ON THE AUTOMORPHISM GROUPS OF CAYLEY GRAPHS OF FINITE SIMPLE GROUPS

XIN GUI FANG, CHERYL E. PRAEGER AND JIE WANG

Abstract

Let $G$ be a finite nonabelian simple group and let $\Gamma$ be a connected undirected Cayley graph for $G$. The possible structures for the full automorphism group $\text{Aut}\Gamma$ are specified. Then, for certain finite simple groups $G$, a sufficient condition is given under which $G$ is a normal subgroup of $\text{Aut}\Gamma$. Finally, as an application of these results, several new half-transitive graphs are constructed. Some of these involve the sporadic simple groups $G = J_1, J_4, Ly$ and $BM$, while others fall into two infinite families and involve the Ree simple groups and alternating groups. The two infinite families contain examples of half-transitive graphs of arbitrarily large valency.

1. Introduction

For a group $G$ and a subset $S$ of $G$ satisfying $1_G \notin S$ and $S^{-1} = S$, the Cayley graph $\text{Cay}(G,S)$ of $G$ relative to $S$ is defined as the graph $(G,E(S))$ with vertex set $G$ and edge set $E(S)$ consisting of those unordered pairs $\{x,y\}$ from $G$ for which $yx^{-1} \in S$. Let $\langle S \rangle$ denote the subgroup of $G$ generated by $S$. If $\Gamma = \text{Cay}(G,S)$ is not connected, then $\Gamma$ is a disjoint union of $|G:\langle S \rangle|$ copies of the Cayley graph $\text{Cay}(\langle S \rangle, S)$. Therefore we focus on connected Cayley graphs $\text{Cay}(G,S)$, that is those graphs for which $G = \langle S \rangle$. Each Cayley graph $\Gamma = \text{Cay}(G,S)$ admits the group $G.A(G,S)$ as a subgroup of automorphisms, where $G$ acts by right multiplication, and

$$A(G,S) = \{x \in \text{Aut}(G) \mid S^x = S\}$$

acts naturally. Moreover (see [9]), $N_{\text{Aut}\Gamma}(G) = G.A(G,S)$. Here we study Cayley graphs for nonabelian simple groups. First we investigate the possible structure of the full automorphism groups of arbitrary connected Cayley graphs $\text{Cay}(G,S)$ for such groups $G$ (Theorem 1.1). Then we study the special subclass of such graphs for which the subgroup $G.A(G,S)$ is transitive on $E(G)$. Such Cayley graphs are said to be normal edge-transitive, and were studied in [22]. We determine a set of special conditions under which one can guarantee that $\text{Aut}\Gamma = G.A(G,S)$ (Theorem 1.3). Although the conditions are rather technical, it turns out that they are satisfied for certain of the sporadic simple groups, for the family of Ree simple groups, and for infinitely many finite alternating groups. This has led to the construction of several new half-transitive graphs, that is, graphs for which $\text{Aut}\Gamma$ is edge-transitive, but not arc-transitive (Constructions 4.1 and 4.2). Although half-transitive graphs of every even valency are known to exist from the work of Bouwer [4], rather few families of such graphs containing graphs of arbitrarily large valency seem to be known (see, for example, [17]).
Table 1. Product action possibilities for Theorem 1.1.

|   | G   | T          | m   | |VT_K| |
|---|-----|------------|-----|---|----|
| 1. | A_6 | G          | 6   | |m^2| |
| 2. | M_{12} | G or A_m | 12  | |m^2| |
| 3. | Sp_4(q) (q = 2^r > 2) | G or A_m or Sp_{4(q)}(q = q_0^r) | \frac{q^2(q^2-1)}{2} | |m^2| |
| 4. | Sp_4(q_0) (q = q_0^r) | \frac{q^2(q^2-1)}{2} | |2m^2| |
| 5. | PΩ_8(q) | G or A_m or Sp_2(2) (if q = 2) | \frac{q^4(q^4-1)}{(2,q-1)} | |m^2| |

Before stating our results we introduce the following definitions and notation.

A permutation group G on Ω is said to be quasiprimitive if each of its nontrivial normal subgroups is transitive on Ω. For a group G, let soc(G) denote the socle of G, that is, the product of all the minimal normal subgroups of G. If soc(G) is a non-abelian simple group, then G is said to be almost simple. For a graph Γ, the vertex set and edge set will be denoted by V_Γ and E_Γ respectively, and if K ∈ AutΓ, then the quotient graph Γ_K of Γ relative to K is defined as the graph with vertices the K-orbits in V_Γ, such that two K-orbits X, Y are adjacent (joined by an edge) in Γ_K if and only if at least one x ∈ X and at least one y ∈ Y are adjacent in Γ. Thus if Γ = Cay(G,S) is a finite connected Cayley graph and K is a subgroup of G, then V_Γ_K = \{Kg | g ∈ G\}, and Kx is adjacent to Ky if and only if yx^{-1} ∈ KSK.

The first theorem gives a general description of the possibilities for the full automorphism group of a connected Cayley graph of a finite nonabelian simple group.

**Theorem 1.1.** Let G be a finite nonabelian simple group and Γ = Cay(G,S) a connected Cayley graph for G. Let M be a subgroup of AutΓ containing G.A(G,S). Then either M = G.A(G,S) or one of the following holds.

1. M is almost simple, and soc(M) contains G as a proper subgroup and is transitive on VT.
2. G · Inn(G) ≤ M = G.A(G,S).2 and S is a self-inverse union of G-conjugacy classes.
3. M is not quasiprimitive on VT and there is a maximal intransitive normal subgroup K of M such that one of the following holds:
   - M/K is almost simple, and soc(M/K) contains GK/K ≅ G and is transitive on VT_K.
   - M/K = AGL_2(2), G = L_2(7), and Γ_K ≅ K_3.
   - soc(M/K) ≅ T × T, and GK/K ≅ G is a diagonal subgroup of soc(M/K), where T and G are given in Table 1. Moreover, either M acts primitively on VT_K in product action of degree m^2 (with m as given in Table 1), or line 4 of Table 1 holds with G = Sp_4(q), T = Sp_{q_0}(q_0) (q = q_0^r) and M acts primitively in product action on a set of m^2 blocks of size 2 in VT_K.
Moreover, there are examples of connected Cayley graphs for finite nonabelian simple groups in each of these cases.

