+p}$ for $1 \leq i \leq p$. Let $T = \mathrm{soc}\, G$ and for convenience set $D = D_1$, $B = B_1$ and let $\alpha \in B$. Now G_D is a subgroup of G of index p, and as G_D is transitive on $\{B, B_{1+p}\}$, G_D has a subgroup of index 2, namely G_B. Since G_B is transitive on B, $(G_B)_\alpha = G_\alpha$ is a subgroup of G_B of index q. Hence, by Lemma 4.2(d), $T = PSL_m(r)$ where $(r^m - 1)/(r - 1) = p$ and by Lemma 4.3, m is an odd prime and $PSL_{m-1}(r)$ is a nonabelian simple group with no subgroup of index q. If T were not transitive on Σ then T would have 2 orbits in Σ of length p. The T-orbits would be blocks for G and so $G^\Sigma \leq S_p wr S_2$ whence Proposition 7.1 would be true by Lemma 7.2. So we may assume that T is transitive on Σ of degree $2p$.

Suppose that T^V is intransitive. Then T has q orbits in V of length $2p$, and by minimality $G = \langle T, x\rangle$ for some q-element x. Let $P \simeq Z_p$ be a Sylow p-subgroup of G. Then $G = TN_G(P)$, so we may assume that $x \in N_G(P)$. However, since $G \lesssim S_p$, $|N_G(P)|$ divides $|N_{S_p}(P)| = p(p-1)$ and hence q divides $p-1$ which is a contradiction. Therefore T^V is transitive and, by minimality, $G = T$.

Now $T_D = Z_r^{m-1}.GL_{m-1}(r)$ has T_B as a subgroup of index 2, and hence r is odd and $T_B \geq Z_r^{m-1}.SL_{m-1}(r)$. Since $|T_B : T_\alpha| = q$ is prime $T_\alpha \geq Z_r^{m-1}.SL_{m-1}(r)$ for otherwise $PSL_{m-1}(r)$ would have a subgroup of index q. By Lemma 4.4, T_α is transitive on $V\backslash D$, whence $\Gamma \simeq \Gamma_\Delta[\overline{D}_1]$ which contradicts Lemma 5.1. This completes the proof of Proposition 7.1. □

In the remainder of this section we assume (as we may do, by Proposition 7.1), that $K \neq 1$. Then G^Σ is a minimal transitive subgroup of S_{2p}. We shall show that there are no non-Cayley graphs in this case.

PROPOSITION 7.2. *There are no examples with* $|\Sigma| = 2p$.

First we investigate a Sylow q-subgroup Q of K. Let $B \in \Sigma$, and $\alpha \in B$.

LEMMA 7.4. *The group Q is normal in G and $Q_{(B)}$ fixes pointwise r blocks, where r is 2, p or $2p$, and $Q_{(B)}$ is transitive on each of the $2p - r$ blocks not fixed pointwise by Q.*

Proof. By Lemma 5.2(a) q divides $|K|$, so $Q \neq 1$. Since $G = KN_G(Q)$, $N_G(Q)$ is transitive on Σ and hence on V. By minimality, $G = N_G(Q)$. Since the set of rq fixed points of $Q_\alpha = Q_{(B)}$ is a block of imprimitivity for G in V, r divides $2p$. By Lemma 5.2, $r \neq 1$. □

LEMMA 7.5. *The number r is not p.*

Proof. If $r = p$ then there are two distinct subgroups, Q_1 and Q_2 of index q in Q, each fixing pointwise half of the blocks, and $Q_1 \cap Q_2 = 1$. Hence $Q \cong Q_1 \times Q_2$. Suppose that Q_1 fixes the blocks $D_1 = \{B_1, B_2, \ldots, B_p\}$ and Q_2 fixes the blocks $D_2 = \{B_{p+1}, B_{p+2}, \ldots, B_{2p}\}$. Then G/K acts imprimitively on Σ with D_1 and D_2 being blocks of size p. Let H be the subgroup of G of index 2 fixing D_1 and D_2 setwise.

Let P be a Sylow p-subgroup of G. Since p is odd, P normalizes Q_1 and Q_2, and since p does not divide $q-1$, P centralizes Q_1 and Q_2. Hence P centralizes Q. Now $P \leq H$ and hence $G = N_G(P).H$, so $N_G(P)$ contains a 2-element x which interchanges D_1 and D_2. Since $\langle Q, P, x\rangle$ is transitive on V, it follows by the minimality of G that $G = \langle P, Q, x\rangle = (Q.P).\langle x\rangle$ and $|G| = p^s q^2 2^t$ for some $s, t \geq 1$. Since P centralizes Q, P is normal in G, so P has $2q$ orbits of length p. Now, for $\alpha \in B_1$, P_α fixes each block in D_1 pointwise. Hence P is Z_p or $Z_p \times Z_p$. Suppose that $|P| = p^2$ and let $P_2 = P_\alpha$ and, for $\beta \in B_{p+1}$, let $P_1 = P_\beta$. Then $Q_k \times P_k$ is transitive on the set $\overline{D}_k$ of pq points in D_k and fixes $V \setminus \overline{D}_k$ pointwise, for $k = 1, 2$. It follows that $\Gamma \simeq K_2[\overline{D}_1]$ which contradicts Lemma 5.1. Hence $|P| = p$. Since Aut $P \simeq Z_{p-1}$ and $p \equiv 3 (\mathrm{mod}\ 4)$, it follows that $x^2 \in C_G(P)$.

