On vertex-imprimitive graphs of order a product of three distinct odd primes

Akbar Hassani*

Mohammad A. Iranmanesh †‡ and Cheryl E. Praeger §

Department of Mathematics
The University of Western Australia,
Nedlands, WA 6907, Australia
praeger@maths.uwa.edu.au

Dedicated to Anne Penfold Street.

Abstract

This paper is a contribution to the determination of all integers of the form pqr, where p, q, and r are distinct odd primes, for which there exists a vertex-transitive graph on pqr vertices which is not a Cayley graph. The paper deals with the situation in which there is a vertex-transitive subgroup G of automorphisms of such a graph which has a chain $1 < N < K < G$ of normal subgroups such that both N and K are intransitive on vertices and the N-orbits are proper subsets of the K-orbits.

*It was with great sadness that the second and third author learned of the death of their colleague Akbar Hassani of a heart attack on May 20, 1998, after this paper had been submitted for publication.

†Current address: Department of Mathematics, Iran University of Science and Technology, Narmak, Tehran 16844, Iran. iranmanesh@sun.iust.ac.ir

‡The second author was financially supported by the Ministry of Culture and Higher Education of the Islamic Republic of Iran. This paper will form part of his Ph.D. thesis.

§This paper forms part of ARC project A69800706.

1 Introduction

This paper is a contribution to the solution of a problem of Marušič concerning finite vertex-transitive graphs which are not Cayley graphs. Marušič [5] asked for a determination of the set $\mathcal{NC}$ of natural numbers n for which there exists a vertex-transitive graph of *order* n, that is on n vertices, which is not a Cayley graph. The elements of $\mathcal{NC}$ are called *non-Cayley numbers.* The set $\mathcal{NC}$ is closed under multiplication by arbitrary positive integers k, for if Γ is a non-Cayley, vertex-transitive graph of order n then the vertex-disjoint union of k copies of Γ is a non-Cayley, vertex-transitive graph of order kn. Thus it is important to understand which natural numbers with few prime divisors lie in $\mathcal{NC}$. The question of membership of $\mathcal{NC}$ has been settled for all natural numbers which are not square-free [9, 10], or are the twice the product of two distinct odd primes [2, 11].

We are concerned here with integers $n = pqr$ where p, q, r are distinct odd primes. By our remarks above we may assume that pq, qr, $pr \notin \mathcal{NC}$. Integers n of this form for which there exists a vertex-transitive graph Γ of order n, with $\mathrm{Aut}\,\Gamma$ quasiprimitive on vertices, were determined in [15]. (A permutation group is said to be *quasiprimitive* if every non-identity normal subgroup is transitive.) Thus we need to determine the integers n of this form for which there exists a vertex-transitive graph Γ of order n for which $\mathrm{Aut}\,\Gamma$ is not quasiprimitive on vertices, that is, $\mathrm{Aut}\,\Gamma$ is transitive on vertices and has a non-identity intransitive normal subgroup, N say. The set of N-orbits forms an $(\mathrm{Aut}\,\Gamma)$-invariant partition of the vertex set in the sense that elements of $\mathrm{Aut}\,\Gamma$ permute the N-orbits amongst themselves. We say that the set of orbits of a normal subgroup of a transitive permutation group is a *normal partition*; the orbits of a normal subgroup are *blocks of imprimitivity* for the group. Since $n = pqr$, either the length of the N-orbits or the number of N-orbits is a prime. We are especially concerned in this paper with the case where $\mathrm{Aut}\,\Gamma$ has a vertex-transitive subgroup G such that there is a sequence of normal subgroups of G, $1 < N < K < G$, with both N and K intransitive on vertices, and the N-orbits being proper subsets of the K-orbits; such a group G is said to be *genuinely 3-step imprimitive* on vertices. Note that the lattice of G-invariant partitions of the vertex set, for such a group G, contains a chain of length 3 of normal partitions corresponding to this sequence of normal subgroups.

In addition to handling the quasiprimitive case, the paper [15] by Seress contains a construction of a family of non-Cayley, vertex-transitive graphs of order pqr which admit genuinely 3-step imprimitive subgroups of automorphisms. The construction is analogous to one in [11, Construction 2.1] of graphs of order $2pq$. Thus it is shown in [15] that, for $\{p, q, r\}$ in the

p	q	r	Conditions or Comments
$p \mid q-1$	$q \mid r-1$	–	–
–	$\frac{3p+1}{2}$	$3p+2$	–
–	$6p-1$	$6p+1$	–
$p \mid r+1$	$\frac{r-1}{2}$	–	possibly $p > q$ if $p = \frac{r+1}{2}$
$\frac{k^{d/2}+1}{k+1}$	$\frac{k^{d/2}-1}{k-1}$	$\frac{k^{d-1}-1}{k-1}$	$k, d-1, \frac{d}{2}$all prime
$\frac{k^{(d-1)/2}+1}{k+1}$	$\frac{k^{(d-1)/2}-1}{k-1}$	$\frac{k^{d}-1}{k-1}$	$k, d, \frac{d-1}{2}$all prime
k^2-k+1	$\frac{k^5-1}{k-1}$	$\frac{k^7-1}{k-1}$	$k$prime
3	$\frac{2^d+1}{3}$	2^d-1	$d$prime
$\frac{2^d+1}{3}$	2^d-1	$2^{2d\pm2}+1$	$d = 2^t \mp 1$prime
5	11	19	–
7	73	257	–

Table 1: $\{p, q, r\}$ as in Definition 1.1(iii)

following set $\mathcal{N}_3$ of triples, the product $pqr \in \mathcal{NC}$.

Definition 1.1. Let p, q, r be distinct odd primes. Then $\{p, q, r\} \in \mathcal{N}_3$ if and only if $pq, qr, pr \notin \mathcal{NC}$, and one of the following holds.

(i) $pqr = (2^{2^t}+1)(2^{2^{t+1}}+1)$, for some t, or $(2^{d\pm1}+1)(2^d-1)$, for some prime d;

(ii) re-ordering $\{p, q, r\}$ if necessary, we have qr equal to (a) $2p \pm 1$, or (b) $(p+1)/2$, or (c) $\frac{p^2+1}{2}$, or (d) $\frac{p^2-1}{24x}$ where $x = 1, 2$ or 5, or (e) 2^t+1, where p divides 2^t-1 for some t;

(iii) re-ordering $\{p, q, r\}$ if necessary, $p < q < r$ and p, q, r are as in one of the lines Table 1 on this page.

The purpose of this paper is to show that there are no further triples $\{p, q, r\}$ for which there is a non-Cayley, vertex-transitive graph of order pqr admitting a genuinely 3-step imprimitive subgroup of automorphisms.

Theorem 1.1. *Let p, q, r be distinct odd primes such that $pq, qr, pr \notin \mathcal{NC}$, and $\{p,q,r\} \notin \mathcal{N}_3$. Suppose that Γ is a vertex-transitive graph of order pqr which admits a genuinely 3-step imprimitive subgroup of automorphisms. Then Γ is a Cayley graph.*

The case where there is no genuinely 3-step imprimitive subgroup will be treated in a separate paper [3]. Quite different methods are required for that case than those used in this paper.

In Section 3 we give several preliminary results, mainly concerning graphs. Then in Section 4 we discuss two families of genuinely 3-step imprimitive permutation groups which will arise in our proof of Theorem 1.1. We show that every graph admitting a group from one of these two families, as a vertex-transitive subgroup of automorphisms, is a Cayley graph. Finally, in Section 5, we give the proof of Theorem 1.1.

For completeness we state the result from [7, 9, 10], which determines membership in $\mathcal{NC}$ of numbers of the form pq.

Proposition 1.2. *Suppose that p and q are distinct odd primes and $q < p$. Then $pq \in \mathcal{NC}$ 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) $(p, q) = (11, 7)$.

2 Notation

In this section we record some of the definitions and notation we will be using in the paper.

2.1 Notation for permutation groups

If a group G acts on a set Σ then we write G^Σ for the permutation group on Σ induced by G, and we write g^Σ for the permutation of Σ induced by g, for each $g \in G$. In Lemma 3.2 we introduce a more restrictive meaning for this symbol which will only apply in Lemma 3.2 and its applications.

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 $\Delta_0 = \{(\alpha, \alpha) \mid \alpha \in V\}$ 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 set $\Delta(\alpha) := \{\beta \mid (\alpha, \beta) \in \Delta\}$ where Δ is an orbital. For each orbital Δ, the set $\Delta^* := \{(\beta, \alpha) \mid (\alpha, \beta) \in \Delta\}$ 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. A union of orbitals, say Θ, is called a *generalised orbital* and Θ is said to be *self-paired* if, whenever an orbital $\Delta \subseteq \Theta$ then also the paired orbital $\Delta^* \subseteq \Theta$. Let Θ be a union of orbitals which is self-paired and such that $\Delta_0 \not\subseteq \Theta$. The *generalised 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. If Θ consists of a single self-paired orbital then $\Gamma^{(\Theta)}$ is called an *orbital graph*.

Let V be a set and $G \leq \mathrm{Sym}(V)$. A partition $\mathcal{P}$ of V is said to be *G-invariant* if the elements of G permute the parts of V *blockwise*, that is, $P^g \in \mathcal{P}$ for all $P \in \mathcal{P}$ and $g \in G$ (where $P^g := \{\alpha^g \mid \alpha \in P\}$). The *trivial partitions* $\{V\}$ and $\{\{\beta\} \mid \beta \in V\}$ are G-invariant for all transitive groups G, and a transitive permutation group G on V is said to be *primitive* on V if these are the only G-invariant partitions of V. If G is transitive, but not primitive on V, then G is said to be *imprimitive* on V. Also a non-empty subset B of V is a *block of imprimitivity* for G in V if, for all $g \in G$, either $B^g = B$ or $B^g \cap B = \emptyset$. It is not difficult to show that B is a block of imprimitivity for G if and only if $\{B^g \mid g \in G\}$ is a G-invariant partition of V. For this reason a G-invariant partition of V is sometimes called a *system of blocks of imprimitivity* or simply *block system*. For a block system Σ and $B \in \Sigma$, we denote by $G_{(\Sigma)}$ and G_B the subgroup of G fixing each block in Σ setwise, and fixing B setwise respectively.

A permutation group G on V is said to be *regular* on V if it is transitive on V and the only element of G which fixes a point of V is the identity. For any subgroup $G \leq \mathrm{Sym}(V)$ we denote by $\mathrm{fix}_V(G)$ the subset of points of V which are fixed by G, that is $\{\alpha \in V \mid \alpha^g = \alpha \text{ for all } g \in G\}$. By $H \wr K$ we mean the *wreath product* of H and K. For a finite group G and a set of primes π, a subgroup $H \leq G$ is called a *Hall π-subgroup* if every prime dividing $|H|$ belongs to π, and π contains no prime dividing $|G : H|$.