This result prompts the question of whether there exist conditions under which we can guarantee that a connected Cayley graph Cay(G, S) for a nonabelian simple group G has automorphism group equal to G.A(G, S).

Such a Cayley graph was called a normal Cayley graph by Xu in [27]. A suitable set of conditions might involve restrictions on both G and S. For example, if we require that S is not a union of complete G-conjugacy classes, then Theorem 1.1(2) does not arise, and if we require that G is not one of the groups arising in Theorem 1.1(3)(b) or (c), then these cases do not arise either. To ensure that the possibilities in cases (1) and (3)(a) do not arise we would need restrictions on the way an almost simple group M (or M/K) can factorize with one of the factors being isomorphic to G. This might remove all possibilities except case (3)(a) with M/K ∼= G. Further conditions would be necessary to eliminate this case.

The next result, Theorem 1.3, provides an example of a set of rather technical restrictions on G and S, which between them guarantee that Cay(G, S) is a normal Cayley graph. We are particularly interested in finding edge-transitive Cayley graphs, and it turns out that the examples satisfying the conditions of Theorem 1.3 are normal edge-transitive Cayley graphs which are not arc-transitive (that is, no automorphism interchanges the endpoints of an edge). Such graphs have been called, in the literature, half-transitive graphs (see [17]).

To begin with we choose a cyclic subgroup P of the nonabelian simple group G such that the order |P| is an odd prime p, and we choose an element x ∈ G of order |x| at least 3, such that xp = {xn | u ∈ P} generates G. Then, setting S := xP ∪ (x−1)P, the graph Γ = Cay(G, S) is a connected undirected Cayley graph for G, and A(G, S) contains the group I(P) of inner automorphisms of G induced by elements of P. This implies that G.A(G, S) is edge-transitive on Γ. Our first condition is that A(G, S) = I(P), which guarantees that G.A(G, S) is not arc-transitive on Γ. The other conditions comprising Hypothesis 1.2 are designed to guarantee that AutΓ is equal to G.A(G, S), and this will be proved in Theorem 1.3.

In order to state the hypothesis, we introduce the following concepts. For an almost simple group M with socle T, an expression M = AB, with A, B proper subgroups of M, is called a factorization of M. Also, for a prime r, Rr(T) denotes the minimal dimension of a faithful, irreducible, projective FT-module, where F is an algebraically closed field of characteristic r.

Hypothsis 1.2. Let G be a finite nonabelian simple group, and p an odd prime divisor of |G|. Let P be a subgroup of G of order p, and let x ∈ G have order |x| ≥ 3 such that G = ⟨x⟩. Set S = xP ∪ (x−1)P. Suppose in addition that the following hold:

(1) A(G, S) = I(P) (the group of inner automorphisms of G induced by P), and G has no subgroups of order 2ip for i ≥ 2.

(2) There is no finite almost simple group L which has a factorization L = AB satisfying:

(i) neither A nor B contains soc(L),

(ii) A is maximal in L and A ∼= G or G × Zp; and

(iii) A ∩ B ∼= Zp.

(3) If G is isomorphic to a group of Lie type over a field of odd characteristic r, then p ≠ r and G contains no subgroups of order rmp, for any m ≥ Rr(G).
Theorem 1.3. Let $G$ be a finite nonabelian simple group, $p$ an odd prime divisor of $|G|$, and $S < G$ such that $G, S, p$ satisfy Hypothesis 1.2. Then the graph $\Gamma = \text{Cay}(G, S)$ is a connected undirected Cayley graph with $\text{Aut}\Gamma = G.A(G, S) \cong G \times \mathbb{Z}_p$. In particular $\Gamma$ is half-transitive of valency $2p$.

The proofs of Theorems 1.1 and 1.3 depend on the finite simple group classification, and will be given in Section 2 and Section 3 respectively. As an application of our theorems, in the final section, we construct several new half-transitive graphs.

We will use the following concepts and notation in the paper. Let $M$ be a subgroup of a virtually simple group with socle $T$. Then $M$ can be factorized $M = AB$ in which neither $A$ nor $B$ contains $T$. Given such a factorization we may replace $A$ by a subgroup containing $A$ which is maximal subject to the condition that it does not contain $T$, and similarly for $B$. Suppose then that both $A$ and $B$ are maximal subject to not containing $T$. If both $A$ and $B$ are maximal subgroups of $M$, then $M = AB$ is called a max$^+$ factorization, while if at least one of them is not maximal in $M$ then $M = AB$ is called a max$^-$ factorization. The max$^+$ factorizations and the max$^-$ factorizations of the almost simple groups have been classified in [15, 16] respectively. As above, $R_r(T)$ denotes the minimal dimension of a faithful, irreducible, projective $FT$-module, where $F$ is an algebraically closed field of characteristic $r$, and $m(T)$ denotes the least index of a proper subgroup of $T$. Also, for a positive integer $n$, $n_r$ denotes the highest power of $r$ dividing $n$; $n_r$ is called the $r$-part of $n$.

2. Proof of Theorem 1.1

Let $G$ be a finite nonabelian simple group and $\Gamma = \text{Cay}(G, S)$ a connected Cayley graph for $G$, where $S = S^{-1}$ and $1 \notin S$. Let $M$ be a subgroup of $\text{Aut}\Gamma$ containing $G.A(G, S)$, and suppose that $M \neq G.A(G, S)$. Let $K$ be a normal subgroup of $M$ which is maximal by inclusion, subject to being intransitive on $VT$. Note that we may have $K = 1$. Let $V$ be the set of $K$-orbits in $VT$, and let $\Gamma_K$ denote the quotient graph relative to $K$, so $V = VT_{\Gamma_k}$. The maximality of $K$ implies that $M$ induces a quasiprimitive action on $V$ with kernel $K$. Also, since $G$ is transitive on $VT$ and is a simple group it follows that $G \cap K = 1$, and hence that $GK/K \cong G$. Thus the action induced by $G$ on $V$ is faithful and quasiprimitive. Let $M^V = M/K$, $G^V = GK/K \cong G$ denote the (quasiprimitive) permutation groups induced by $M, G$ on $V$ respectively. Note that $\text{soc}(M^V)$ is transitive on $V$ since $M^V$ is quasiprimitive. We consider the cases where $M^V$ is primitive, and where it is quasiprimitive but imprimitive, separately.