Now $Q = Q_1 \times Q_2$ where $Q_1 = \langle a\rangle$ and $Q_2 = \langle b\rangle$ (say) are cyclic groups of order q. For each $1 \leq i \leq q-1$, $\overline{Q}_i = \langle ab^i\rangle$ is transitive on each block of Σ and, if $\langle x\rangle$ normalized $\overline{Q}_i$ then $\overline{Q}_i.P\langle x\rangle$ would be a transitive subgroup of G, contradicting the minimality of G. Hence $\langle x\rangle$ does not normalize $\overline{Q}_i$ for any $1 \leq i \leq q-1$. Since $Q_1^x = Q_2$ we may assume that $a^x = b$ and $b^x = a^j$ for some $1 \leq j \leq q-1$. Then $\overline{Q}_i^x = \langle ba^{ij}\rangle$ which equals $\overline{Q}_i$ if and only if $i^2 j \equiv 1 (\mathrm{mod}\ q)$. Since $\langle x\rangle$ normalizes no $\overline{Q}_i, j$ is a nonsquare modulo q. Now x^2 conjugates each element y of Q to y^j. Since j is a nonsquare $x^2 \notin C_G(Q)$. But since $q \equiv 3 (\mathrm{mod}\ 4)$, x^4 centralizes Q, and since $a^{x^4} = a^{j^2}$ it follows that $j^2 = 1$, whence $j = -1$. Now x^4 centralizes P and Q and fixes $\overline{D}_1$ and $\overline{D}_2$ setwise. Hence $x^4 = 1$.

So $|G| = 4pq^2$ and, setting $P = \langle c\rangle$, $G = \langle a, b, c, x\rangle$ where $a^q = b^q = c^p = x^4 = 1$, and $[a, b] = [a, c] = [b, c] = 1$, $a^x = b$, $b^x = a^{-1}$ and, since x either centralizes or inverts P, $c^x = c^\delta$ where $\delta = \pm 1$. Also $G_\alpha = \langle a, x^2\rangle$ and it follows from Proposition 3.1 that Γ is a Cayley graph. □

The remaining possibilities for r are $r = 2$ and $r = 2p$. We shall treat the case $r = 2p$ next, but as preparation we prove the following technical lemma.

LEMMA 7.6. *If G^Σ has a set $\Delta = \{D_1, D_2, \ldots, D_p\}$ of p blocks of size 2, and if $L = G_{(\Delta)}$, the subgroup of G fixing each block setwise, is such that $L = K$, then $G^\Sigma \simeq D_{2p}$.*

Proof. Suppose that $L = K$. Then $G^\Sigma \simeq G^\Delta \leq S_p$, G^Σ is a minimal transitive group of degree $2p$, and for $D = \{B, C\} \in \Delta$, $(G_D)^\Delta$ has a subgroup $(G_B)^\Delta$ of index 2. If G^Δ has socle Z_p then this implies that $G^\Sigma \simeq D_{2p}$, so assume that the socle N of G^Δ is nonabelian. Then by Lemma 4.2(c), either $N = M_{11}$, $p = 11$ or $N = PSL_m(r)$, $p = (r^m - 1)/(r - 1)$. In the latter case $m \geq 3$ by Lemma 4.3.

Suppose that $N = PSL_m(r)$. Let $K < R \leq G$ such that $R/K \simeq PSL_m(r)$. If R^Σ is intransitive then R^Σ has 2 orbits of length p and, for a Sylow p-subgroup P of R, $G = RN_G(P)$. Thus there is some 2-element, x say, belonging to $N_G(P)$ such that $QP\langle x\rangle$ is transitive on V, so $G = QP\langle x\rangle$. In this case $G/K \lesssim P\langle x\rangle$ does not contain $PSL_m(r)$ which is a contradiction. Hence R^Σ, and hence also R^V, is transitive and so, by minimality, $G = R$.

Now $G_D^\Sigma = Z_r^{m-1}.GL_{m-1}(r)$ and, since $|G_D^\Sigma : G_B^\Sigma| = 2$, r must be odd, and $G_B^\Sigma \geq Z_r^{m-1}.SL_{m-1}(r)$. By Lemma 4.4, G_B is transitive on $\Sigma\backslash D$, and since for $\alpha \in B$, $G_B = QG_\alpha$, also G_α is transitive on $\Sigma\backslash D$. If $|Q| > q$ then G_α is transitive on $V\backslash\overline{D}$ where $\overline{D} = B \cup C$, and so $\Gamma \simeq \Gamma_\Delta[\overline{D}]$ which contradicts Lemma 5.1. Hence $|Q| = q$. Since Aut $Q \simeq Z_{q-1}$, $C_G(Q)$ has N as a composition factor, and hence $C_G(Q)$ is transitive on V. By minimality of G, $G = C_G(Q)$, and in particular $K = Q$ and $G_B^B = Q^B \simeq Z_q$. Now Q^D is central in G_D^D and $G_D/Q = Z_r^{m-1}.GL_{m-1}(r)$. If $G_\alpha^C \simeq Z_q$, then we would have $G_D^D \simeq Z_q\, wr\, Z_2$ but G_D has no quotient of this type. Hence $G_D^D \simeq Z_{2q}$. So G_D has a subgroup H of index q and H^D is the unique subgroup of G_D^D of order 2. Let $B' \in \Sigma\backslash D$. If $G_{\alpha,B'}^{B'}$ is transitive then, since G_α is transitive on $\Sigma\backslash D$, G_α is also transitive on $V\backslash\overline{D}$ and $\Gamma \simeq \Gamma_\Delta[\overline{D}]$ as above. Hence $G_{\alpha,B'}^{B'} = 1$ and so G_α has q orbits of length $2p - 2$ in $V\backslash\overline{D}$.