2.2 Graph theoretic notation

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 $\Gamma = (V, E)$. By $\mathrm{Aut}\,\Gamma$ we mean the full automorphism group of $\Gamma = (V, E)$, that is, the subgroup of $\mathrm{Sym}(V)$ that preserves E, and we say that Γ is *vertex-transitive* if $\mathrm{Aut}\,\Gamma$ acts transitively on V.

For a group G and a subset S of G such that $1 \notin S$ and $S = S^{-1}$, where $S^{-1} = \{s^{-1} \mid s \in S\}$, the *Cayley graph* $\mathrm{Cay}(G, S)$ of G relative to S is the graph with vertex set G such that $\{g, h\}$ is an edge if and only if there exists $s \in S$ such that $g = sh$. Every Cayley graph $\mathrm{Cay}(G, S)$ for G admits the group G acting by right multiplication ($g : x \longmapsto xg$) as a group of automorphisms acting regularly on vertices. Thus $\mathrm{Cay}(G, S)$ is a vertex-transitive graph. Conversely, see [1], a vertex-transitive graph Γ is isomorphic to a Cayley graph for some group if and only if $\mathrm{Aut}\,\Gamma$ has a subgroup which is regular on vertices. There are vertex-transitive graphs which are not Cayley graphs. For example, the *Petersen graph* on 10 vertices is a non-Cayley, vertex-transitive graph. Thus $10 \in \mathcal{NC}$ and in fact 10 is the least non-Cayley number.

If $\Gamma = (V, E)$ is a graph and 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* $\bar{B}$ is the graph with vertex set B and edge set $\{\{\alpha, \beta\} \in E \mid \alpha, \beta \in B\}$. 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 $\bar{B}$, for $B \in \Sigma$, is independent (up to isomorphism) of the choice of B. The two graphs, Γ_Σ and $\bar{B}$ will be analysed in detail for many pairs G, Σ in this paper.

For a graph $\Gamma = (V, E)$ and a vertex $\alpha \in V$, we denote by $\Gamma_1(\alpha)$, or simply $\Gamma(\alpha)$, the set $\{\beta \mid \{\alpha, \beta\} \in E\}$ of *neighbours* of α in Γ. Two disjoint nonempty subsets U, W of V are said to be *trivially joined* if either, for all $\alpha \in U$, we have $W \subseteq \Gamma(\alpha)$, or for all $\alpha \in U$, we have $\Gamma(\alpha) \cap W = \emptyset$. 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 two vertices (α_1, β_1) and (α_2, β_2) are adjacent if and only if either $\{\alpha_1, \alpha_2\} \in E_1$ or $\alpha_1 = \alpha_2$ and $\{\beta_1, \beta_2\} \in E_2$.

3 Preliminary results

The following theorem which can be found in [12, Theorem 2.1] is one of the most important facts about generalised orbital graphs of transitive permutation groups. It underlies all of our analysis in later sections.

Theorem 3.1. *A group G is a vertex-transitive subgroup of automorphisms of a graph Γ if and only if Γ is a generalised orbital graph for G, namely for the self-paired generalised orbital $\Delta := \{\{\alpha,\beta\} \mid \{\alpha,\beta\} \in E\}$.*

In other words every graph admitting a vertex-transitive subgroup G of automorphisms is a generalised orbital graph for G corresponding to some self-paired union of orbitals. The next lemma which was proved in [11] is useful for proving that a graph Γ contains a larger group of automorphisms than a given group. Note that in this lemma, for a graph $\Gamma = (V, E)$ and an automorphism h which fixes a subset $U \subseteq V$ setwise, h^U will denote the permutation of V which fixes $V \backslash U$ pointwise and which induces the same permutation of U as h does.

Lemma 3.2. *[11, Lemma 3.1] Let $\Gamma = (V, E)$ be a finite graph, and suppose that $\{U, W_1, \ldots, W_t\}$ is a partition of V, where $t \geq 1$. Let H be a subgroup of $\operatorname{Aut}\Gamma$ 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 $\operatorname{Aut}\Gamma$.*

The next lemma can sometimes be used to prove that a graph has the structure of a nontrivial lexicographic product. It can often be applied after an application of Lemma 3.2 above.

Lemma 3.3. *Let $\Gamma = (V, E)$ be a graph and $G \leq \operatorname{Aut}\Gamma$ be such that G is imprimitive on V with block system Σ. Let $B \in \Sigma$. If there exists $H < G$ such that H fixes $B \in \Sigma$ pointwise and H is transitive on every $B' \in \Sigma \backslash \{B\}$, then $\Gamma \cong \Gamma_\Sigma[\bar{B}]$.*

Proof. By assumption each block $B' \in \Sigma$ is trivially joined to every point of B. Hence by [14, Lemma 1.1], $\Gamma \cong \Gamma_\Sigma[\bar{B}]$. □

If both Γ_1 and Γ_2 are Cayley graphs, it turns out that the lexicographic product $\Gamma_1[\Gamma_2]$ is also a Cayley graph.

Lemma 3.4. *Suppose that $\Gamma_1 = (V_1, E_1)$ and $\Gamma_2 = (V_2, E_2)$ are Cayley graphs of orders m and n respectively. Then the lexicographic product $\Gamma_1[\Gamma_2]$ of Γ_1 and Γ_2, is a Cayley graph.*

Proof. Suppose that M and N are regular subgroups of $\operatorname{Aut}\Gamma_1$ and $\operatorname{Aut}\Gamma_2$ respectively, so $|N| = n$ and $|M| = m$. Then $K := M \wr N = M^n.N$ is a subgroup of $\operatorname{Aut}\Gamma_1 \wr \operatorname{Aut}\Gamma_2$ which is transitive on $V_1 \times V_2$ (see [13] pages 32-33). Let

$$D := \{(x, x, \ldots, x) \mid x \in M\} \leq M^n.$$

From the definition of multiplication in the wreath product $M \wr N$, D and N centralise each other. Also $D \cap N = 1$, and hence $D \times N$ is a subgroup of K. Since $D \cong M$, (and D and N centralise each other) we conclude that $D \times N$ is transitive on $V_1 \times V_2$ and has order mn. Thus $D \times N$ is regular on $V_1 \times V_2$. So $\operatorname{Aut}\Gamma_1 \wr \operatorname{Aut}\Gamma_2$ (and thereforeAut $\Gamma_1[\Gamma_2]$) has a regular subgroup. Hence $\Gamma_1[\Gamma_2]$ is a Cayley graph. □

We shall need the following result about Hall π-subgroups, sometimes called the *Frattini argument.*

Lemma 3.5. *Let $1 \neq K \lhd G$ and π be a nonempty set of primes. Also suppose that*

(i) there exists a Hall π-subgroup H of K, and

(ii) all Hall π-subgroups of K are conjugate in K.

Then $G = K\mathrm{N}_G(H)$.

Proof. Let $g \in G$. Since $|K : H^g| = |K : H|$ is a π'-number, H^g is a Hall π-subgroup of K, and since all Hall π-subgroups of K are conjugate in K there exists a $k \in K$ such that $H^g = H^k$, so $gk^{-1} \in \mathrm{N}_G(H)$. Therefore $G = K\mathrm{N}_G(H)$. □

4 Some minimal transitive groups and their graphs

In our analysis of this problem we need to deal with several families of transitive permutation groups of degree pqr. We present these families of groups here, with the information we need about them. Our first family of groups is similar to the family studied in [11, Proposition 3.1]. We denote $\mathbb{Z}_p \backslash \{0\}$ by $\mathbb{Z}_p{}^*$. Recall that, for $x \in \mathbb{Z}_p{}^*$, $o(x \mod p)$ is the least positive integer i such that $x^i \equiv 1 \pmod p$. Let $c \in \{1,2\}$ and $e \in \mathbb{Z}_q{}^*$ with $o(e^p \bmod q) = r^{c-1}$. We define a group G by generators and relations as follows

$$G = \langle a_1, \ldots, a_r, y \mid y^{r^c p} = a_i{}^q = [a_i, a_j] = 1 \text{ for all } i, j,$$
$$a_i^y = a_{i+1} \text{ for } i \le r-1 \text{ and } a_r{}^y = a_1{}^e\rangle. \qquad (1)$$

Note that the above relations and generators form a *power-conjugate presentation* or *AG-System* for G [4].

Proposition 4.1. *Let p, q, and r be distinct odd primes such that p divides $q-1$. Suppose that $\Gamma = (V, E)$ is a graph of order pqr admitting the group G defined in* (1) *as a vertex-transitive group of automorphisms, where the action of G on V is such that, for some $\alpha \in V$, $G_\alpha = \langle a_2, \ldots, a_r, y^{rp}\rangle$. Then Γ is a Cayley graph.*

Proof. Set $H = G_\alpha$ and $Q = \langle a_1, \ldots, a_r\rangle$. The action of G on V is equivalent to its action by right multiplication on $\{Hg \mid g \in G\}$. The set $T = \{a_1{}^i y^j \mid 0 \le i \le q-1, 0 \le j \le rp-1\}$ is a set of coset representatives for H in G, and so we may identify V with T in such a way that $\alpha = 1_G$ and $g \in G$ maps $t \in T$ to $\overline{tg} \in T$ where for $x \in G$, we write $\bar{x}$ for the unique element of T such that $Hx = H\bar{x}$. With this identification, the actions of the generators $a_1, \ldots a_r, y$, and the element y^{rp} are given as follows. (Note that $a_i{}^{y^r} = a_i{}^e$ for all i, so $a_i{}^{y^{pr}} = a_i{}^{e^p}$ for all i; also $ya_\ell = a_{\ell-1}y$ if $\ell \ge 2$ and $ya_1 = a_r{}^{e^{-1}}y$, where e^{-1} is the element of $\mathbb{Z}_q$ such that $ee^{-1} = 1$ in $\mathbb{Z}_q$.)

$$y : a_1^i y^j \longmapsto \begin{cases} a_1^i y^{j+1} & \text{if } 0 \le j \le pr-2 \\ a_1^{ie^p} & \text{if } j = pr-1 \end{cases}$$

$$y^{pr} : a_1^i y^j \longmapsto a_1^{ie^p} y^j$$

$$a_\ell : a_1^i y^j \longmapsto \begin{cases} a_1^i y^j & \text{if } j \not\equiv \ell - 1 \pmod r \\ a_1^{i+e^{-k}} y^j & \text{if } j = kr + \ell - 1 \text{ and } 0 \le k \le p-1. \end{cases}$$

That the actions of y and y^{pr} are as claimed follows from our remarks above. To see that the action claimed for a_ℓ is correct, note that if $j = kr+j'$ where $0 \le k \le p-1$ and $0 \le j' \le r-1$, then if $j' \ne \ell - 1$ then $a_1^i y^j a_\ell \in Ha_1^i y^j$, so a_ℓ fixes $a_1^i y^j$, while if $j' = \ell - 1$ then $a_1^i y^j a_\ell = a_1^i y^{kr} a_1 y^{j'} = a_1^{i+e^{-k}} y^j$.