Lemma 2.1. If $M^V$ is primitive, then one of (1)–(3) of Theorem 1.1 holds.

Proof. By [1, 19] applied to the inclusion $G^V < M^V$ it follows that one of the following holds.

(i) $M^V = \text{AGL}_3(2)$, $G = L_2(7)$, and $|V| = 8$.
(ii) $G^V$ is regular, and $\text{soc}(M^V) \cong G \times G$ is the product of two minimal normal subgroups of $M^V$.
(iii) $M^V$ is almost simple.
(iv) $G^V$ is regular, and $\text{soc}(M^V) \cong G \times G$ is the unique minimal normal subgroup of $M^V$. 


(v) \( \soc(M^V) \cong T \times T \), and \( G^V \cong G \) is a diagonal subgroup of \( \soc(M^V) \), where the possibilities for \( T, G, \) and \( m^2 := |V| \) are given in Table 1. Moreover, \( M^V \) induces a product action on \( V \) of degree \( m^2 \).

We consider these cases in turn. In case (i) the subgroup \( K \neq 1 \) since \( G^V \) is not regular, and since \( M^V \) is 2-transitive, and \( \Gamma \) is connected, it follows that \( \Gamma_K \cong K_S \). Thus Theorem 1.1(3)(b) holds. In cases (ii) and (iv), we have \( K = 1 \) since \( G^V \) is regular. However in case (ii) this means that \( M = GA(G, S) \) which we are assuming is not so. In case (iv), we have \( M = GA(G, S).2 \) and \( C_M(G) \cong G \), whence \( A(G, S) \) contains \( \Inn(G) \) and since \( S = S^{-1} \), Theorem 1.1(2) holds. In case (iii), if \( K = 1 \) then \( G \subseteq \soc(M) \) since \( M/\soc(M) \) is soluble, so \( \soc(M) \) is transitive on \( V \Gamma \), and Theorem 1.1(1) holds. If \( K \neq 1 \) in case (iii), then for the same reason \( G \cong G K / K \subseteq \soc(M / K) \), and so \( \soc(M / K) \) is transitive on \( V \Gamma_K \), and Theorem 1.1(3)(a) holds.

Finally in case (v), for each of the possibilities, \( G^V \) is not regular and hence \( K \neq 1 \). Thus Theorem 1.1(3)(c) holds.

**Lemma 2.2.** If \( M^V \) is quasiprimitive and imprimitive, then one of (1) or (3) of Theorem 1.1 holds.

**Proof.** Suppose now that \( M^V \) is an imprimitive quasiprimitive permutation group. Then it follows, from applying [23, Theorem 2] to the inclusion \( G^V \leq M^V \), that either (i) \( M^V \) is almost simple whence, arguing as in the proof of Lemma 2.1, Theorem 1.1(1) holds if \( K = 1 \), and Theorem 1.1(3)(a) holds if \( K \neq 1 \), or (ii) \( \soc(M^V) \cong Sp_4(q_0) \times Sp_2(q_0) \), and \( G^V \cong G \cong Sp_4(q) \) is a diagonal subgroup of \( \soc(M^V) \), where \( q = q_0^r, r \geq 1, q \) is even, and \( M^V \) induces a primitive product action on a set of \( m^2 \) blocks of imprimitivity of size 2, where \( m = q^2(q^2 - 1)/2 \). Thus Theorem 1.1(3)(c) holds.

To complete the proof of Theorem 1.1, we need to demonstrate that there are examples of connected Cayley graphs for simple groups in each of the cases of Theorem 1.1. We use the following graph constructions. For a graph \( \Gamma \) and an integer \( t \geq 1 \), we use \( t \cdot \Gamma \) to denote the disjoint union of \( t \) copies of \( \Gamma \) (with no edges between distinct copies of \( \Gamma \)). The **lexicographic product** \( \Gamma[\Delta] \) of a graph \( \Gamma \) with a graph \( \Delta \) has vertex set \( V \Gamma \times V \Delta \) and \( (\gamma, \delta) \) is adjacent to \( (\gamma', \delta') \) if and only if either \( (\gamma, \gamma') \in E \Gamma \) or \( \gamma = \gamma' \) and \( (\delta, \delta') \in E \Delta \). It is clear from the definition that \( \Aut \Gamma[\Delta] \) contains \( \Aut \Delta \leq \Aut \Gamma \).

**Lemma 2.3.** In each of the cases (1)–(3) of Theorem 1.1, there are examples of simple groups \( G \), and connected Cayley graphs \( \Gamma = \Cay(G, S) \), such that some subgroup \( M \) satisfying \( GA(G, S) < M \leq \Aut \Gamma \) has the stated structure.