Now $\alpha^H = \{\alpha, \beta\}$ is a block of imprimitivity for G. Moreover, since $H \leq C_G(Q)$, Q permutes the H-orbits in $V\backslash\overline{D}$, and since $|H : G_\alpha| = 2$ it follows that the H-orbits and G_α-orbits in $V\backslash\overline{D}$ are the same. It follows that each H-orbit in $\overline{D}$ is trivially joined to each G_α-orbit in $V\backslash\overline{D}$, and hence by Lemma 3.1, $H^{\overline{D}} \leq$ Aut Γ. Let $H^{\overline{D}} = \langle\zeta_D\rangle \simeq Z_2$. For $D' \in \Delta$ we therefore have $\langle\zeta_{D'}\rangle \leq$ Aut Γ where $\zeta_{D'}$ is the unique involution in $G_{D'}^{D'}$. Then, for $P \simeq Z_p \leq G$, and $\zeta = \prod_{D'\in\Delta}\zeta_{D'}$, the subgroup $QP\langle\zeta\rangle$ of Aut Γ is regular on V, which is a contradiction. Thus $N \neq PSL_m(r)$.

Hence $N = M_{11}$. Then $G/K = M_{11}$, $G_D^\Sigma = M_{10}$, and $G_B^\Sigma = A_6$ is transitive on $\Delta\backslash\{D\}$. Now M_{11} induces a rank 3 action of Σ (see [7]) and so G_B is transitive on $\Sigma\backslash\{B, C\}$. A similar argument to that used for $PSL_m(r)$ now shows that Γ is a Cayley graph. □

LEMMA 7.7. *The number r is not 2p.*

Proof. If $r = 2p$ then $Q = Z_q$. Since G^Σ is minimal transitive of degree $2p$, $G^\Sigma \not\cong S_{2p}$ or A_{2p}. Since $p \neq 5$, it follows from [16] that G^Σ is imprimitive.

Since p does not divide $q-1$, a Sylow p-subgroup P of G must centralize Q. Hence the normal subgroup H of G generated by Q and all Sylow p-subgroups of G centralizes Q. If H is intransitive then H has two orbits of length pq and, as $G = HN_G(P)$, some 2-element $y \in N_G(P)$ interchanges them. By minimality of G, $G = (Q \times P)\langle y\rangle$, and as $q \equiv 3 \pmod 4$, y inverts or centralizes Q. If H is transitive then $G = H = C_G(Q)$. In particular $C_G(Q)$ is either transitive or has two orbits of length pq.

It is convenient to continue our proof via a series of steps:

Step 1: If p^2 divides $|G^\Sigma|$ then $G = (Q \times P)\langle y\rangle$ where P is a Sylow p-subgroup of G and y is a 2-element normalizing P.

Suppose that p^2 divides $|G^\Sigma|$. Then G^Σ has two blocks, D_1 and D_2 say, of size p and the subgroup H above is intransitive. Then step 1 follows.

Step 2: $K = Q.Z_r$ for some divisor r of $q-1$, and $C_K(Q) = Q$.

Here q does not divide $|K_{(B)}|$, and it follows from Lemma 5.2 that $K_{(B)} = 1$. Thus $K \simeq K^B$, a transitive group of degree q with normal subgroup $Q^B \simeq Z_q$, so $K = Q.Z_r$ for some divisor r of $q-1$. In particular $C_K(Q) = Q$.

Step 3: $G = (Q \times P)\langle y\rangle$ where $y \in N_G(P)$, and y is a 2-element which inverts Q.

Suppose this is not the case. Then, by our observations above, G centralizes Q. By step 2, $K = C_K(Q) = Q$ and $G^\Sigma = G/Q \leq S_{2p}$. Suppose that p^2 divides $|G|$. Then, by step 1, $G = (Q \times P)\langle y\rangle$, where y is a 2-element normalizing P. Using a similar argument to that used in the proof of Lemma 7.5 (and interchanging P and Q), $y^4 \in C_G(Q) \cap C_G(P) \cap C_G(\langle y\rangle)$ and thus $y^4 = 1$. Thus G is as in Proposition 3.1 (with p and q reversed), and hence Γ is Cayley graph, a contradiction. Hence p^2 does not divide $|G|$ and a Sylow p-subgroup P of G is cyclic of order p.

Suppose that G^Σ has 2 blocks D_1 and D_2 of length p. Then, as in step 1, $G = (Q \times P)\langle y\rangle$ for some 2-element y which normalizes P and interchanges D_1 and D_2. Since $p \equiv 3 \pmod 4$, y^2 centralizes P and Q, and fixes D_1 and D_2 setwise, whence $y^2 = 1$. Therefore $|G| = 2pq$, so G is regular on V, which is a contradiction.

Hence G^Σ has a set $\Delta = \{D_1, D_2, \ldots, D_p\}$ of p blocks of size 2, $G/Q = G^\Sigma \leq S_2 wr S_p$ and a Sylow p-subgroup P of G has order p and acts transitively on Δ. Let $L = G_{(\Delta)}$, the subgroup of G fixing each D_i setwise. Then $K \leq L$.

Suppose that $L^{\Sigma} = 1$. Then $L = K = Q$, and $G^{\Sigma} \simeq G^{\Delta} \lesssim S_p$. By Lemma 7.6 $G/K = G/Q \simeq D_{2p}$, which implies that G is regular on V, a contradiction. So L has p orbits of length $2q$. Let S be a Sylow 2-subgroup of L. Then $G = LN_G(S)$, so we may choose $P \leq N_G(S)$. Then, by minimality of G, $G = QSP$. Since $C_G(Q) = G$ we have in fact $G = Q \times SP$. Also, since $QS = Q \times S$ is transitive on each D_1, $|(QS)^{D_i}| = 2q$ and QS is regular on D_i. Now S is elementary abelian of order 2^a say, where $a \leq p$. Thus $G = \langle x_1, x_2, \ldots, x_a, b, c\rangle$ where $\langle x_1, x_2, \ldots, x_a\rangle = Z_2^a$, $b^q = c^p = 1$, b centralizes x_i for $1 \leq i \leq a$ and b centralizes c. If c centralized S then PS would be an abelian transitive group of degree $2p$ and hence regular whence QSP would be regular on V which is a contradiction. Hence c acts nontrivially on S, and by the minimality of G, c acts irreducibly on S. Then, setting $y = bc, G$ is as in Proposition 3.2 and it follows that Γ is a Cayley graph which is a contradiction. Thus step 3 follows.