The set Σ of Q-orbits in $T = V$ is a block system for G. It consists of pr blocks of size q, namely $B_j = \{a_1^i y^j \mid 0 \le i \le q-1\}$, for $0 \le j \le pr-1$. Our next task is to identify all of the H-orbits in V and find the paired orbits for each of them. From the actions determined above we see that y^{pr} and each of the a_i fixes setwise each block $B_j \in \Sigma$. Moreover, if $j \not\equiv 0 \pmod r$ then there exists ℓ such that $2 \le \ell \le r$ and $j \equiv \ell - 1 \pmod r$; hence $a_\ell \in H$ and $\langle a_\ell \rangle$ is transitive on B_j. Thus for $0 \le j \le pr-1$ and $j \not\equiv 0 \pmod r$, $\Delta_j(\alpha) = B_j$ is an H-orbit. Since y^{-j} maps the pair $(1, y^j)$ to $(y^{pr-j}, 1)$ it follows that the H-orbit $\Delta_j{}^*(\alpha)$ paired with $\Delta_j(\alpha)$ is $\Delta_{pr-j}(\alpha)$. Consider now $j = kr$ where $0 \le k \le p-1$. The group $Q \cap H = \langle a_2, a_3, \ldots, a_\ell \rangle$ fixes each of the points $a_1^i y^j$, so the H-orbit containing $a_1^i y^j$ is equal to the $\langle y^{pr} \rangle$-orbit containing $a_1^i y^j$. If $e^p = 1$ in $\mathbb{Z}_q$ then H has qr orbits $\Delta_{i,j}(\alpha) = \{a_1^i y^j\}$ of length 1, and since $y^{-j} a_1^{-i}$ maps $(1, a_1^i y^j)$ to $(a_1^{-e^k i} y^{pr-j}, 1)$ it follows that

$$\Delta_{i,kr}{}^*(\alpha) = \Delta_{-e^k i,(p-k)r}(\alpha)$$

(reading the first subscript modulo r). On the other hand if $o(e^p \mod q) = r$ then we see from the action of y^{pr} that $\langle y^{pr} \rangle$ fixes the point y^j and has $(q-1)/r$ orbits of length r in B_j. Thus the H-orbits in B_j are $\Delta_{0,kr}(\alpha) = \{y^{kr}\}$ and $\Delta_{d,kr}(\alpha) = \{a_1^i y^{kr} \mid i \in d\}$ for each coset d of the multiplicative subgroup $\langle e^p \rangle$ of $\mathbb{Z}_q{}^*$ of order r. Arguing as above

$$\Delta_{0,kr}{}^*(\alpha) = \Delta_{0,(p-k)r}(\alpha)$$

(where we have to read $(p-k)r$ modulo pr if $k = 0$) and

$$\Delta_{d,kr}{}^*(\alpha) = \Delta_{-e^k d,(p-k)r}(\alpha)$$

for each coset d of $\langle e^p \rangle$ in $\mathbb{Z}_q{}^*$. (Note that $-e^k d$ is a coset whenever d is, and $-d \neq d$.) In the case where $e^p = 1$, each coset of $\langle e^p \rangle$ is a singleton subset of $\mathbb{Z}_q$. Thus in this case also we may use the notation $\Delta_{d,kr}(\alpha)$ for $\Delta_{i,kr}(\alpha)$ where $d = \{i\}$.

By Theorem 3.1 any graph Γ with vertex set $V = T$ admitting G as a vertex-transitive subgroup of automorphisms is a generalised orbital graph for G and the set $\Gamma(\alpha)$ of vertices adjacent to α is a union of H-orbits in $V \backslash \{\alpha\}$ which is closed under pairing. Thus

$$\Gamma(\alpha) = \Big(\bigcup_{(d,j) \in K} \Delta_{d,j}(\alpha) \Big) \cup \Big(\bigcup_{j \in J} \Delta_j(\alpha) \Big)$$

where $J \subseteq \{j \mid 0 < j < pr, j \not\equiv 0 \pmod r\}$ and $j \in J$ implies $pr - j \in J$; and $K \subseteq (\{0\} \cup \{i\langle e^p\rangle \mid i \in \mathbb{Z}_q{}^*\}) \times \{kr \mid 0 \le k \le p-1\}$ is such that $(d, kr) \in K$ implies $(-e^k d, (p-k)r) \in K$ (where the second entry must be read modulo pr if $k = 0$). Now we apply Lemma 3.2 to the the group H and the partition of V with parts $C_0 := \bigcup_{k=0}^{p-1} B_{kr}$, and the B_j with $j \not\equiv 0 \pmod r$. Suppose that there is an edge e from some point $a_1^i y^{kr} \in C_0$ to a point $a_1^{i'} y^{j'}$ in $B_{j'}$ where $j' \not\equiv 0 \pmod r$. Then $y^{-kr} a_1^{-i}$ maps e to an edge e', where $e' = \{1, a_1^{i'} y^{j'-kr}\}$ if $j' \ge kr$ and is $\{1, a_1^{i' e^{-p}} y^{j'+(p-k)r}\}$ if $j' < kr$. Thus J contains $j'' = j' - kr$ (if $j' \ge kr$) or $j'' = j' + (p-k)r$ (if $j' < kr$), and it follows that $\alpha = 1_G$ is joined to each point of $B_{j''}$. Applying $a_1{}^{i'} y^{kr} \in G$, for all i', to these edges we conclude that every point of B_{kr} is joined by an edge to every point of $B_{j'}$. Since B_{kr} is a union of H-orbits, it follows that every H-orbit in C_0 is trivially joined to every $B_{j'}$ for $j' \not\equiv 0 \pmod r$. Hence by Lemma 3.2, the group $H^{C_0} = \{h^{C_0} \mid h \in H\} \le \operatorname{Aut}\Gamma$. (Here h^{C_0} denotes the permutation of V which is equal to h in its action on points of C_0, and fixes $V \backslash C_0$ pointwise.) In particular $u_0 := (y^{pr})^{C_0} \in \operatorname{Aut}\Gamma$. For each $\ell = 0, \ldots, r-1$, set $C_\ell := B_\ell \cup B_{\ell+r} \cup \cdots \cup B_{\ell+(p-1)r}$, and $u_\ell := (y^{pr})^{C_\ell}$. Then $u_{\ell+1} = u_\ell{}^y$ for $\ell = 0, 1, \ldots, r-2$ and $u_{r-1}^y = u_0$; and each $u_\ell \in \operatorname{Aut}\Gamma$.

Now we wish to find a regular subgroup R of $A = \langle G, u_0, \ldots, u_{r-1}\rangle \le \operatorname{Aut}\Gamma$. Recall that this will imply that Γ is a Cayley graph. Suppose first that $|y| = pr$, so $e^p = 1$. If r does not divide $q-1$ then the map $x \longmapsto x^r$ is a bijection on $\mathbb{Z}_q{}^*$, and so there exists $m \in \mathbb{Z}_q{}^*$ such that $m^r \equiv e \pmod q$. Also if r divides $q-1$ then, since in this case $o(e \mod q) = 1$ or p, e is an r^{th} power, so again there exists $m \in \mathbb{Z}_q{}^*$ such that $m^r \equiv e \pmod q$. Set $a := a_1{}^{m^{r-1}} a_2{}^{m^{r-2}} \ldots a_{r-1}{}^m a_r$. Then $\langle a\rangle$ is transitive on every block of Σ, $|a| = q$, and

$$a^y = a_2{}^{m^{r-1}} a_3{}^{m^{r-2}} \ldots a_r{}^m a_1{}^e = (a_1{}^{m^{r-1}} a_2{}^{m^{r-2}} \ldots a_{r-1}{}^m a_r)^m = a^m.$$

Thus y normalises $\langle a\rangle$ and $\langle a, y\rangle$ is regular on V.

Suppose now that $|y| = r^2 p$. Since $p \ne r$, there exists an integer f such that $fp \equiv -1 \pmod r$, say $fp = kr - 1$. Set $m := e^k \in \mathbb{Z}_q$. Note that $m^r = e^{kr} = e^{1+fp} \in \mathbb{Z}_q$. Now set $z := y u_0{}^f$. Then in their actions on Σ,

$z^\Sigma = y^\Sigma$, so $|z|$ is divisible by pr and $\langle z\rangle$ is transitive on Σ; also

$$\begin{aligned} z^r &= (yu_0{}^f)^r = y^r(u_0{}^f)^{y^{r-1}}(u_0{}^f)^{y^{r-2}}\dots(u_0{}^f)^y(u_0)^f \\ &= y^r(u_{r-1})^f(u_{r-2})^f\dots(u_1)^f(u_0)^f = y^r(u_{r-1}u_{r-2}\dots u_1u_0)^f \\ &= y^{r+prf} = y^{r^2k}, \end{aligned}$$

so $z^{pr} = y^{r^2pk} = 1$. Further $\langle a\rangle$ is transitive on every block of Σ, so $\langle a, z\rangle$ is transitive on V; note that, since $u_0 = (y^{pr})^{C_0}$, it follows that u_0 centralises $a_2, \dots, a_r$. Thus,

$$\begin{aligned} a^z &= (a_1{}^{m^{r-1}}a_2{}^{m^{r-2}}\dots a_r)^{yu_0{}^f} = (a_2{}^{m^{r-1}}a_3{}^{m^{r-2}}\dots a_r{}^m a_1{}^e)^{u_0{}^f} \\ &= a_2{}^{m^{r-1}}a_3{}^{m^{r-2}}\dots a_r{}^m(a_1{}^e)^{y^{prf}} = a_2{}^{m^{r-1}}a_3{}^{m^{r-2}}\dots a_r{}^m a_1{}^{e^{1+pf}} \\ &= a_2{}^{m^{r-1}}a_3{}^{m^{r-2}}\dots a_r{}^m a_1{}^{m^r} = a^m. \end{aligned}$$

(Recall that $e^{1+pf} = e^{kr} = m^r$.) Hence $\langle a\rangle$ is normalised by z, and so $\langle a, z\rangle$ has order pqr, and hence is regular on V. This completes the proof of Proposition 4.1. □

Now we introduce the next family of groups. For $2 \le t \le r$ let $\beta_1, \dots, \beta_t \in \mathbb{Z}_q$ with $\beta_1 \ne 0$, let $\delta \in \mathbb{Z}_p$ with $\delta^r \equiv 1 \pmod p$, and let $n \in \mathbb{Z}_q$, with $o(n \bmod q) = r^{\varepsilon-1}$, where $\varepsilon = 1$ or 2 (so $n = 1$ if $\varepsilon = 1$). In the case where $\varepsilon = 2$, set $t = r$, $\beta_2 = \dots = \beta_t = 0$ and $\beta_1 = n$. We define a group G by generators and relations in terms of these parameters as follows

$$G = \langle a_1, a_2, \dots, a_t, c, x \mid a_i^q = c^p = x^{r^\varepsilon} = [a_i, a_j] = [a_i, c] = 1 \text{ for all } i, j,$$

$$a_i{}^x = a_{i+1} \text{ for } i \le t-1; \text{ and } a_t{}^x = a_1{}^{\beta_1}\dots a_{t-1}{}^{\beta_{t-1}}, c^x = c^\delta\rangle. \quad (2)$$

Note that $[c, x^r] = 1$.