**Proof.** First, if \( S = G \setminus \{1\} \), then we may take \( M = \Sym(G) \) and case (1) holds. Next, whenever \( S = x^G \cup (x^{-1})^G \) for some \( x \in G \), the subgroup \( A(G, S) \) contains \( \Inn(G) \) and we may choose \( M \) so that case (2) holds. For the other cases, suppose that \( H \) is a self-normalizing subgroup of \( G \) of order \( t \), say, and \( S = H g H \cup H g^{-1} H \neq H \) such that \( A(G, S) \cap \Inn(G) = 1(H) \), the group of inner automorphisms of \( G \) induced by \( H \). (There are many instances of this, for example, we may take \( G = A_5, H = S_3 = G_{12,2}, \) and \( g = (13)(24) \).) The graph \( \Gamma = \Cay(G, S) \) is isomorphic to the lexicographic product \( \Gamma [t \cdot K_1] \), and so we have
Let \( K = (S_\ell)^{G:H} \), the base group of the wreath product, so \( K \leq \text{Aut}_\Gamma \). Since \( \text{Aut}(G,S) \cap \text{Inn}(G) = 1 \) \( (H) \), we have \( \text{Cap}(G) \cong H \), consisting of the elements of \( H \) acting by left multiplication. Thus \( \text{Cap}(G) \) is a diagonal subgroup of \( H \supseteq (S_\ell)^{G:H} = K \). If \( M := K(GA(G,S)) \), then \( M \) contains \( GA(G,S) \) and \( M/K \) is almost simple with socle \( G \), so case (3)(a) holds. If \( G = L_2(7) \), \( H = F_{21} \) (a Frobenius group of order 21), and \( S = G/H \), then \( \Gamma_H = \Gamma_K = K_8 \), and for \( M = K \operatorname{AGL}_3(2) \), case (3)(b) holds.

To obtain examples as in case (3)(c), we first consider the product action of \( L \ell S_2 \) of degree \( m^2 \) with soc \( L \ell L \) containing \( S_2 \) and \( L \ell S_2 \) corresponding to \( m^2 \) (or \( 2m^2 \)), and then choose the subset \( S \) to be the union of \( H \)-double cosets corresponding to a non-trivial self-paired orbital for the action of \( L \ell S_2 \) of degree \( m^2 \) (or \( 2m^2 \)). As in the previous paragraph, \( \Gamma = \text{Cay}(G,S) \) is isomorphic to the lexicographic product \( \Gamma_H \langle t \cdot K_1 \rangle \), where \( t = |H| \), and so we have \( S \ell \text{Aut}_\Gamma \leq \text{Aut}_\Gamma \). Let \( K = (S_\ell)^{G:H} \), the base group of the wreath product, so \( K \leq \text{Aut}_\Gamma \). In this case the graph \( \Gamma_H = \Gamma_K \) is isomorphic to the orbital graph for \( L \ell S_2 \) corresponding to this orbital, and consequently \( L \ell S_2 \) is contained in \( \text{Aut}_\Gamma \). Finally we choose \( M = K(GA(G,S)) \). If \( M \) acts faithfully on \( \Gamma_K \), and induces the group \( H \) on a block of the lexicographic product, standard theory for imprimitive permutation groups yields \( GA(G,S)) / \text{Cap}(M) \cong H \langle (L \ell S_2) \rangle \leq M \). From the previous paragraph, \( \text{Cap}(M) = \text{Cap}(G) \leq M \), and for each possibility for \( T, m \) it is easy to check that we have \( GA(G,S) \leq M \). Hence case (3)(c) holds. This completes the proof of Theorem 1.1.

3. Proof of Theorem 1.3

The following two lemmas will be used in the proof of Theorem 1.3. The first provides background information about representations of simple groups. The definitions of \( m(G) \), \( R_s(G) \) and \( |G|_r \), for a prime \( r \), were given at the end of Section 1.

**Lemma 3.1.** Let \( G \) be a finite nonabelian simple group, \( r \) a prime, and let \( |G|_r = r^{e(r)} \). Then the following hold:

(a) \( e(r) \leq (m(G) - 1)/(r - 1) < m(G) \), and \( e(2) \leq m(G) - 2 \).

(b) If \( r \) is odd, and \( G \) is not isomorphic to a simple group of Lie type in characteristic \( r \), then \( e(r) < R_s(G) \).

**Proof.** A proof of part (a) may be found, for example, in [7, Lemma 2.1]. For part (b) we refer to [13]. Suppose then that \( r \) is odd and that \( G \) is as in part (b). If \( G \cong A_n \), then by assumption \( n \neq (5,5) \) or \( (6,3) \). In this case the assertion follows from [13, Proposition 5.3.7]. Next, if \( G \) is a sporadic simple group, then the assertion follows from [13, Proposition 5.3.8]. Thus we may assume that \( G \) is a Lie type simple group in characteristic \( p \), say, where \( p \neq r \). Here very careful checking of the possibilities using [13, Theorem 5.3.9] yields the assertion. \( \square \)

The second of our preliminary lemmas describes the possible structure of an overgroup of \( GA(G,S) \) in \( \text{Aut}_\Gamma \) in the case where some, but not all, of the conditions of Hypothesis 1.2 hold.
Lemma 3.2. Let $G$ be a finite nonabelian simple group and $p$ a prime divisor of $|G|$. Let $P$ be a subgroup of $G$ of order $p$, and $x \in G$ of order $|x| > 2$, such that $\langle x^p \rangle = G$. Set $S = x^p \cup (x^{-1})^p$ and $\Gamma = \text{Cay}(G,S)$. Then the following hold:

(a) $\Gamma$ is a connected undirected graph of valency $2p$.

(b) If $M$ is a subgroup of $\text{Aut}\Gamma$ containing $GA(G,S)$ such that $M$ contains an intransitive normal subgroup $K$, then either

(i) $K$ is semiregular on $V\Gamma$, or

(ii) $M$ is arc-transitive on $\Gamma$, the stabilizer in $K$ of a vertex is a 2-group, and the quotient graph $\Gamma_K$ relative to $K$ has valency $p$.

Proof. (a) Since $\langle x^p \rangle = G$ and $x^p \subseteq S$, $\Gamma$ is connected. Also, since $S = S^{-1}$, $\Gamma$ is undirected. Write $S^+ = x^p$ and $S^- = (x^{-1})^p$. If $S^+ \cap S^- \neq \emptyset$, then there is an element $u \in P$ satisfying $x^u = x^{-1}$. It follows that $\langle x \rangle$ is normalized by $P$ and hence $\langle x^2 \rangle = \langle x \rangle$, which contradicts the assumption that $\langle x^2 \rangle = G$. Thus $S^+ \cap S^- = \emptyset$ and hence the valency of $\Gamma$ is $2p$.