Now we complete the proof of Lemma 7.7. By step 3, $G = (Q \times P)\langle y\rangle$ where y is a 2-element which inverts Q and normalizes P. By step 2, $K = Q$. So $P \simeq P^{\Sigma}$, and $|P|$ is p or p^2. If $|P| = p^2$ then, by a proof similar to that for Lemma 7.5, $y^4 = 1$. If y has order 4 then G is as in Propositon 3.1 (with p and q interchanged), so Γ is a Cayley graph which is a contradicton. On the other hand if y has order 2 then G contains a regular subgroup, again a contradiction. Hence $P = Z_p$ acts transitively on the Q-orbits within each $C_G(Q)$-orbit. As $y^2 \in C_G(P) \cap C_G(Q)$ and y^2 preserves the sets D_1 and D_2, $y^2 = 1$, but then G is regular, which is a contradiction. □

Proof of Proposition 7.2. By Lemmas 7.4, 7.5, and 7.7, $r = 2$ and Q has p distinct subgroups, $Q_1, Q_2, \ldots, Q_p$, of index q that fix pointwise two blocks and are transitive on each of the other $2p-2$ blocks of Σ, say Q_i fixes pointwise blocks B_i and B_{i+p}, for $1 \leq i \leq p$. Moreover $G = N_G(Q)$ permutes the subgroups Q_i and hence the set $\Delta = \{D_i = B_i \cup B_{i+p} | 1 \leq i \leq p\}$ is a system of p blocks of imprimitivity of length $2q$ in V. Let $D \in \Delta$, where $D = B \cup C$, $B, C \in \Sigma$. The group $Q^D = \langle \zeta^D\rangle \simeq Z_q$ for some $\zeta \in Q$. It follows from Lemma 3.1 that $\zeta^D \in$ Aut Γ, and Aut Γ contains $\hat{Q} = \prod_{D\in\Delta} Q^D = Z_q^p$. Now $Q \leq \hat{Q} = Z_q^p$, so $Q \simeq Z_q^a$ for some $a \leq p$. Since $Q_1 \neq 1$, $a \geq 2$.

Let L be the subgroup of G that fixes the sets D_i, for $1 \leq i \leq p$, setwise. Suppose that $L \neq K$. Then L has p orbits of length $2q$. Let S be a Sylow 2-subgroup of L. Since $G = LN_G(S)$, $N_G(S)$ is transitive on Δ, and by minimality $G = QN_G(S)$. Let x be a p-element in $N_G(S)$ acting nontrivially on Δ. Then, again by minimality, $G = QS\langle x\rangle$. Set $P = \langle x\rangle$. Now x^p fixes each D_i setwise, and so normalizes $Q^{D_i} \simeq Z_q$. Since p does not divide $q-1$ it follows that x^p centralizes Q^{Di} and hence x^p fixes D_i pointwise, for all i, whence $x^p = 1$. So $P \cong Z_p$.

Suppose that $|S^{\Sigma}| \geq 4$. Then S_B fixes only B and C setwise and interchanges the two blocks of Σ in all other $D' \in \Delta\backslash\{D\}$. Let $\alpha \in B$. Now $G_\alpha^{\Sigma} = G_B^{\Sigma} = S_B^{\Sigma}$, and since $G_\alpha > Q_1$ it follows that G_α is transitive on D' for each $D' \in \Delta\backslash\{D\}$. Therefore $\Gamma \simeq \Gamma_\Delta[\overline{D}]$, contradicting Lemma 5.1. Hence $|S^{\Sigma}| = 2$, and therefore

$G^{\Sigma} \simeq Z_{2p}$. Let H be the subgroup of index 2 in G such that $H^{\Sigma} \simeq Z_p$. Then $P \subseteq H$ and so $G{=}HN_G(P)$. So there is a 2-element $y \in N_G(P)$ interchanging the two H-orbits. By minimality $G{=}QP\langle y\rangle$, and $\langle y\rangle$ is a Sylow 2-subgroup of G. Now y fixes each D_i setwise and hence normalizes each Q^{D_i}. Since 4 does not divide $q-1$, y^2 centralizes each Q^{D_i} and hence $y^2 \in C_G(Q) \cap K = Q$, so $y^2 = 1$. Hence $|S| = 2$ and as P normalizes S, PS is cyclic and $S = \langle y\rangle$.

Now since $P = \langle x\rangle$ and S permute the Q_i, they normalize $\hat{Q}$. If $D_i^x = D_{i+1}$ for $1 \leq i < p$, we may choose $Q^{D_i} = \langle \zeta_i\rangle$ such that $\zeta_i^x = \zeta_{i+1}$ for $i = 1, \ldots, p-1$. Then $\zeta_p^x = \zeta_1^{x^p} = \zeta_1$ since $x^p = 1$ and hence $\zeta_1\zeta_2\cdots\zeta_p$ is centralized by x. Also y normalizes each Q^{D_i}, and, since x centralizes y, y acts in the same way on each Q^{D_i}, so either $y \in C_G(\hat{Q})$ or y inverts each element of $\hat{Q}$. In either case $\langle \zeta_1\zeta_2\cdots\zeta_p, x, y\rangle$ is regular on V, a contradiction.