Proposition 4.2. *Let p, q, r be distinct odd primes. Suppose that $\Gamma = (V, E)$ is a graph of order pqr which admits the group G defined in (2) as a vertex-transitive subgroup of automorphisms, where the action of G on V is such that, for some $\alpha \in V$, $G_\alpha = \langle a_2, \dots, a_t, x^r\rangle$. Then Γ is a Cayley graph.*

Proof. Set $H = G_\alpha$. The set $T = \langle a_1, c\rangle \cup \langle a_1, c\rangle x \cup \dots \cup \langle a_1, c\rangle x^{r-1}$ is a set of right coset representatives for H in G, and so we may identify V with

T in such a way that $\alpha = 1_G$ and $g \in G$ maps $t \in T$ to $\overline{tg} \in T$ where, for $x \in G$, we denote by $\overline{x}$ the unique element of T such that $Hx = H\overline{x}$. First we determine the actions on T of the generators and of the element x^r. For $\delta \in \mathbb{Z}_p{}^*$, by δ^{-1} we denote the element in $\mathbb{Z}_p$ such that $\delta^{-1}\delta \equiv 1 \pmod p$.

$$c : a_1^i c^j x^m \longmapsto a_1^i c^{j+\delta^{-m}} x^m$$

$$x : a_1^i c^j x^m \longmapsto \begin{cases} a_1^i c^j x^{m+1} & \text{if } 0 \leq m \leq r-2 \\ a_1^{in} c^j & \text{if } m = r-1 \end{cases} .$$

(Recall that $n = 1$ if $\varepsilon = 1$.) Thus the action of x^r is given by

$$x^r : a_1^i c^j x^m \longmapsto a_1^{in} c^j x^m.$$

The set of orbits of the normal subgroup $Q = \langle a_1, a_2, \ldots, a_t \rangle$ of G is a block system for G. It consists of pr blocks of size q and we denote them by $B_{j,k} = (c^j x^k)^Q = \{a_1^i c^j x^k \mid i \in \mathbb{Z}_q\}$, for $j \in \mathbb{Z}_p$, $k \in \mathbb{Z}_r$. Let $D = \{d_1, d_2, \ldots, d_{(q-1)/r^{\varepsilon-1}}\}$ denote the set of cosets of the multiplicative subgroup $\langle n \rangle$ in $\mathbb{Z}_q{}^*$. For $a \in Q$, since Q is a normal subgroup of G, we have $c^j x^m a \in c^j x^m Q = Q c^j x^m$, and so (since $Q \cap H = \langle a_2, \ldots, a_t \rangle$) $c^j x^m a \in H a_1{}^{\alpha_1} c^j x^m$ for some $\alpha_1 \in \mathbb{Z}_p$, depending on a, j and m. If $a = a_k$ then we write $\alpha_1 = \alpha(k, j, m)$. Moreover in the case where $\varepsilon = 2$, $x a_\ell = a_{\ell-1} x$ if $\ell \geq 2$, and $x a_1 = a_r{}^{n^{-1}} x$, where n^{-1} is the element of $\mathbb{Z}_q{}^*$ such that $nn^{-1} \equiv 1 \pmod q$. Hence $x^m a_\ell \in \langle a_{\ell-m} \rangle x^m$ (where the subscript $\ell - m$ is to be read modulo r), and so $\alpha(k, j, m)$ is 0 if $\ell \not\equiv m+1$ and is 1 if $\ell = m+1$. Thus the action of a_ℓ on an arbitrary element $a_1{}^i c^j x^m$ of T, in the case $\varepsilon = 2$, is as follows.

$$a_\ell : a_1^i c^j x^m \longmapsto \begin{cases} a_1^{i+1} c^j x^m & \text{if } 0 \leq m \leq r-1 \text{ and } \ell = m+1 \\ a_1^i c^j x^m & \text{if } 0 \leq m \leq r-1 \text{ and } \ell \not\equiv m+1. \end{cases}$$

In the case where $\varepsilon = 1$, the action of a_ℓ on an arbitrary element $a_1{}^i c^j x^m$ of T is given by:

$$a_\ell : a_1^i c^j x^m \longmapsto a_1^{\alpha(\ell,j,m)+i} c^j x^m$$

where $0 \leq i \leq q-1$, $0 \leq j \leq p-1$ and $0 \leq m \leq r-1$. Note that $\alpha(\ell, j, 0) = 0$ for each l, j, since c centralises Q.

Now we show that the set $F =$ of fixed points of H in V is contained in $\bigcup_{j=0}^{p-1} B_{j,0}$. If $\varepsilon = 2$ then $t = r$ and, for each $k \in \mathbb{Z}_r{}^*$, $\langle a_{k+1} \rangle$ is transitive on $B_{j,k}$ and $a_{k+1} \in H$. Thus in this case $F \subseteq \bigcup_{j=0}^{p-1} B_{j,0}$. Now consider the case $\varepsilon = 1$. Set $P = \langle c \rangle$. In this case $H \leq Q$ and we have $Q = \langle H, a_1 \rangle$ and $Q \times P \subseteq \mathrm{N}_G(H)$. Since $Q \times P$ is maximal in G, and since H is not normal in G, we have $\mathrm{N}_G(H) = Q \times P$. Now $\mathrm{N}_G(H)$ is transitive on F (see [16, Theorem 3.6]) and $|F| = |\mathrm{N}_G(H) : H| = qp$. From the action of $a_2, \ldots, a_t$ on T we see that each of these generators of H fixes each $B_{j,0}$ pointwise. Hence if $\varepsilon = 1$ then $F = \bigcup_{j=0}^{p-1} B_{j,0}$.

Our next step is to determine the H-orbits in V. We use the following convention for labelling the H-orbits contained in $\bigcup_{j=0}^{p-1} B_{j,0}$. For subsets u, v, w of $\mathbb{Z}_q$, $\mathbb{Z}_p$ and $\mathbb{Z}_r$ respectively we set

$$\Delta_{u,v,w}(\alpha) = \{a_1^i c^j x^m \mid i \in u, j \in v, m \in w\}$$

and if one of these sets is a singleton, say $u = \{i\}$ we will write $\Delta_{u,v,w}(\alpha) = \Delta_{i,v,w}(\alpha)$. Since $a_2, \ldots, a_t$ all fix $B_{j,0}$ pointwise ($j \in \mathbb{Z}_p$), the H-orbits in $B_{j,0}$ are the same as the $\langle x^r \rangle$-orbits. Thus, the H-orbits in $B_{j,0}$ ($j \in \mathbb{Z}_p$) are in $1-1$ correspondence with the set $D \cup \{0\}$, where D is the set of $(q-1)/r^{\varepsilon-1}$ cosets of $\langle n \rangle$ in $\mathbb{Z}_q{}^*$, namely we have the orbits

$$\Delta_{d,j,0}(\alpha) = \begin{cases} \{c^j\} & \text{if } d = 0 \\ \{a_1^u c^j \mid u \in d\} & \text{if } d \in D. \end{cases}$$

Since $a_1^{-u} c^{-j}$ maps the pair $(1, a_1^u c^j)$ of vertices to the pair $(a_1^{-u} c^{-j}, 1)$, we have (noting that $-d$ is a coset of $\langle n \rangle$ if d is) that $\Delta_{0,j,0}{}^*(\alpha) = \Delta_{0,-j,0}(\alpha)$ and $\Delta_{d,j,0}{}^*(\alpha) = \Delta_{-d,-j,0}(\alpha)$ for each $d \in D$.

We claim that the other H-orbits are the sets $\Delta_{j,k}(\alpha) = B_{j,k}$ for $j \in \mathbb{Z}_p$ and $k \in \mathbb{Z}_r{}^*$. Each of the generators $a_2, \ldots, a_t, x^r$ of H fixes each of these sets $B_{j,k}$ setwise, so $B_{j,k}$ is a union of H-orbits. If $\varepsilon = 2$ then, as we remarked above, $\langle a_{k+1} \rangle$ is transitive on $B_{j,k}$ and so $B_{j,k}$ is an H-orbit. If $\varepsilon = 1$ then we showed that H is a q-group acting nontrivially on $B_{j,k}$ (since in this case $F = \bigcup_{j=0}^{p-1} B_{j,0}$) and hence again $B_{j,k}$ is an H-orbit. Since $x^{-k} c^{-j}$ maps the pair $(1, c^j x^k)$ to the pair $(c^{j'} x^{-k}, 1)$, where $j' = -j\delta^k$, we have that

$$\Delta_{j,k}{}^*(\alpha) = \Delta_{-j\delta^k,-k}(\alpha) = B_{-j\delta^k,-k}.$$

Let Γ be a graph with vertex set V, which admits G as a vertex-transitive subgroup of automorphisms. Then by Theorem 3.1, Γ is a generalised orbital graph for G, and the set $\Gamma(\alpha)$ is a union of orbits of H in

$V\backslash\{\alpha\}$ which is closed under pairing. Thus

$$\Gamma(\alpha) = \Big(\bigcup_{j\in J_1} \Delta_{0,j,0}(\alpha)\Big) \cup \Big(\bigcup_{(d,j)\in J_2} \Delta_{d,j,0}(\alpha)\Big) \cup \bigcup_{(j,k)\in J_3} B_{j,k},$$

where $J_1 \subseteq \mathbb{Z}_p{}^*$ is such that $J_1 = -J_1$; $J_2 \subseteq D\times\mathbb{Z}_p$ and J_2 has the property that if $(d,j) \in J_2$ then $(-d,-j) \in J_2$, that is $J_2 = -J_2$; and $J_3 \subseteq \mathbb{Z}_p\times\mathbb{Z}_r{}^*$, and J_3 has the property that if $(j,k) \in J_3$ then $(-j\delta^k, -k) \in J_3$. Note that some of the J_i may be empty.

Our aim is to show that $\mathrm{Aut}\,\Gamma$ contains a regular subgroup. To do this we apply Lemma 3.2 to the partition M of V consisting of $U = \bigcup_{j=0}^{p-1} B_{j,0}$ and each of the $B_{j,k}$ for $j \in \mathbb{Z}_p$, $k \in \mathbb{Z}_r{}^*$, relative to the group $L = \langle x^r\rangle$ if $\varepsilon = 2$ or the group Q if $\varepsilon = 1$.