(b) For $z \in V\Gamma$, let $\Gamma(z)$ denote the set of vertices of $V\Gamma$ adjacent to $z$. Since $K$ is normal in $M$ and $M$ is transitive on $V\Gamma$, all $K$-orbits in $V\Gamma$ have the same length. Suppose that $K$ is not semiregular on $V\Gamma$. Then $K_x \neq 1$, for each vertex $z$.

Let $x = 1 \in G = V\Gamma$, and let $\beta \in \Gamma(z)$. Suppose first that $M$ is arc-transitive on $\Gamma$. Then $M_x$ is transitive on $\Gamma(z)$. Since $K^{(\beta)} \leq M^{(\beta)}$, all of the $K_x$-orbits in $\Gamma(z)$ have the same length, and since $\Gamma$ is connected and $K_x \neq 1$, we have $K^{(\beta)} \neq 1$. If $K_x$ is transitive on $\Gamma(z)$, then the connectivity of $\Gamma$ implies that $\Gamma$ is bipartite with bipartition $V\Gamma = xK \cup \beta K$. However this means that $G$ contains a subgroup of index 2, which is not the case since $G$ is simple. Hence $K_x$ has orbits in $\Gamma(z)$ of length 2 or $p$. If the length is $p$, then the quotient graph $\Gamma_K$ has valency 2, and hence $\Gamma_K$ is a cycle. This implies that $\text{Aut}\Gamma_K$ contains a subgroup isomorphic to $G$, and hence $\Gamma_K$ is a 2-group. By [18, Lemma 1.5], the valency of $\Gamma_K$ is a proper divisor of $2p$, and since $\Gamma_K$ is not a cycle, the valency of $\Gamma_K$ is $p$. Thus (b)(ii) holds.

Suppose now that $M$ is not arc-transitive on $\Gamma$. Since $A(G,S)$ acts transitively on $S^+$ and $S^-$ and $A(G,S) < M$, it follows that $M_x$ has two orbits on $\Gamma(z)$, namely $S^+$ and $S^-$. Now each of $S^+$, $S^-$ has length $p$, and so $M_x$ is primitive on $S^+$ and $S^-$. Since $K_x \neq 1$, it follows from the connectivity of $\Gamma$ that $K_x$ acts nontrivially on at least one of $S^+$ and $S^-$. We may assume, without loss of generality, that $K^{(x)} \neq 1$. Since $M^{(x)}$ is primitive, it follows that $K^{(x)}$ is transitive. If also $K^{(x)} \neq 1$, then the same argument shows that $K^{(x)}$ is transitive. In this case the quotient graph $\Gamma_K$ has valency 2, which as above leads to a contradiction. Hence $K_x^{(x)} = 1$. Let $\beta = x^{-1} \in S^-$. Then $K_x \subseteq K_\beta$. Since $M$ is transitive on $V\Gamma$, $K_x$ and $K_\beta$ are conjugate in $M$, and so $[K_x] = [K_\beta]$. Hence $K_x = K_\beta$. On the other hand, the element $x^{-1} \in G \subseteq \text{Aut}\Gamma$ acts by right multiplication on $V\Gamma$ and sends $x$ to $x^{-1} = x^{-1} = \beta$. Hence $K^{(x)} = K^{(x)} = K^{(x)}$ acts transitively on $(S^+)^{-1} = S^+ x^{-1}$. However $z = 1 = xx^{-1} \in S^+ x^{-1}$ and $z$ is fixed by $K_\beta = K_x$, which is a contradiction. Thus the case where $M$ is not arc-transitive does not arise.

Now we turn to the proof of Theorem 1.3.
Proof of Theorem 1.3. Suppose that $G$, $P$, $S$ are as in Hypothesis 1.2, and that all the conditions of Hypothesis 1.2 hold. We have $\Gamma = G$, with $G$ acting by right multiplication and $A(G, S)$ acting naturally. Set $N := G.\langle A(G, S) \rangle$, then $N = N_{\text{Aut}}(G)$, and $G.\langle A(G, S) \cap \text{Inn}(G) \rangle = C_{\text{Aut}}(G) \times G$. Since $A(G, S) = I(P) \subset \text{Inn}(G)$, we have $N = C_{\text{Aut}}(G) \times G$ and $C_{\text{Aut}}(G) \cong P$. Now $P = \langle u \rangle$, for some $u \in G$. Set

$$\tau_u : g \mapsto u g, \quad \forall \ g \in G.$$ 

Then $C := C_{\text{Aut}}(G) = \langle \tau_u \rangle$, and $A(G, S) = \langle (\tau_u^{-1}, u) \rangle \leq C \times G = N$. Clearly, $N$ acts transitively on the vertices and edges of $\Gamma$. As in the proof of Lemma 3.2, we write $S^+ = x^p$ and $S^- = (x^{-1})^p$, so that $S = S \cup S^{-1}$. Since $\langle x^p \rangle = G$ and $S = S^{-1}$, $\Gamma$ is a connected undirected graph of valency $2p$ by Lemma 3.2.

To complete the proof it is sufficient to prove that $N$ is normal in $\text{Aut}\Gamma$. We suppose that this is not true. Then there exists a subgroup $M$ of $\text{Aut}\Gamma$ such that $N$ is a maximal proper subgroup of $M$. Since $N_{\text{Aut}}(G) \neq M$, $G$ is not normal in $M$. Let $K$ be a normal subgroup of $M$ which is maximal with respect to being intransitive on $\Gamma$. Possibly $K = 1$. Since $G$ is simple and is transitive on $\Gamma$, we have $G \cap K = 1$. Since $N \cap K$ is an intransitive normal subgroup of $N = G \times C$, it follows that $N \cap K = 1$ or $C$. First we apply Theorem 1.1 to clarify the possibilities for the structure of $M$.

Lemma 3.3. The normal subgroup $K$ is nontrivial, and $M = K.G$ with $N \cap K = C \neq K$. Moreover $|K|_2 := |K|/|K|_2$ divides $|G|$. Let $L$ be a minimal normal subgroup of $M$ which is contained in $K$. Then one of the following holds:

(a) $L = K$,

(b) $L = C$, and $K/C$ is a minimal normal subgroup of $M/C$.