Thus $L = K$, so $G^{\Sigma} \simeq G^{\Delta} \lesssim S_p$ and, by Lemma 7.6, $G^{\Sigma} \simeq D_{2p}$. Since $K \leq \prod_{B\in\Sigma} K^B \leq AGL(1, q)^{2p}$, the prime p does not divide $|K|$ and so a Sylow p-subgroup $P = \langle x\rangle$ of G has order p. Moreover, as $QN_G(P)$ is transitive it follows that, for some 2-element $y \in N_G(P)$, $G{=}QP\langle y\rangle$, and $K = Q\langle y^2\rangle$. Since y normalizes Q, $y^2 \in C_K(Q) = Q$, so $y^2 = 1$ and $\langle \zeta_1\zeta_2\cdots\zeta_p, x, y\rangle$ is regular on V, a contradiction. □

8. The case $|\Sigma| = pq$

Finally we treat the case where $\Gamma = (V, E)$ is a non-Cayley graph of order $2pq$ with minimal transitive group G such that $|\Sigma|$ is equal to pq. By the results of the previous sections we may assume that G preserves no partition with blocks of size p, q, or pq. We assume as usual that $pq \notin NC$, $p \not\equiv 1 (\text{mod } q)$, $q \not\equiv 1$ (mod p) and $p \equiv q \equiv 3$ (mod 4). First we show that G is not faithful on Σ.

PROPOSITION 8.1. *If* $|\Sigma| = pq$ *then* $K \neq 1$.

Proof. Suppose that $G_{(\Sigma)} = K = 1$. Then $G \cong G^{\Sigma} \lesssim S_{pq}$. If G^{Σ} is primitive then G is a transitive primitive permutation group of degree pq and so, by Lemma 4.1, either $G \geq A_{pq}$, or $PSL_m(r) \leq G \leq P\Gamma L_m(r)$ with $pq = (r^m - 1)/(r - 1)$. Let $\alpha \in B \in \Sigma$. If $G \geq A_{pq}$ then, since G_B has a subgroup of index 2 (namely G_α), $G = S_{pq}$. Now S_{pq} has a transitive subgroup of the form $G_1 \times G_2$, where $G_1 = Z_p.Z_{p-1}$ and $G_2 = Z_q.Z_{q-1}$, which contains an odd permutation. Therefore $G_1 \times G_2$ is transitive on V, contradicting the minimality of G. Suppose that $T{=}PSL_m(r) \leq G \leq P\Gamma L_m(r)$. If T^V is not transitive the T-orbits provide a system of two blocks for G of size pq, which is a contradiction. Hence, by minimality, $G = T$. Then $T_B = Z_r^{m-1}.GL_{m-1}(r)$ and, since T_B has a subgroup of index 2, r is odd. If $m = 2$ then $pq = r + 1 \equiv 1$ (mod 4) whence r is even, which is a contradiction. Hence $m \geq 3$, and since $(r^m - 1)/(r - 1) = pq$, (m, r) is not (3, 3) and hence $PSL_{m-1}(r)$ is a nonabelian simple group. Therefore

$T_\alpha \geq Z_r^{m-1}.SL_{m-1}(r)$ and by Lemma 4.4, T_α is transitive on $V\backslash B$ and hence $\Gamma \cong \Gamma_\Sigma[\overline{B}]$, which contradicts Lemma 5.1.

Thus G^Σ is imprimitive and, without loss of generality, we may assume that G^Σ preserves a set $\Delta = \{D_1, D_2, \ldots, D_p\}$ say, of p blocks of size q. Each D_i is a subset of q blocks of Σ; let $\overline{D}_i$ denote the union of these blocks. Then $\overline{\Delta} = \{\overline{D}_1, \overline{D}_2, \ldots, \overline{D}_p\}$ is a set of blocks of imprimitivity of size $2q$ for G in V.

Suppose that G^Σ is not faithful on Δ and let H be the subgroup of G that fixes each block of Δ setwise. For $D \in \Delta$ let $\overline{H} = H^D \leq S_q$. Let M be the socle of H and T the minimal normal subgroup of $\overline{H}$. Since the M-orbits form a G-invariant partition of V and there is no G-invariant partition with blocks of size q, M has p orbits of length $2q$ in V and in particular $|M|$ is even. Now $M = T^a$ for some $1 \leq a \leq p$. If $a \geq 2$ it follows that $\Gamma \simeq \Gamma_\Delta[\overline{D}]$ which contradicts Lemma 5.1. Hence $M = T \leq H$ and M^D is a simple primitive group of degree q. Moreover, since $|M|$ is even, M is a nonabelian simple group. Since M_B has M_α as a subgroup of index 2, it follows from Lemma 4.2(c) that M is M_{11} with $q = 11$, or $PSL_m(r)$ with $q = (r^m - 1)/(r - 1)$ and (from Lemma 4.3(a)) m is prime, and $r = r_0^{m^c}$ for some prime r_0 and $c \geq 0$. In the latter case, since $|M_B : M_\alpha| = 2$, r is odd.

If p does not divide $|OutM|$ then a p-element x of G/M centralizes M. Since $\langle M, x\rangle$ is transitive, $G = \langle M, x\rangle$ and $C_G(M) = \langle x\rangle$ is a normal subgroup of G with $2q$ orbits of length p contradicting the fact that there are no such G-invariant partitions of V. Hence p must divide $|OutM|$ and $C_G(M) = 1$. Hence $M \neq M_{11}$, and so $M = PSL_m(r)$ and p divides $|Out\ PSL_m(r)| = 2m^c.(m, r - 1)$. It follows that $p = m$. If p divides $r - 1$ then $q = 1 + r + \cdots + r^{m-1} \equiv m \pmod p \equiv 0 \pmod p$ which is a contradiction. Hence $c \geq 1$. By minimality of G, $G = \langle M, x\rangle \leq P\Gamma L_m(r)$ for some p-element x. It follows that the actions of H on $D_1, D_2, \ldots, D_p$ are equivalent and hence that H_α fixes a set C of $2p$ points, two from each of the D_i. Now C is block of imprimitivity for G and $G_C^C \simeq Z_{2p}$. Therefore G_C has a subgroup of index 2 containing G_α, whence G has a block of imprimitivity of size p, which is a contradiction. Hence G acts faithfully on Δ, that is $G \cong G^\Sigma \cong G^\Delta \lesssim S_p$.