Suppose first that $\varepsilon = 2$. From the action of $L = \langle x^r\rangle$ on an arbitrary element of T, we see that L fixes setwise U and each of the $B_{j,k}$, $k \in \mathbb{Z}_r{}^*$. Furthermore the L-orbits in U are the sets $\{a_1^u c^j \mid u \in d\}$ for $d \in D \cup \{0\}$, $j \in \mathbb{Z}_p$. Suppose that there is an edge e from $a_1{}^u c^j$ to a point $a_1^{u'} c^{j'} x^k$ in $B_{j',k}$ for some $k \neq 0$. Then the image of e under $c^{-j} a_1{}^{-u}$ is $\{1, a_1^v c^{j'-j\delta^{-k}} x^k\}$ for some v, and is an edge. Hence $(j' - j\delta^{-k}, k) \in J_3$. Since H is transitive on $\Delta_{j'-j\delta^k,k}(\alpha)$ it follows that $\alpha = 1_G$ is joined by an edge to each point of $\Delta_{j'-j\delta^k,k}(\alpha)$, and hence that $a_1{}^u c^j$ is joined by an edge to each point of $B_{j',k}$. It follows that the L-orbit containing $a_1{}^u c^j$ is completely joined to $B_{j',k}$. Since this is true for all $B_{j',k}$ with $k \neq 0$, each L-orbit in U is trivially joined to each $B_{j,k}$ with $j \in \mathbb{Z}_p$, $k \in \mathbb{Z}_r{}^*$. Hence by Lemma 3.2, $\sigma := (x^r)^U \in \mathrm{Aut}\,\Gamma$, where $(x^r)^U$ denotes the permutation of V which fixes $V\backslash U$ pointwise and induces the same permutation as x^r on U. For $i \geq 2$, since a_i fixes U pointwise, it follows that $a_i{}^\sigma = a_i$, while a small computation shows that $\sigma^{-1} a_1 \sigma$ induces the same action on V as a_1^n, and hence $a_1{}^\sigma = a_1{}^n$. Moreover the action of $\sigma^{-1} c\sigma$ on V is as follows

$$(a_1{}^i c^j x^k)^{\sigma^{-1}c\sigma} = \begin{cases} (a_1{}^{in^{-1}} c^j)^{c\sigma} = (a_1{}^{in^{-1}} c^{j+1})^\sigma = a_1{}^i c^{j+1} & \text{if } k = 0 \\ (a_1{}^i c^j x^k)^{c\sigma} = (a_1{}^i c^{j+\delta^{-k}} x^k)^\sigma = a_1{}^i c^{j+\delta^{-k}} x^k & \text{if } k \neq 0 \end{cases}$$

and therefore $c^\sigma = c$. Consider the subgroup $Y := \langle g, c, \sigma^{-1}x\rangle$ of $\mathrm{Aut}\,\Gamma$, where $g = a_1{}^n a_2 \dots a_r$. By the definition of σ,

$$\sigma^{-1}x : a_1^i c^j x^m \longmapsto \begin{cases} a_1^{in^{-1}} c^j x & \text{if } m = 0 \\ a_1^i c^j x^{m+1} & \text{if } 1 \le m \le r-2 \\ a_1^{in} c^j & \text{if } m = r-1. \end{cases}$$

A further straightforward computation shows that $(\sigma^{-1}x)^r$ acts as the identity element on V. Therefore $\sigma^{-1}x$ has order r.

Also

$$g^{\sigma^{-1}x} = (a_1{}^n a_2 \dots a_r)^{\sigma^{-1}x} = (a_1 a_2 \dots a_r)^x = (a_1{}^n a_2 \dots a_r) = g$$

since $a_1{}^\sigma = a_1{}^n$ and $a_i{}^\sigma = a_i$ for $i \in \{2, 3, \dots, r\}$. Thus $\sigma^{-1}x$ centralises g. Since also c centralises g, $\langle g \rangle \cong \mathbb{Z}_q$ is normal in Y. Also $c^{\sigma^{-1}x} = c^x = c^\delta$, so $\sigma^{-1}x$ normalises $\langle c \rangle$. Hence $Y = (\langle g \rangle \times \langle c \rangle).\langle \sigma^{-1}x \rangle$ and so $|Y| = pqr$. Moreover it is easy to check that Y is transitive on V; the set of images of 1_G under $\langle g \rangle c^j (\sigma^{-1}x)^k$ is $B_{j,k}$. Thus Y is a transitive subgroup of $\operatorname{Aut}\Gamma$ of order pqr. Hence Y is regular and so Γ is a Cayley graph in this case.

Now we consider the case where $\varepsilon = 1$. Suppose that there is an edge e joining a point $a_1{}^i c^j x^k \in B_{j,k}$ (where $k \in \mathbb{Z}_r{}^*$) and a point $a_1{}^{i'} c^{j'} \in B_{j',0}$. Since x^k does not normalise H, there exists an element $a \in Q \backslash H$ and an element $b \in H$ such that $ax^k = x^k b$. Since $a \in Q \backslash H$ we can write $a = a_1^\gamma b'$ with $b' \in H$ and $\gamma \neq 0$. Now H fixes $B_{j',0}$ pointwise, and so $a_1{}^{i'} c^{j'}$ is joined by an edge to the image t of $(a_1{}^i c^j x^k)$ under b. We have $Ht = Ha_1{}^i c^j x^k b = Ha_1{}^i c^j a x^k = Ha_1{}^{i+\gamma} c^j x^k$ and so $t = a_1{}^{i+\gamma} c^j x^k$. Repeatedly applying b we see that $a_1{}^{i'} c^{j'}$ is joined to every point of $B_{j,k}$. Also by considering the action of Q we see that $B_{j',0}$ and $B_{j,k}$ are completely joined. Thus each Q-orbit in U is trivially joined to each of the $B_{j,k}$ with $k \neq 0$, and hence by Lemma 3.2, Q^U is a subgroup of $\operatorname{Aut}\Gamma$. Since $x \in \mathrm{N}_{\operatorname{Aut}\Gamma}(Q)$, $Q^{x^m} = Q^{U_m}$ is also a subgroup of $\operatorname{Aut}\Gamma$, where $U_m = U^{x^m}$ for $m \in \{0, 1, \dots, r-1\}$. Thus $\operatorname{Aut}\Gamma \geq \prod_{m=0}^{r-1} Q^{U_m} \cong \mathbb{Z}_q^r$. Let $Q^U = \langle \lambda_0 \rangle$ and define $\lambda_m = \lambda_{m-1}^x$ for $m \in \{1, \dots, r-1\}$. Then $\lambda_{r-1}^x = \lambda_0{}^{x^r} = \lambda_0$ since $x^r = 1$, and therefore $(\lambda_0 \lambda_1 \dots \lambda_{r-1})^x = (\lambda_0 \lambda_1 \dots \lambda_{r-1})$. Since each point of V belongs to exactly one of the U_m, the group generated by $(\lambda_0 \lambda_1 \dots \lambda_{r-1})$ is transitive on $B_{j,k}$ for each j, k, and $\langle c \rangle$ permutes the $B_{j,k}$ in r orbits of length p. Also x maps U_m to U_{m+1} for all m (subscripts must be read modulo p). Hence $Z := \langle \lambda_0 \lambda_1 \dots \lambda_{r-1}, c, x \rangle = (\langle \lambda_0 \lambda_1 \dots \lambda_{r-1} \rangle \times \langle c \rangle).\langle x \rangle$ is transitive and regular on V. Consequently in this case also Γ is a Cayley graph. This completes the proof of Proposition 4.2. □

5 Proof of Theorem 1.1

Suppose that p, q and r are distinct odd primes such that $pq, qr, pr \notin \mathcal{NC}$ and $\{p, q, r\} \notin \mathcal{N}_3$, and suppose that $\Gamma = (V, E)$ is a vertex-transitive non-Cayley graph of order pqr such that $\operatorname{Aut}\Gamma$ has a genuinely 3-step imprimitive subgroup G. We shall derive a contradiction by constructing a regular subgroup of $\operatorname{Aut}\Gamma$. We may assume that G is minimal by inclusion subject to being genuinely 3-step imprimitive. Thus G is transitive on V and we have $1 < N < K < G$, with N, K normal subgroups of G, K intransitive on V, and the N-orbits on V are proper subsets of the K-orbits. Let Σ denote the set of K-orbits and Δ denote the set of N-orbits. Since $|V| = pqr$, it follows that $|\Sigma|$ is a prime, say $|\Sigma| = r$. Also the N-orbits have prime length, say p. Moreover we may assume that K is equal to the kernel $G_{(\Sigma)}$ of the action of G on Σ, and also that N is equal to the kernel $G_{(\Delta)}$ of the action of G on Δ. Note that G is not regular on V since we are assuming that Γ is not a Cayley graph. Thus pqr divides $|G|$ (since G is transitive on V) and $|G| > pqr$.

Our first aim is to describe the structure of G in greater detail. We prove in Proposition 5.3 that $G = PQR$ where P is the unique (normal) Sylow p-subgroup of G, Q is a Sylow q-subgroup of G, PQ is normal in G, and R, a Sylow r-subgroup of G, is cyclic and normalises Q. We complete the proof by analysing the various possibilities for P, Q and R using the results of Section 4. We prove in all cases that $\operatorname{Aut}\Gamma$ contains a regular subgroup.

Lemma 5.1. *Suppose that Σ, the set of K-orbits has order r. Then $G/K \cong \mathbb{Z}_r$.*

Proof. Since G^Σ is transitive there exists $x \in G \setminus K$, such that x^Σ is an r-cycle. Replacing x by some power x^i if necessary we may assume that x is an r-element. Then $\langle x \rangle$ acts transitively on the K-orbits, so $\langle K, x \rangle$ is transitive on V. Since $\langle K, x \rangle$ has a chain of intransitive normal subgroups $1 < N < K < \langle K, x \rangle$, it follows from the minimality of G that $G = \langle K, x \rangle$. Moreover x^r fixes each K-orbit setwise and hence $x^r \in K$ and $G/K = \langle xK \rangle$ is cyclic of order r. □

Lemma 5.2. *The group N has a unique Sylow p-subgroup P.*

Proof. Let P be a Sylow p-subgroup of N. Since each N-orbit has length p, it follows that P has no fixed points, for if $P \leq N_\alpha$ then $p = |N : N_\alpha|$ would divide $|N : P|$ which is not the case. Hence P has qr orbits of length p. By Lemma 3.5, $G = N\mathrm{N}_G(P)$, so $\mathrm{N}_G(P)$ is transitive on Δ. Since every block in Δ is an orbit of P it follows that $\mathrm{N}_G(P)$ is transitive on V. Moreover $\mathrm{N}_G(P) \cap K = \mathrm{N}_K(P)$ has index r in $\mathrm{N}_G(P)$, since $\mathrm{N}_G(P)$ is transitive on Σ and $G/K \cong \mathbb{Z}_r$, and hence $\mathrm{N}_G(P)$ is a genuinely 3-step imprimitive group relative to the chain $1 < \mathrm{N}_N(P) < \mathrm{N}_K(P) < \mathrm{N}_G(P)$ of normal subgroups. By the minimality of G, we must have $G = \mathrm{N}_G(P)$. Hence P is the unique Sylow p-subgroup of N. □

Since $|G/K| = r$ and pqr divides $|G|$, the Sylow q-subgroup Q of K is nontrivial. As in the proof of Lemma 5.2, Q has no fixed points in V, and a similar argument shows that Q does not fix setwise any block of Δ.