(c) $K = L.C$ and $L \cap C = 1$.

Proof. We apply Theorem 1.1. Note that we have $M = NM_z$, where $z = 1 \in G = \Gamma$, and that $N \cong G \times Z_p$ is a maximal subgroup of $M$ and $N \cap M_z = A(G, S) \cong Z_p$. Also $M_z$ does not contain any nontrivial normal subgroup of $M$. Suppose first that case (1) of Theorem 1.1 holds. Then $G$ is a proper subgroup of the simple group $\text{soc}(M)$, and it follows that $N$ does not contain $\text{soc}(M)$. This contradicts condition (2) of Hypothesis 1.2. Thus case (1) does not hold for $M$. If case (2) of Theorem 1.1 holds, then $\text{Inn}(G) \leq A(G, S) \cong Z_p$, which contradicts condition (1) of Hypothesis 1.2. Thus case (3) of Theorem 1.1 holds, and in particular $K \neq 1$.

Let $H \leq M$ contain $K$ such that $H/K = \text{soc}(M/K)$. If case (3)(b) holds, then $C \subseteq K$ since $G.K/K \cong L_3(7)$ is self-centralizing in $M/K \cong \text{AGL}_3(2)$. Thus $N \leq K.G < M$, and since $N$ is maximal in $M$, this implies that $K = C$ and $N = K.G$. This means however that the $K$-orbits have length $p$, whereas in case (3)(b) they have length $|G|/8 = 21$. Thus case (3)(b) does not hold. If case (3)(c) holds, then $M \neq K.N$ since $M/K$ has socle $H.K \cong T \times T \supseteq G \times G$. Since $N$ is maximal, this means that $K \leq N$, and hence $K = C$. However this implies that $N$ is a proper subgroup of $H$, and hence by maximality $M = H$. However $H/K = \text{soc}(M/K)$ is a minimal normal subgroup of $M/K$ in this case and hence has index divisible by 2, so (3)(c) does not hold. Hence (3)(a) holds for $M$. Thus $N/K$ is almost simple, and $G.K \leq H.K$, so $G \leq H$. Suppose that $K = C$. Then $N = G.K \leq H$. If $N = H$ then $G$ is a characteristic subgroup of $N$ and $N = H$ is normal in $G$, so $G$ is normal in $M$, which is not the case. Hence $N < H$, and by the maximality of $N$, we have $H = M$ and $N/K \cong G$ is a maximal proper subgroup of the simple group $H/K$. Let $\Delta$ be the $K$-orbit containing $z$, and let $H_\Delta$ denote the setwise stabilizer of $\Delta$ in $H$. 


Then \(|G \cap H_A| = |A| = |K| = p\), and since \(H\) and \(G\) are transitive on \(V \Delta K\), we have a factorization \(H = GH_A\). This gives rise to the factorization \(H/K = (GK/K)(H_A/K)\) of the simple group \(H/K\), with \((GK/K) \cap (H_A/K) \cong \mathbb{Z}_p\), which contradicts condition (2) of Hypothesis 1.2. Hence \(K \neq C\). Thus \(K\) is not contained in \(N\), and so by the maximality of \(N\), we have \(M = K.N\). This means that \(M/K \cong N/(N \cap K)\) and \(N \cap K \leq C\). Since \(M/K\) is almost simple, \(M/K \not\cong G \times \mathbb{Z}_p\), and hence \(N \cap K = C \neq K\), \(M/K \cong G\), and \(M = K.G\). By Lemma 3.2, \(K_G\) is a 2-group, and so \(|K_G|\) divides the length of the \(K\)-orbits in \(V \Delta\), and hence divides \(|G|\). Let \(L\) be a minimal normal subgroup of \(M\) contained in \(K\), and suppose that \(L \neq K\). Suppose first that \(L\) contains \(C\). Then \(N \leq L.G\), and since \(L \neq K\), \(L.G\) is a proper subgroup of \(M\). The maximality of \(N\) implies that \(N = L.G\), and hence \(L = C\). The maximality of \(N\) now implies that \(K/C\) is a minimal normal subgroup of \(M/C\), and (b) holds. Thus we may assume that \(L \cap C = 1\). Then \(L\) is not contained in \(N\), and the maximality of \(N\) yields \(M = L.N\), whence \(K = L.C\) and (c) holds. \(\square\)

We now use Lemma 3.1 to help prove that \(K\) is soluble.

**Lemma 3.4.** The subgroup \(K\) is soluble.

**Proof.** Suppose that \(K\) is insoluble. Let \(X\) denote the characteristically simple group \(L, K/L, L\) in cases (a), (b) and (c) of Lemma 3.3 respectively. Then \(X = T^m\) for some nonabelian simple group \(T\) and positive integer \(m\), and \(G\) acts on \(X\). Note that in case (b), under the assumption that \(K/L\) is insoluble, it follows that \(L = C\) is central in \(K\), and consequently \(K \cong C \times X\). Thus in all cases we may assume that \(X\) is a minimal normal subgroup of \(M\). Let \(r\) be an odd prime divisor of \(|T|\). Then by Lemma 3.3, \(|G|\) is divisible by \(|T|^m\). If \(G\) permutes the simple direct factors of \(X\) nontrivially, then \(m \geq m(G)\), and so \(r^m(G)\) divides \(|G|\), which contradicts Lemma 3.1(a). Hence \(G\) normalizes each of the simple direct factors of \(X\). Since \(C_M(G) = C_{\text{Aut}}(G) = C \cong \mathbb{Z}_p\), there exists at least one of these simple direct factors which is not centralized by \(G\). Let \(T\) be one of these. Then as \(G\) is a nonabelian simple group, \(G\) is isomorphic to a subgroup of \(\text{Aut}(T)\), and as \(\text{Aut}(T)/\text{Inn}(T)\) is soluble, \(G\) is isomorphic to a subgroup of \(\text{Inn}(T)\). By Lemma 3.3, \(|K_G|\) divides \(|G|\), and this implies that \(m = 1, K = X = T\), and \(|T| = |G|\). In particular, case (a) of Lemma 3.3 holds. We have proved that the group of automorphisms of \(T\) induced by \(G\) by conjugation, is isomorphic to a subgroup of \(\text{Inn}(T)\) corresponding to a subgroup \(G_0\) of \(T\) isomorphic to \(G\). It follows that \(C_M(T) \cong G\) and \(M = T \times C_M(T)\). Since \(M = K.G = T.G\), and since \(G\) does not centralize \(T\), it follows that \(G\) is a diagonal subgroup of \(T \times C_M(T)\); in fact we may assume that \(G = \{(g,g^\sigma)\mid g \in G_0\}\), where \(\sigma : G_0 \longrightarrow C_M(T)\) is an isomorphism. On the other hand \(C = \tau_u < K = T\), and therefore \(\tau_u = \tau_u^{(g,g^\sigma)} = \tau_u^g\) for each \((g,g^\sigma) \in G\). Thus \(G_0\) centralizes \(C\), and so we have \(G_0 \times C \subseteq T\). However this implies that \(|T| = |G|\) for \(G\) of order \(r^m.p\), which is a contradiction. \(\square\)