Again let T denote the minimal normal subgroup of G. If T is abelian then T has $2q$ orbits of length p which form a G-invariant partition of V, contradicting our assumptions. Hence T is a nonabelian simple group. For $B \in D \in \Delta$, G_B is a subgroup of G_D of index q. Hence, by Lemma 4.2(d), $T = PSL_m(r)$ and $p = (r^m - 1)/(r - 1)$.

If T^Σ is intransitive, then the T^Σ-orbits form a block system for G^Σ consisting of q blocks of size p on which G^Σ acts unfaithfully. We have just shown that this is not possible. Hence T is transitive on Σ. If T were intransitive on V then G would preserve a partition of V consisting of two blocks of size pq, which is not the case. Hence T is transitive on V and so by minimality $G = T$. Since q divides $|G|$, it follows from Lemma 4.3 that m is an odd prime, and $r = r_0^{m^c}$ for some prime r_0 and $c \geq 0$. If $m = 3$, $r = 2$, then $q = 3$ would divide $p - 1 = 6$ which is not the case. Also, since $p \equiv 3 \pmod 4$, $(m, r) \neq (3, 3)$.

Hence $PSL_{m-1}(r)$ is a nonabelian simple group. If $PSL_{m-1}(r)$ had a subgroup of index q then, arguing as in the proof of Lemma 4.3(c), $m = 3$, $q = r + 1 \equiv 3 (\mathrm{mod}\ 4)$, and $p = 1 + r + r^2 \equiv 3 (\mathrm{mod}\ 4)$. However $q = r + 1 \equiv 3 (\mathrm{mod}\ 4)$ implies that $r = 2$ contradicting the fact that $(m, r) \neq (3, 2)$. Hence $PSL_{m-1}(r)$ has no subgroup of index q, and it follows that G_B, and hence G_α (where $\alpha \in B$) contains $Z_r^{m-1}.SL_{m-1}(r)$. Then by Lemma 4.4, G_α is transitive on $V \backslash \overline{D}$, and it follows that $\Gamma \simeq \Gamma_\Delta[\overline{D}]$, which is a contradiction. □

PROPOSITION 8.2. *There are no examples with* $|\Sigma| = pq$.

Proof. By Proposition 8.1, K is a nontrivial elementary abelian 2-group, and hence $G^\Sigma = G/K$ is a minimal transitive group of degree pq. If G^Σ is primitive then by Lemma 4.1, either $G^\Sigma \geq A_{pq}$, or $PSL_m(r) \leq G^\Sigma \leq P\Gamma L_m(r)$ with $pq = (r^m - 1)/(r - 1)$, where m is prime or the square of a prime, and $(m, r) \neq (2, 2), (2, 3)$. Since A_{pq} contains a transitive cyclic subgroup, A_{pq} is not minimal transitive.

If $T = PSL_m(r)$ then, since T is transitive of degree pq, by minimality. $G^\Sigma = T$. Since K^B is transitive, $G_B = G_\alpha.K$ and hence $G_\alpha^{\Sigma \backslash \{B\}}$ is transitive. If $|K| \geq 4$ then $K_\alpha \neq 1$ and so there is some $C \in \Sigma$ such that K_α^C is transitive. Therefore G_α is transitive on $V \backslash B$ and so $\Gamma \cong \Gamma_\Sigma[\overline{B}]$ which contradicts Lemma 5.1. Hence $|K| = 2$. Since $\Gamma \ncong \Gamma_\Sigma[\overline{B}]$, G_α must have 2 orbits in $V \backslash B$ and α must be adjacent to the points of one of the these orbits and not the other. By replacing Γ by its complement if necessary (as we may do by Lemma 5.2), we may assume that α is not adjacent to α', where $B = \{\alpha, \alpha'\}$. Since each of α and α' is adjacent to exactly one point in every block of $\Sigma \backslash \{B\}$ and since Γ is connected, it follows that α and α' are at distance 3. Now $\Gamma_1(\alpha')$ is a G_α-orbit containing at least one point at distance 2 from α, and so $\Gamma_1(\alpha') \subseteq \Gamma_2(\alpha)$. It follows that $\Gamma_1(\alpha') = \Gamma_2(\alpha)$, and so Γ is a distance transitive antipodal double cover of a complete graph. These graphs are equivalent to regular "two graphs" with doubly transitive groups, which were classified in [30, Theorem 1]. It follows from [30] that $G^\Sigma = PSL_2(r)$ with $r \equiv 1\ (\mathrm{mod}\ 4)$ whence $pq = r + 1 \equiv 2\ (\mathrm{mod}\ 4)$, which is a contradiction, since pq is odd.

Thus G^Σ is imprimitive and, without loss of generality, we may assume that G^Σ preserves a set $\Delta = \{D_1, D_2, \ldots, D_p\}$ of p blocks of size q. Let $D \in \Delta$ and $B = \{\alpha, \beta\}$ for some $B \in D$. Let L be the subgroup of G that fixes the sets D_i, for $1 \leq i \leq p$, setwise. First suppose that $L \neq K$. Then L has p orbits of length $2q$ and, for a Sylow q-subgroup Q of L, $G = LN_G(Q)$, so $N_G(Q)$ is transitive on Σ. By minimality, $G = KN_G(Q)$. Let c be a p-element in $N_G(Q)$ acting nontrivially on Δ. Then, again by minimality, $G = KQ\langle c \rangle$. Now c^p fixes each $D \in \Delta$ setwise, and so normalizes $Q^D \simeq Z_q$. Since p does not divide $q - 1$ it follows that c^p centralizes Q^D and therefore fixes setwise each block of Σ in D, for each $D \in \Delta$, that is $c^p \in K$. But as K is a 2-group, this implies that $c^p = 1$.