Proposition 5.3. *The group $G = PQR$, where P, Q, R are a Sylow p-subgroup, a Sylow q-subgroup and a Sylow r-subgroup of G respectively, and $P \lhd G$, $PQ \lhd G$, R is cyclic, R normalises Q, and P is elementary abelian.*

Proof. Let P be the unique Sylow p-subgroup of N (see Lemma 5.2), and let Q be a Sylow q-subgroup of K and hence of G. By Lemma 3.5, $G = K\mathrm{N}_G(Q)$, so $\mathrm{N}_G(Q)^\Sigma \cong \mathbb{Z}_r$ and we may choose the r-element x (in the proof of Lemma 5.1) to lie in $\mathrm{N}_G(Q)$. Set $R := \langle x \rangle$. By our remarks above, Q fixes no point of V and hence PQ is transitive on each block of Σ. Then since R^Σ is transitive it follows that PQR is transitive on V. Also PQR is a genuinely 3-step imprimitive group relative to the chain $1 < P < PQ < PQR$ of normal subgroups. By the minimality of G, we have $G = PQR$. Since $|G/P| = |QR| = |Q|.|R|$, it follows that P is a Sylow p-subgroup of G. Also R is a Sylow r-subgroup of G and R is cyclic. Now P is isomorphic to a subgroup of $\prod_{D \in \Delta} P^D$, where P^D is the permutation group induced by P on D. Since $|D| = p$, the group P^D is cyclic of order p, and hence P is elementary abelian. □

Our next step is to deal with the case $|P| = p$.

Proposition 5.4. *Suppose that $G = PQR$ as in Proposition 5.3. Then $|P| > p$.*

Proof. We shall show that G has a power-conjugate presentation as in (2). Set $R = \langle x \rangle$ where $|x| = r^\varepsilon$ and suppose that $P = \langle c \rangle \cong \mathbb{Z}_p$. By Proposition

1.2, r^2 does not divide $p-1$, since $rp \notin \mathcal{NC}$. Hence x^r centralises P. Similarly, if $|Q| = q$ then, since R normalises Q, we find that x^r centralises Q. Suppose that $|Q| = q$. Then $\langle x^r \rangle \lhd G$. Since $x^r \in K$ the length of the orbits of the r-group $\langle x^r \rangle$ must divide the length pq of the K-orbits, and hence $|x| = r$. Therefore $|G| = pqr$ which is a contradiction. Hence $|Q| > q$.

Suppose now that $[P, Q] \neq 1$. Since $P \lhd G$ and $P = \langle c \rangle \cong \mathbb{Z}_p$ the order of $G/\mathrm{C}_G(P)$ divides $p-1$ and therefore q divides $p-1$. Since $pq \notin \mathcal{NC}$, by Proposition 1.2, $q^2 \nmid (p-1)$. So $|Q : \mathrm{C}_Q(P)| = q$ and hence $C = \mathrm{C}_Q(P) \neq 1$. Now $C \lhd G$, since C is a characteristic subgroup of PQ. It follows that all the orbits of C have length q. Thus CPR is a proper transitive subgroup of G which is a genuinely 3-step imprimitive group relative to the chain $1 < P < CP < CPR$ of normal subgroups, which is a contradiction.

Hence $[P, Q] = 1$. Thus Q is normalised by P and also by R and hence Q is normal in G. It follows that all orbits of Q have length q and in particular $Q \cong \mathbb{Z}_q^t$ for some $t \geq 2$. Suppose that there is a nontrivial proper R-invariant subgroup Q_1 of Q. Since Q_1 is centralised by P and Q it follows that $Q_1 \lhd G$, and that PQ_1R is a proper subgroup of G which is genuinely 3-step imprimitive relative to the chain $1 < P < PQ_1 < PQ_1R$ of normal subgroups, contradicting the minimality of G. Hence R acts irreducibly on Q. So we may write $Q = \langle a_1, \ldots, a_t \rangle \cong \mathbb{Z}_q^t$ such that $Q_\alpha = \langle a_2, \ldots, a_t \rangle$, $a_i^x = a_{i+1}$ for $i \in \{1, \ldots, t-1\}$, and $a_t^x = a_1^{\beta_1} \ldots a_t^{\beta_t}$ for some $\beta_i \in \mathbb{Z}_q$ with $\beta_1 \neq 0$. Also since $[P, Q] = 1$ we have $[a_i, c] = 1$ for all i, and since $R = \langle x \rangle$ normalises $P = \langle c \rangle$, and x^r centralises P, we have $c^x = c^\delta$ for some $\delta \in \mathbb{Z}_p$ with $\delta^r \equiv 1 \pmod{p}$. If $|x| = r$ then $G = \langle a_1, \ldots, a_t, c, x \rangle$ and all the relations of (2) hold. So by Proposition 4.2, Γ is a Cayley graph, which is a contradiction.

Hence $|x| = r^\epsilon \geq r^2$. Consider the transitive group $G^\Delta = Q^\Delta.R^\Delta$ of degree qr. The subgroup $Q^\Delta.\langle x^r \rangle^\Delta$ of G^Δ of index r has r orbits of length q in Δ, and since $Q^\Delta \lhd G^\Delta$ it follows that $Q^\Delta.\langle x^r \rangle^\Delta$ is isomorphic to a subgroup of $\mathrm{AGL}(1, q)^r = (\mathbb{Z}_q.\mathbb{Z}_{q-1})^r$. By Proposition 1.2, r^2 does not divide $q-1$ and so $Q^\Delta.\langle x^r \rangle^\Delta$ contains no elements of order r^2. Hence $\langle x^r \rangle^\Delta \cong \mathbb{Z}_r$, that is $x^{r^2} \in N = G_{(\Delta)}$. Now N has qr orbits of length p, and $P \leq N$. Moreover the centraliser of P in N is a p-group. However, x^{r^2} centralises P, and hence $|x| = r^2$. If $\langle x^r \rangle$ centralises Q then $\langle x^r \rangle$ centralises PQ and hence is a characteristic subgroup of K, so $\langle x^r \rangle \lhd G$. This implies that the length r of the $\langle x^r \rangle$-orbits divides the length pq of the K-orbits, which is a contradiction. Hence R acts faithfully as a cyclic group of automorphisms of $Q = \mathbb{Z}_q^t$. We have already shown that R is irreducible on Q, and so r^2 divides $q^t - 1$ and r^2 does not divide $q^{t'} - 1$ for any $t' \in \{1, \ldots, t-1\}$.

Let $S \in \Sigma$ be the K-orbit containing α. Then $|Q : Q_\alpha| = |\alpha^Q| = q$, and Q_α fixes a point in each of the P-orbits in S. Since $[P, Q] = 1$ it follows that $Q_\alpha^S = 1$ and therefore $(PQ)^S$ is regular and is cyclic of order pq. In particular, $(PQ)^S$ is self-centralising in $\mathrm{Sym}(S)$. Now $x^r \in K$ and $x^r \neq 1$. Hence $(x^r)^S \neq 1$. Since $(PQ)^S$ is self-centralising in $\mathrm{Sym}(S)$, $(x^r)^S$ does not centralise $(PQ)^S$. However, x^r centralises P and normalises Q and hence $(x^r)^S$ normalises but does not centralise $Q^S \cong \mathbb{Z}_q$. Hence r divides $q-1$. Since r^2 does not divide $q-1$, r divides

$$\frac{q^t - 1}{q - 1} = q^{t-1} + q^{t-2} + \cdots + q + 1 \equiv 1 + 1 + \cdots + 1 = t \pmod{r}.$$

Thus $t \equiv 0 \pmod{r}$; that is r divides t. However

$$\frac{q^r - 1}{q - 1} = q^{r-1} + q^{r-2} + \cdots + q + 1 \equiv r \equiv 0 \pmod{r}.$$

Hence r^2 divides $q^r - 1$. Since t is the least integer such that r^2 divides $q^t - 1$, it follows that $t = r$. Thus $\Sigma = \{S_1, \ldots, S_r\}$, where $S_i^x = S_{i+1}$ for $i \in \{1, \ldots, r-1\}$ and $S_r^x = S_1$. Since $|Q| = q^r$ it follows that $Q = Q_1 \times \cdots \times Q_r$, where $Q_i = \langle a_i \rangle \cong \mathbb{Z}_q$ acts nontrivially on S_i and fixes S_j pointwise for all $j \neq i$. Moreover we may choose the a_i such that $a_i^x = a_{i+1}$ for $i \in \{1, \ldots, r-1\}$, and $a_r^x = a_1^{x^r} = a_1^n$ for some $n \neq 0$. Since $|x| = r^2$ and $\langle x \rangle$ is faithful on Q, it follows that $n \neq 1$ and $a_1 = {a_1}^{x^{r^2}} = {a_1}^{n^r}$. Hence $o(n \mod q) = r$. Thus $G = \langle a_1, \ldots, a_r, c, x \rangle$ and all the relations of (2) hold. Also $G_\alpha = \langle a_2, \ldots, a_r, x^r \rangle$, and hence by Proposition 4.2, Γ is a Cayley graph which is a contradiction. This completes the proof of Proposition 5.4. □

We consider now the case where $|P| \geq p^2$. Suppose that $S \in \Sigma$ and choose $\alpha \in D$, where $D \in \Delta$, $D \subset S$, and write

$$F = \mathrm{fix}_V(P_\alpha) = \{\beta \in V \mid \beta^g = \beta \text{ for all } g \in P_\alpha\}.$$

Lemma 5.5. *(a) F is a block of imprimitivity for G in V; F is a union of blocks of Δ, and in particular $D \subseteq F$; and $|F| = pt$, where t divides qr and $t < qr$.*

(b) Moreover the group $P^F := \{g^F \mid g \in P\}$, where g^F is defined by

$$\beta^{g^F} = \begin{cases} \beta^g & \text{if } \beta \in F \\ \beta & \text{if } \beta \notin F \end{cases}$$

is contained in $\mathrm{Aut}\,\Gamma$.