Now we complete the proof of Theorem 1.3. As in the proof of Lemma 3.4, let \(X\) denote the characteristically simple group \(L, K/L, L\) in cases (a), (b), (c) of Lemma 3.3 respectively. Then \(X = Z^m_r\) for some prime \(r\) and positive integer \(m\). In case (a) of Lemma 3.3, \(G\) acts irreducibly on \(X = K\), but \(G\) centralizes the proper subgroup \(C\) of \(K\), which is a contradiction. Hence we are in case (b) or (c) of Lemma 3.3, and in particular \(|K| = r^m.p\). Suppose first that \(r\) is odd. Then \(K\) is
semiregular on $VT$ by Lemma 3.2, and so the setwise stabilizer in $G$ of a $K$-orbit is a subgroup of $G$ of order $r^m p$. If $G$ is isomorphic to a Lie-type simple group in characteristic $r$, then by condition (3) of Hypothesis 1.2, $p \neq r$ and $m < R_s(G)$, while if $G$ is not isomorphic to a Lie-type simple group in characteristic $r$, then by Lemma 3.1(b), $G$ is simple and does not centralize $K$. In either case, the subgroup of $\text{Aut}(K)$ which leaves invariant a subgroup of $K$ of order $p$ is soluble, so we have a contradiction. Hence $r = 2$, so $|K| = 2^m p$. By Lemma 3.2(b), the length of the $K$-orbits in $VT$ is $2^p$ for some $i \leq m$. Thus the setwise stabilizer in $G$ of a $K$-orbit is a subgroup of $G$ of order $2^p$ and by condition (1) of Hypothesis 1.2, $i \leq 1$. An argument similar to the one for $r$ odd yields that $G$ does not centralize $X$. Hence $m \geq R_s(G) \geq 2$. Thus $|K_3| = 2^{m-1} \geq 2^{m-1} > 1$. Since $\Gamma$ is connected, $K_3$ acts nontrivially on $\Gamma(z)$. By Lemma 3.2, $M$ is arc-transitive on $\Gamma$, so $K_3^{(2)}$ is a nontrivial normal subgroup of the transitive group $M_2^{(2)}$ of degree $2p$. Since $K_3$ is a 2-group, it follows that $K_3$ has $p$ orbits of length 2 in $\Gamma(z)$.

Suppose that we are in case (b) of Lemma 3.3. Let $X_0$ be a Sylow $2$-subgroup of $K$. Then $K = C.X_0$, and $X_0 \cong X \cong Z_2^n$ with $m \geq 2$. Since $\text{Aut}(C) \cong Z_{p-1}$ it follows that $C_X(C)$ has order at least $2^{m-1}$. Since $G$ normalizes $C_X(C) = C \times C_X(C)$, $G$ also normalizes $C_X(C)$. However, since $G$ is irreducible on $X = K/C$, it follows that $C_X(C) = X_0$, and $X_0$ is a minimal normal subgroup of $M$. Thus we may assume that we are in case (c) of Lemma 3.3. Then $K = L.C$, and so $L_2 = K_2$. Since the $K$-orbits in $VT$ have length $2^p$, with $i \leq 1$, it follows that the $L$-orbits have length 2, and form a $G$-invariant partition of $VT$. The $p$ orbits of length 2 of $L_2$ in $\Gamma(z)$ are therefore $L$-orbits. Let $\beta = g$ be the second point in the $L$-orbit containing $z = 1$. Then $g \in G$ maps $x$ to $\beta$, and hence leaves the $L$-orbit $\{x, \beta\}$ invariant. This means that $g$ maps $\beta$ to $x$; so $1 = \beta^g = g$. Let $\gamma \in \Gamma(z)$. Then $\Gamma(\gamma)$ is a union of $p$ orbits of $L$, and so $\beta \in \Gamma(\gamma)$. It follows that $\Gamma(z) = \Gamma(\beta)$. Thus we have $S = \Gamma(z) = \Gamma(\beta^g) = \Gamma(\beta)^g = \Gamma(\beta)^g = \Gamma(z)^g = Bg$. Since $S = S^{-1}$, we also have $g^{-1}Sg = g^{-1}S = g^{-1}S^{-1} = (Sg)^{-1} = S^{-1} = S$. Hence the inner automorphism of $G$ induced by the involution $g$ lies in $\text{Aut}(G,S)$, contradicting condition (1) of Hypothesis 1.2. This final contradiction completes the proof of Theorem 1.3.

4. Constructing half-transitive Cayley graphs of some finite simple groups

The purpose of this section is to construct some new families of half-arc transitive graphs using Theorem 1.3. Recall that a graph is half-transitive if it is vertex-transitive and edge-transitive, but not arc-transitive. Our first construction involves the alternating groups $A_{p+1}$, where $p$ is any prime satisfying $p \equiv 3 \pmod{4}$, and $p + 1$ is not a power of 2, that is, $p$ is not a Mersenne prime. This construction and Construction 4.4 give families of half-transitive graphs containing graphs of arbitrarily large valency. The proof refers to max+ and max− factorizations of almost simple groups. These were defined at the end of Section 1.