Now $Q \leq \prod_{D \in \Delta} Q^D = Z_q^p$, so $Q \cong Z_q^a$ for some $a \leq p$. Since c normalizes Q,

$(Q_{(D)})^c = Q_{(D')}$ for $D' = D^c \in \Delta\backslash\{D\}$. It follows that either $Q_{(D)}$ fixes only the q blocks of Σ contained in D, or $Q = Z_q$. Similarly, since K is normal in G, both Q and $\langle c\rangle$ normalize K and it follows that one of (i) $K_{(B)}$ fixes only the block B pointwise, or (ii) $K_{(B)}$ fixes pointwise one block of Σ in each block of Δ and is transitive on the rest, or (iii) $K_{(B)}$ fixes pointwise all the blocks of Σ in D and is transitive on the rest, or (iv) $K = Z_2$. We shall analyze these possibilities according to the nature of the set of fixed points of $K_{(B)}$.

In case (i), since $K_{(B)}$ is transitive on B' for all $B' \in \Sigma\backslash\{B\}$, $\Gamma \simeq \Gamma_\Sigma[B]$, contradicting Lemma 5.1.

In case (ii), G preserves the block system $\Phi = \{(\text{fix } K_{(B)})^g | g \in G\}$ consisting of q blocks of size $2p$ with each block the union of p blocks of Σ. Since $Q^\Phi = (KQ)^\Phi$ is a normal subgroup of G^Φ and Q^Φ is transitive, $G^\Phi \lesssim AGL(1, q)$ and p does not divide $|G^\Phi|$ (since p does not divide $q-1$). We therefore have $K\langle c\rangle \leq G_{(\Phi)}$ and $G^\Phi = Q^\Phi \simeq Z_q$. Moreover $K.(Q \cap G_{(\Phi)})$ is normal in G and so the length of its orbits divides $|\text{fix } K_{(B)}| = 2p$. It follows that $Q \cap G_{(\Phi)} = 1$, that is $|Q| = q$. Thus $Q\langle c\rangle \cong Z_{pq}$, $K = \langle x_1, x_2, \ldots, x_d\rangle \cong Z_2^d$ for some $d \geq 2$, and by minimality $Q\langle c\rangle = \langle y\rangle \cong Z_{pq}$ acts irreducibly on K. It follows from Proposition 3.2 that Γ is a Cayley graph, which is a contradiction.

In case (iii), if $|Q| \geq q^2$ then Q_α is transitive on all $D' \in \Delta\backslash\{D\}$, and hence $Q_\alpha.K_{(B)}$ is transitive on $V\backslash\overline{D}$, where $\overline{D}$ is the union of the blocks of Σ contained in D. Thus $\Gamma \simeq \Gamma_\Delta[\overline{D}]$, contradicting Lemma 5.1. Hence $|Q| = q$ and $Q\langle c\rangle \cong Z_{pq}$. Thus $K = \langle x_1, x_2, \ldots, x_d\rangle \cong Z_2^d$ for some $d \geq 2$, and by minimality $Q\langle c\rangle = \langle y\rangle \cong Z_{pq}$ acts irreducibly on K. it follows from Proposition 3.2 that Γ is a Cayley graph which is a contradiction.

In case (iv), $|K| = 2$ and so $K \leq Z(G)$. Hence Q is normal in G and it follows that G has blocks of size q, which is a contradiction.

Thus $L = K$, so $G^\Sigma \simeq G^\Delta \lesssim S_p$, and G_B^Δ is a subgroup of G_D^Δ of index q. Let N denote the minimal normal subgroup of G^Δ. By Lemma 4.2(d), $N = PSL_m(r)$ where $p = (r^m - 1)/(r-1)$ and, by Lemma 4.3, m is an odd prime (since $p \neq 3$). Since $p \not\equiv 1(\text{mod } q)$, $(m, r) \neq (3, 2)$, and since $p \equiv 3(\text{mod } 4)$, $(m, r) \neq (3, 3)$. Hence $PSL_{m-1}(r)$ is a nonabelian simple group. As in the proof of Proposition 8.1, $PSL_{m-1}(r)$ has no subgroup of index q. It follows that $G_B/K \geq Z_r^{m-1}\cdot SL_{m-1}(r)$ and hence, by Lemma 4.4, that G_B/K (and thus G_B) is transitive on $\Sigma\backslash D$. Since $G_B = KG_\alpha$, G_α is transitive on $\Sigma\backslash D$. If $|K| \geq 4$, then, for $\alpha \in B$, $K_\alpha = K_{(B)}$ is normal in G_B, and $K_\alpha \neq 1$. If K_α is transitive on each block of Σ in $\Sigma\backslash D$, then G_α is transitive on $V\backslash\overline{D}$ and $\Gamma \simeq \Gamma_\Delta[\overline{D}]$, which contradicts Lemma 5.1. Hence K_α fixes a point of $V\backslash\overline{D}$, and since G_α is transitive on $\Sigma\backslash D$, K_α fixes $V\backslash\overline{D}$ pointwise. Since fix K_α is a block of imprimitivity for G, $|\text{fix } K_\alpha|$ divides $2pq$ while $|\text{fix } K_\alpha| \geq |V\backslash\overline{D}| = 2q(p-1)$, and we have a contradiction. Hence $|K| = 2$ and $K = Z(G)$. If $K \not\leq G'$ (where G' is the derived subgroup of G), then $G \geq K \times G'$, $G' \geq PSL_m(r)$, and by minimality, G' is intransitive. Since G has no blocks of length p or pq, G' must have q orbits of length $2p$, but then q divides $|G : K \times G'|$, and if x is a q-element which permutes the G'-orbits, then $\langle G', x\rangle$

would be a transitive proper subgroup of G, which is a contradiction. Hence $K \leq Z(G) \cap G'$. So K is contained in the Schur multiplier of $PSL_m(r)$. But (see [12]), since m is an odd prime and $p = (r^m - 1)/(r - 1)$ is prime, the Schur multiplier of $PSL_m(r)$ has order $(m, r - 1)\delta$ where either $\delta = 1$ or $(\delta, m, r) = (2, 3, 2)$. But since $(m, r) \neq (3, 2)$, this is a contradiction. Hence there are no examples with $|\Sigma| = pq$. This completes the proof of Proposition 8.2. □

The results in Sections 5–8, namely Propositions 5.1, 6.1, 7.2, and 8.2, together complete the proof of Theorem 2.