Proof. (a) Let $g \in G$ be such that $F \cap F^g \neq \emptyset$ and let $\gamma \in F \cap F^g$, say $\gamma = \beta^g$ where $\beta \in F$. Then $P_\alpha \leq P_\gamma$ and $|P_\gamma| = \frac{|P|}{|D|} = |P_\alpha|$, so $P_\alpha = P_\gamma$. Hence $F = \mathrm{fix}_V(P_\gamma)$. Since $\beta \in F$, by the same argument $F = \mathrm{fix}_V(P_\beta)$. Hence $F^g = (\mathrm{fix}_V(P_\beta))^g = \mathrm{fix}_V(P_{\beta^g}) = \mathrm{fix}_V(P_\gamma) = F$. Thus F is a block of imprimitivity for G. Since P is abelian, P_α is normal in P and since P acts transitively on D, it follows that P_α fixes D pointwise, that is $D \subseteq F$. It follows that F is a union of blocks of Δ. Thus the set $\bar{F}$ of blocks of Δ contained in F forms a block of imprimitivity for G in Δ and so $t = |\bar{F}|$ divides qr. Since $|P| \geq p^2$, $F \neq V$, so $t < qr$; also $|F| = pt$.

(b) Let $\{\beta, \gamma\} \in E$, and let $g^F \in P^F$. If both of β and γ lie in $V \backslash F$ then $\{\beta^{g^F}, \gamma^{g^F}\} = \{\beta, \gamma\} \in E$. If both of β and γ lie in F then $\{\beta^{g^F}, \gamma^{g^F}\} = \{\beta^g, \gamma^g\} \in E$, since $g \in \mathrm{Aut}\,\Gamma$. So suppose finally that one of β, γ is in F and the other is in $V \backslash F$, say $\beta \in F$ and $\gamma \in V \backslash F$. Then $\{\beta^{g^F}, \gamma^{g^F}\} = \{\beta, \gamma^g\}$, and we note that $\gamma^g \in \gamma^P$ and the P-orbit γ^P is a block of Δ, say $\gamma^P = D'$. We showed above that $P_\alpha = P_\beta$ (since $\beta \in F$) and so P_β is transitive on D' (since $D' \subset V \backslash F$). Thus since β is adjacent to $\gamma \in D'$, β is adjacent to every point of D' and in particular β is adjacent to γ^g. Hence g^F maps every edge of Γ to an edge and this implies that $g^F \in \mathrm{Aut}\,\Gamma$ (since Γ is finite). Since this is true for all $g \in P$, $P^F \subseteq \mathrm{Aut}\,\Gamma$. □

Lemma 5.6. *Suppose that $t = |F|/p$ as in previous lemma. Then $t \neq 1$.*

Proof. Suppose that $t = 1$. Then $F = D$, and P_α fixes D pointwise and is transitive on each $D' \in \Delta$, $D' \neq D$. By Lemma 3.3, $\Gamma \cong \Gamma_\Delta(\bar{D})$. Since $qr, p \notin \mathcal{NC}$, both Γ_Δ and $\bar{D}$ are Cayley graphs. Hence Γ is a nontrivial lexicographic product of two Cayley graphs. By Lemma 3.4, Γ is a Cayley graph, which is a contradiction. □

Let $\Phi := \{F^g \mid g \in G\}$. Then Φ is a block system for G, since F is a block of imprimitivity for G in V.

Lemma 5.7. *Either*

(a) $F = S$, $\Phi = \Sigma$ *and* $t = q$, *or*

(b) F *consists of one block of* Δ *from each block of* Σ *and* $t = r$.

Proof. (a) If $S \subseteq F$, then F is a union of complete blocks of Σ. For if $S' \in \Sigma$ and $F \cap S'$ contains a point γ, then for $\beta \in S$ and $g \in G$ mapping β to γ, $F \cap F^g$ contains $\beta^g = \gamma$. So (as F is a block) $F = F^g$ and hence $S^g \subseteq F$. But $S^g \in \Sigma$ and S^g contains $\beta^g = \gamma$, so $S^g = S'$. Thus the set $\widehat{F}$ of blocks of Σ contained in F is a block of imprimitivity for the primitive action of G on Σ. Since $\widehat{F} \neq \Sigma$ (because $|F| < |V|$), we must have $|\widehat{F}| = 1$, that is, $F = S$ and therefore $t = q$. By the definition of Φ, $\Phi = \{S^g \mid g \in G\} = \Sigma$.

(b) Thus we may assume that $F \cap S \neq S$. Now $F \cap S$ (the intersection of two blocks) is a block of imprimitivity for G containing D. It is also a block of imprimitivity for the action of G_S on S of degree pq. Since D is a maximal block of imprimitivity for G_S in S it follows that $F \cap S = D$. By Lemma 5.6, $F \neq D$, so there is an $S' \in \Sigma \backslash \{S\}$ such that $F \cap S' \neq \emptyset$.

By the proof of part (a), we see that $F \cap S' \neq S'$, so $F \cap S'$ is a block of Δ. Thus F consists of one block of Δ from each of a certain subset $\widehat{S}$ of blocks of Σ, and $\widehat{S}$ is a block for the primitive action of G on Σ. Since $|\widehat{S}| \geq 2$, $\widehat{S} = \Sigma$ and so $|F| = pr$. Thus $t = r$. □

For $F' \in \Phi$ let $P^{F'}$ denote the permutation group on V which fixes $V \backslash F'$ pointwise and acts on F' in the same way that P does. Set $P_0 := \prod_{F' \in \Phi} P^{F'}$. By Lemma 5.5, $P_0 \leq \mathrm{Aut}\,\Gamma$. Also G normalises P_0.

Proposition 5.8. *Case (b) of Lemma 5.7 does not arise.*

Proof. Suppose that case (b) holds. Then $|\Phi| = q$ and Q^Φ is transitive. Let L be the kernel of G on Φ. Then L contains P and we consider the following cases:

1. The L-orbits have size p. In this case the L-orbits are the blocks of Δ, so $L \subseteq G_{(\Delta)}$. On the other hand by Lemma 5.7(b) it follows that $G_{(\Delta)} \subseteq L$. So $L = G_{(\Delta)}$ and $G/L \cong G^\Phi$ is transitive of degree q with a normal q-subgroup $(PQ)L/L \cong Q/Q \cap L$. Hence $G/L \lesssim \mathrm{AGL}(1, q) = \mathbb{Z}_q.\mathbb{Z}_{q-1}$.

Since $L = G_{(\Delta)} \subseteq K$, it follows that r divides $|G/L|$ and hence r divides $q-1$. Now $L \lesssim \prod_{D\in\Delta} L^D \leq (AGL(1,p))^{qr} = (\mathbb{Z}_p.\mathbb{Z}_{p-1})^{qr}$. Since r divides $q-1$ it follows from Definition 1.1 that q does not divide $p-1$ and hence q does not divide $|L|$. Thus $Q \cap L = 1$ and $|Q| = q$. We may assume that $\Phi = \{F_1 = F, F_2, \ldots, F_q\}$ is labelled in such a way that $Q = \langle b \rangle$ and $F_i^b := F_{i+1}$ for all i (reading subscripts modulo q). Let $P^{F_1} := \langle a_1 \rangle \cong \mathbb{Z}_p$, and define $a_{i+1} := a_i^b$ for all $i < q$ so that $P^{F_i} = \langle a_i \rangle$ for all i, and the group $P_0 = \langle a_1, \ldots, a_q \rangle \cong \mathbb{Z}_p^q$. By the remark preceding the statement of Proposition 5.8, $P_0 \leq \mathrm{Aut}\,\Gamma$. Since $b^q = 1$, the element $a := a_1a_2\ldots a_q$ is centralised by $Q = \langle b \rangle$. Set $P_1 = \langle a \rangle$. Then $\mathrm{N}_{GP_0}(Q)$ contains $G_1 := \langle P_1, Q, R \rangle$ and G_1 is transitive with normal subgroup Q of order q. Also G_1 preserves the partition Σ and the kernel of G_1 on Σ is $K_1 := (G_1)_{(\Sigma)} = \langle P_1, Q, x^r \rangle$ of index r in G_1, so $G_1^\Sigma \cong \mathbb{Z}_r$. Let Δ_1 be the set of Q-orbits and set $N_1 := (G_1)_{(\Delta_1)}$. Then N_1 contains $Q \cong \mathbb{Z}_q$ as a normal Sylow q-subgroup. Applying the arguments and analysis of this section to the group G_1 with chain of normal subgroups $1 < N_1 < K_1 < G_1$ (and interchanging p and q) we find (essentially by Propositions 5.3 and 5.4) that Γ is a Cayley graph in this case, which is a contradiction.

2. The L-orbits have size pr. Let $b \in G\backslash L$, be a q-element. Then b permutes the blocks of Φ transitively, so $\langle L, b \rangle$ is transitive on V. Also $\langle L, b \rangle$ is genuinely 3-step imprimitive relative to the chain of normal subgroups $1 < L \cap K < L < \langle L, b \rangle$. Thus by the minimality of G, $G = \langle L, b \rangle$. Also $G/L \cong \mathbb{Z}_q$ and it follows that $G/(L \cap K) \cong (L/(L\cap K)) \times (K/(L \cap K)) \cong \mathbb{Z}_{qr}$. Moreover $L \cap K$ fixes setwise each $F_i \cap S_j$, which are the blocks of Δ. Thus $L \cap K \subseteq G_{(\Delta)}$ and conversely $G_{(\Delta)}$ fixes each of the blocks of Φ and Σ setwise, so $L \cap K = G_{(\Delta)}$. Since $P \subseteq L \cap K$, the $(L\cap K)$-orbits are the blocks of Δ of size p. Hence $G = \langle L\cap K, y \rangle$, where y is a $\{q,r\}$-element (that is $|y| = q^m r^n$ for some $m \geq 1$, $n \geq 1$). Using a similar argument, we see that $\langle P, y \rangle$ is transitive on V, and is genuinely 3-step imprimitive relative to the chain of normal subgroups $1 < P < \langle P, y^q \rangle < \langle P, y \rangle$. Thus by the minimality of G, $G = \langle P, y \rangle$. Again we set $P^{F_1} = \langle a_1 \rangle$ and $a_{i+1} := a_i^y$ for $i \in \{1, 2, \ldots, q-1\}$, and $P_0 = \langle a_1, \ldots, a_q \rangle$. By the remark preceding the statement of Proposition 5.8, $P_0 \leq \mathrm{Aut}\,\Gamma$, and $P \leq P_0 \cong {\mathbb{Z}_p}^q$. Now $a_q^y = {a_1}^{y^q} \in P^{F_1} = \langle a_1 \rangle$, so $a_q^y = {a_1}^{y^q} = a_1^e$ for some $e \in {\mathbb{Z}_p}^*$. Also for all $i \geq 2$, ${a_i}^{y^q} = {a_1}^{y^{i-1}y^q} = ({a_1}^e)^{y^{i-1}} = ({a_1}^{y^{i-1}})^e = a_i^e$. Hence if

$a := a_1a_2\dots a_q$, then $a^{y^q} = a^e$. So $P_1 := \langle a\rangle \cong \mathbb{Z}_p$, and is normalised by $\langle y^q\rangle$. If $e = 1$ then y centralises a and so $G_1 := \langle P_1, y\rangle$ is transitive on V, and is genuinely 3-step imprimitive relative to the chain of normal subgroups $1 < P_1 < \langle P_1, y^r\rangle < G_1$. Since $P_1 \cong \mathbb{Z}_p$ and P_1 is the unique Sylow p-subgroup of G_1 it follows (from the arguments of Propositions 5.3 and 5.4) that Γ is a Cayley graph, which is a contradiction. Hence $e \neq 1$.

Then $\langle y^q\rangle$ acts nontrivially on $\langle a\rangle$. In fact y^q maps a' to $(a')^e$ for all $a' \in P_0$, that is y^q acts as "Scalars" on P_0. We may assume that $R = \langle x\rangle \leq \langle y^q\rangle$, so there is an $f \in \mathbb{Z}_p{}^*$ such that x maps a' to $(a')^f$ for all $a' \in P_0$. If R centralises P_0 then R centralises P and hence $R \trianglelefteq G = \langle P, y\rangle$. The R-orbits therefore all have the same length which divides pqr and $|R|$, and hence the R-orbits have length r, so R is elementary abelian as well as cyclic, and hence $|R| = r$. So we have $1 < R < PR < G$ and now G is a genuinely 3-step imprimitive permutation group with normal subgroup R of order r. By the arguments of Propositions 5.3 and 5.4 (replacing p, q, r by r, p, q respectively) it follows that Γ is a Cayley graph which is a contradiction. Hence R acts nontrivially on P_0 and hence on $\langle a\rangle$. Hence r divides $p-1$. By Proposition 1.2, $r^2 \nmid (p-1)$ and so $\langle x^r\rangle$ centralises P_0 and hence $\langle x^r\rangle \trianglelefteq G$. If $x^r \neq 1$ then the $\langle x^r\rangle$-orbits all have length r and are subsets of the K-orbits of length pq, which is a contradiction, since $r \nmid pq$. Hence $x^r = 1$.

In a similar way we shall show that $|Q| \leq q^2$. We may assume that $Q = \langle b\rangle \leq \langle y\rangle$ and hence $\langle b^q\rangle \leq \langle y^q\rangle$ and so b^q acts as "Scalars" on P_0. By Proposition 1.2, $q^2 \nmid (p-1)$ so $\langle b^{q^2}\rangle$ centralises P_0 and R and hence $\langle b^{q^2}\rangle \lhd G$. Arguing as in the previous paragraph, if $b^{q^2} \neq 1$ then $\langle b^{q^2}\rangle$ has order q, and the $\langle b^{q^2}\rangle$-orbits all have the same length q and are subsets of $K_{(\Delta)}$-orbits of length p, which is a contradiction. So $b^{q^2} = 1$.

Hence $|y| = q^c r$ where c is 1 or 2. Now consider the subgroup $\langle P_0, y\rangle = \langle a_1, \dots, a_q, y\rangle$ of $\mathrm{Aut}\,\Gamma$. We shall show that the generators $a_1, \dots, a_q, y$ satisfy all of the relations of the group defined in (1) (with p, q, r replaced by r, p, q respectively). We have, for all i and j, that $a_i{}^p = y^{q^c r} = [a_i, a_j] = 1$. Moreover $a_i{}^y = a_{i+1}$, for $i \in \{1, \dots, q-1\}$ and $a_q{}^y = a_1{}^e$. We claim that $o(e^r \mod p) = q^{c-1}$. Since $a_i{}^{y^q} = a_i{}^e$ and $|y| = q^c r$, we have $a_i = a_i{}^{y^{q^c r}} = a_i{}^{e^{q^{c-1}r}}$. Thus $o(e \mod p)$ divides $q^{c-1}r$ and so $o(e^r \mod p)$ divides q^{c-1}. If $c = 1$ then $o(e^r \mod p) = 1 = q^{c-1}$. So assume that

$c = 2$ and suppose that $e^r = 1$. Since $a_i^{y^{qr}} = a_i^{e^r} = a_i$ for all i, then y^{qr} centralises $\langle P_0, y\rangle$. Hence $\langle y^{qr}\rangle \lhd \langle P_0, y\rangle$ and all of the $\langle y^{qr}\rangle$-orbits have length q and are subsets of the $G_{(\Delta)}$-orbits of length p, which is a contradiction. So $e^r \neq 1$. Hence $o(e^r \mod p) = q = q^{c-1}$ in this case, since $o(e \mod p)$ divides q. Therefore in all cases $o(e^r \mod p) = q^{c-1}$ and the group $\langle P_0, y\rangle = \langle a_1, \ldots, a_q, y\rangle$ satisfies all the relations specified in (1). Also r divides $p-1$ and the stabiliser of α in $\langle P_0, y\rangle$ is the subgroup $\langle a_2, \ldots, a_q, y^{qr}\rangle$. It follows from Proposition 4.1 that Γ is a Cayley graph, which is a contradiction.

□

This leaves us with case (a) of Lemma 5.7.

Proposition 5.9. *Case (a) of Lemma 5.7 does not arise.*

Proof. Suppose that case (a) of Lemma 5.7 holds and consider Q^Δ, which has r orbits of length q. If $|Q^\Delta| \geq q^2$, then Q_D^Δ fixes exactly q blocks of Δ (namely those contained in S) and is transitive on the other Q^Δ-orbits of length q. (This can be proved with a similar argument to that used for Lemma 5.7(b)). In this case it follows that K_α is transitive on S_i for each $i \in \{2, \ldots, r\}$. By Lemma 3.3, $\Gamma \cong \Gamma_\Sigma[\bar{S}]$, and since $pq, r \notin \mathcal{NC}$ it follows from Lemma 3.4 that Γ is a Cayley graph, which is a contradiction. Thus $|Q^\Delta| = q$, and $G^\Delta = Q^\Delta.\langle x^\Delta\rangle$. Now if x^Δ centralises Q^Δ, then G^Δ has a normal subgroup $\langle x^\Delta\rangle$ of index q with q orbits of length r. Hence G has a normal subgroup of index q with q orbits in V of length pr. In this case, interchanging q and r we see that case (b) of Lemma 5.7 holds, and we have already shown in that case that all graphs arising are Cayley graphs. Hence x^Δ acts nontrivially on Q^Δ, and so r divides $q-1$. If $(x^r)^\Delta \neq 1$, then $(x^r)^\Delta$ centralises Q^Δ (since $r^2 \nmid (q-1)$) and so $\langle (x^r)^\Delta\rangle \lhd G^\Delta$. However $\langle (x^r)^\Delta\rangle \subseteq K^\Delta$ which has r orbits of length q, and $(x^r)^\Delta$ is an r-element, and so we have a contradiction. Hence $(x^r)^\Delta = 1$. Let $L = G_{(\Delta)}$. Then G/L is a Frobenius group of order qr. Consider $Q \cap L$ (of index q in Q). Since $Q \cap L$ fixes each S_i setwise, $Q \cap L$ normalises each ${P_0}^{S_i}$. Since r divides $q-1$, it follows that $q \nmid (p-1)$, since $\{p, q, r\} \notin \mathcal{N}_3$. Hence $Q \cap L$ centralises ${P_0}^{S_i}$ for each i, so $Q \cap L$ centralises P_0 and hence P. Thus $Q \cap L \lhd G$. However L has qr orbits of length p and $Q \cap L$ is a q-group. Hence $Q \cap L = 1$ and $|Q| = q$. Since q does not divide $p-1$, it follows that

$Q \cong \mathbb{Z}_q$ centralises each of the ${P_0}^{S_i}$. Thus Q centralises P and so $Q \lhd G$. By interchanging p and q, we have a genuinely 3-step imprimitive group G, which has a chain of normal subgroups, $1 < Q < PQ < G$ where $|Q| = p$. By the arguments of Propositions 5.3 and 5.4, Γ is a Cayley graph, which is a contradiction. □

Propositions 5.8 and 5.9 complete the proof that there are no possibilities for G with $|P| \geq p^2$. This completes the proof of Theorem 1.1.

Acknowledgements
The second author wishes to thank the University of Western Australia for its hospitality while most of this work was done. In particular the advice of Greg Gamble and Alice Niemeyer on numerous occasions was much appreciated.

References

[1] N. L. Biggs, *Algebraic graph theory*, (Cambridge University Press, London, New York, 1974).

[2] G. Gamble and C. E. Praeger, Vertex-primitive groups and graphs of order twice the product of two distinct odd primes, (in preparation).

[3] M. A. Iranmanesh and C. E. Praeger, On vertex-transitive graphs of order a product of three distinct odd primes, (in preparation).

[4] R. Laue, J. Neubüser, and U. Schoenwaelder, Algorithms for finite soluble groups and the SOGOS system, in *Computational group theory*, Michael D. Atkinson (ed.) (Academic Press, London, 1984), 105–135.

[5] D. Marušič, Cayley properties of vertex-symmetric graphs, *Ars. Combin.* **16B** (1983), 297–302.

[6] D. Marušič, Vertex-transitive graphs and digraphs of order p^k, *Ann. Discrete Math.* **27** (1985), 115–128.

[7] D. Marušič, R. Scapellato, Characterising vertex-transitive pq-graphs with an imprimitive automorphism subgroup, *J. Graph Theory* **16** (1992), 375–387.

[8] D. Marušič, R. Scapellato, and B. Zgrablič, On quasiprimitive *pqr*-graphs, *Alg. Colloq.* **2** (1995), 295–314.

[9] B. D. McKay and C. E. Praeger, Vertex-transitive graphs which are not Cayley graphs, I, *J. Austral. Math. Soc. (A)* **56** (1994), 53–63.

[10] B. D. McKay and C. E. Praeger, Vertex-transitive graphs that are not Cayley graphs, II, *J. Graph Theory* **22** (1996), 321–334.

[11] A. A. Miller and C. E. Praeger, Non-Cayley vertex-transitive graphs of order twice the product of two odd primes, *J. Algebraic Combinatorics* **3** (1994), 77–111.

[12] C. E. Praeger, Finite transitive permutation groups and finite vertex-transitive graphs, in *Graph symmetry*, G. Hahn and G. Sabidussi (eds.) (Kluwer Academic Publishers, Netherlands, 1997), 277-318.

[13] D. J. Robinson, *A course in the theory of groups*, **1**, (Springer-Verlag, Berlin, New York, 1982).

[14] G. F. Royle and C. E. Praeger, Constructing the vertex-transitive graphs of order 24, *J. Symbolic Computation* **8** (1989), 309–326.

[15] A. Seress, On vertex-transitive non-Cayley graphs of order *pqr*, *Discrete Math.* **182** (1998), 279–292.

[16] H. Wielandt, *Finite permutation groups*, (Academic Press, New York, 1964).