References

1. B. Alspach and T.D. Parsons, "A construction for vertex-transitive graphs," *Canad. J. Math.* **34** (1982), 307–318.
2. B. Alspach and R.J. Sutcliffe, "Vertex-transitive graphs of order 2p," *Ann. New York Acad. Sci.* **319** (1979), 18–27.
3. A.E. Brouwer, A.M. Cohen, and A. Neumaier, *Distance-Regular Graphs*, Springer-Verlag, Berlin, 1989.
4. P.J. Cameron, "Finite permutation groups and finite simple groups," *Bull. London Math. Soc.* **13** (1981), 1–22.
5. P.J. Cameron, P.M. Neumann, and D.N. Teague, "On the degrees of primitive permutation groups," *Math. Z.* **180** (1982), 141–149.
6. J.J. Cannon, "An introduction to the group theory language Cayley," in (Atkinson, M., ed.), *Computational Group Theory (Proc. of LMS Meeting, Durham)* Academic Press, 1982, pp. 145–183.
7. J.H. Conway, R.T. Curtis, S.P. Norton, R.A. Parker, and R.A. Wilson, *Atlas of Finite Groups*, (Clarendon Press, Oxford, England, 1985).
8. B.N. Cooperstein, "Minimal degree for a permutation representation of a classical group," *Israel J. Math.* **30** (1978), 213–235.
9. L.E. Dickson, *Linear Groups with an Exposition of the Galois Field Theory*, Dover, New York, 1958.
10. R. Frucht, J. Graver, and M.E. Watkins, "The groups of the generalized Petersen graphs," *Proc. Cam. Phil. Soc.* **70** (1971), 211–218.
11. D. Gorenstein, *Finite Groups*, Harper and Row, New York, 1968.
12. D. Gorenstein and R. Lyons, "The local structure of finite groups of characteristic 2 type," *Mem. Amer. Math. Soc.* **42** (276), p. 72, 1983.
13. R. Guralnick, "Subgroups of prime power index in a simple group," *J. Alg.* **81** (1983), 304–311.
14. M.W. Liebeck, "The affine permutation groups of rank three," *Proc. London Math. Soc.* **54** (1987), 477–516.
15. M.W. Liebeck, C.E. Praeger, and J. Saxl, "A classification of the maximal subgroups of the finite alternating and symmetric groups," *J. Alg.* **111** (1987), 365–383.
16. M.W. Liebeck and J. Saxl, "Primitive permutation groups containing an element of large prime order," *J. London Math. Soc. (2)* **31** (1985), 237–249.
17. B.D. McKay, "Transitive graphs with fewer than twenty vertices," *Math. Comp.* **33** (1979), 1101–1121, and a microfiche supplement.
18 B.D. McKay, "Nauty user's guide (version 1.5)," Technical report TR-CS-90-02, Computer Science Department, Australian National University, 1990.
19. B.D. McKay and C.E. Praeger, "Vertex-transitive graphs which are not Cayley graphs, I," *J. Austral. Math. Soc.(A)* to appear.
20. B.D. McKay and C.E. Praeger, "Vertex-transitive graphs which are not Cayley graphs, II," preprint (1992).

21. B.D. McKay and G.F. Royle, "The transitive graphs with at most 26 vertices," *Ars Combinatoria* to appear.
22. D. Marušič, "Cayley properties of vertex symmetric graphs," *Ars Combin.* **16B** (1983), 297–302.
23. D. Marušič, "Vertex-transitive graphs and digraphs of order p^k," *Ann. of Disc. Math.* **27** (1985), 115–128.
24. D. Marušič and R. Scapellato, "Characterising vertex-transitive *pq*-graphs with an imprimitive automorphism group," *J. Graph Theory*, **16** (1992), 375–387.
25. D. Marušič and R. Scapellato, "Imprimitive representations of SL(2, 2^k)," *J. Combin. Theory (B)*, to appear.
26. C.E. Praeger and M.Y. Xu, "Vertex-primitive graphs of order a product of two distinct primes," *J. Combin. Theory (B)*, to appear.
27. G.F. Royle and C.E. Praeger, "Constructing the vertex-transitive graphs of order 24," *J. Symbolic Comput.* **8**, (1989), 309–326.
28. M. Schönert, et. al., "GAP: Groups, Algorithms and Programming," *Lehrstuhl D für Mathematik, RWTH Aachen* (1992).
29. L.H. Soicher, "GRAPE: a system for computing with graphs and groups," in *Groups and Computation* (eds. L. Finkelstein and W.M. Kantor) DIMACS Series in Discrete Mathematics and Theoretical Computer Science, **11** Amer. Math. Soc., 1993, pp. 287–291.
30. D.E. Taylor, "Two-graphs and doubly transitive groups," *J. Combin. Theory (A)* **61** (1992), 113–122.
31. R.J. Wang and M.Y. Xu, "A classification of symmetric graphs of order 3*p*," *J. Combin. Theory (B)*, **58** (1993), 197–216.
32. M.E. Watkins, "Vertex-transitive graphs which are not Cayley graphs," in *Cycles and Rays* (eds. G. Hahn et al.) Kluwer, Netherlands, 1990, pp. 243–256.
33. H. Wielandt, "Permutation groups through invariant relations and invariant functions," Lecture Notes, Ohio State University, Columbus, Ohio, 1969.