Construction 4.1. Let $G = A_{p+1}$, where $p$ is any prime satisfying $p \equiv 3 \pmod{4}$ such that $p + 1$ is not a power of 2. Let $P = (u) < G$, where $u = (1, 2, \ldots, p)$, and let
x = (1, 2, p+1). Set $S := \mathbb{Z}/(x^{-1})^p$, and $\Gamma := \text{Cay}(G, S)$. Then $\Gamma$ is a connected half-transitive graph of valency $2p$, and $\text{Aut}\Gamma = G \cdot I(P)$, where $I(P)$ denotes the subgroup of $\text{Inn}(G)$ induced by conjugation by elements of $P$.

**Proof.** We show that Hypothesis 1.2 holds. Let $G$ act naturally on the set $X = \{1, 2, \ldots, p+1\}$. First we consider $A(G, S)$. Clearly this group contains $I(P)$. Since $A(G, S) \leq S_{p+1}$, and since $p+1$ is the unique point of $X$ which is moved by every element of $S$, $A(G, S)$ fixes $p+1$. Suppose that $y \in A(G, S)$ fixes both $p+1$ and 1. Then $(1, 2, x^p = x^y) \in S$, and hence $2^p = 2$. Similarly $(2, 3, p+1 = x^y) \in S$ which implies that $y = 3$. It follows, since $I(P)$ is transitive on $\{1, 2, \ldots, p\}$, that $A(G, S) = I(P)$.

Next let $L < G$ be a subgroup of order $2^p$ for some $i$. Then $L$ is soluble, and without loss of generality we may assume that $L \leq L$. Thus either $L$ is 2-transitive on $X$, or $L$ fixes $p+1$ and is transitive on $X \setminus \{p+1\}$. In the former case, $L$ must have a normal elementary abelian 2-subgroup acting regularly on $X$, contradicting the fact that $p+1$ is not a power of 2. Thus $L$ acts faithfully as a soluble transitive permutation group of prime degree $p$. In particular $|L|$ divides $p(p-1)$, and since $p-1 \equiv 2 \pmod{4}$, it follows that $|L| = p$ or $2p$. Thus condition (1) of Hypothesis 1.2 holds.

Now we prove that condition (2) holds also. Suppose to the contrary that $L$ is an almost simple group and that $L = AB$, where $A, B$ do not contain $N := \text{soc}(L)$, $A$ is maximal in $L$, $A \cong G$ or $G \times \mathbb{Z}_p$, and $A \cap B \cong \mathbb{Z}_p$. Let $\hat{B}$ be maximal in $L$ such that $\hat{B} \cap B$ contains $B$ but does not contain $N$. Then it follows from [16] that for $L' := AN \cap \hat{B}N$, $A' := A \cap L'$, $\hat{B}' := \hat{B} \cap L'$, $L' = A' \hat{B}'$ is a max + factorization. That is, each of $A'$, $\hat{B}'$ is a maximal subgroup of $L'$ and does not contain $N$. Since also $A' \cong G$ or $G \times \mathbb{Z}_p$, we may assume without loss of generality that $L' = AB$ is a max + factorization. Such factorizations are classified in [15], and the possibilities are (i) $N = A_n$ for some $n$, or (ii) $N = \Omega_{12}(2) = A_{12}P_l$. However in the latter case (see [15, p. 115]), $A \cap \hat{B} \leq S_6 \times S_6$ so that $p = 11$ does not divide $|A \cap \hat{B}|$.

Hence $N = A_n$ and $L \leq S_6$. Let $Y$ be a set of size $n$ on which $L$ acts naturally. Since $n \geq p+1 \geq 12$, it follows from [15, Theorem D], that one of $A, B$ is contained in $S_{n-k} \times S_k$ and contains $A_{n-k}$, for some $k$ with $1 \leq k \leq 5$, and the other of $A, B$ is $k$-homogeneous on $Y$. Suppose first that $A_{n-k} \leq A \leq S_{n-k} \times S_k$. Then, since $A$ is maximal in $L$, $A$ has index 1 or 2 in $S_{n-k} \times S_k$, and hence $n = p+2$, $k = 1$, $A = A_{p+1}$, and $L = A_{p+2}$. In this case $B$ is transitive on $Y$ and $A \cap B \cong \mathbb{Z}_p$ is a point stabilizer in this action. This is impossible, since the fact that $p$ divides $|B|$ implies that $B$ is primitive on $Y$, while the fact that $|A \cap B| = p$ implies that $A \cap B$ fixes two points, and this is not allowed for a primitive group. Hence $A_{n-k} \leq B \leq S_{n-k} \times S_k$, and $A$ is $k$-homogeneous. Since $A$ is maximal in $L$, and is not a subgroup of index 1 or 2 in a wreath product, it follows that $A$ is primitive on $Y$, and hence $A \cong A_{p+1}$. This means that $A \leq A_n$, and by maximality, we therefore have $L = A_n$. Suppose that $k = 1$. Then $B = A_{n-1}$, and $A \cap B$ is a point stabilizer for the action of $A$ on $Y$. Since $|A \cap B| = p$, it follows that $A \cap B$ acts semiregularly on the $n-1$ remaining points of $Y$, and so $A$ is a Frobenius group, which is a contradiction, since Frobenius groups are not simple (see [25, 5.1 and 8.6]). Hence $2 \leq k \leq 5$, but there are no 2-homogeneous representations of $A_{p+1}$ of degree greater than $p+1$ (see [5]). Thus condition (2) of Hypothesis 1.2 holds. Now the required result follows from Theorem 1.3. \qed
Our second construction produces half-transitive graphs with automorphism groups involving some of the sporadic simple groups, namely $\text{BM}$, $J_1$, $J_4$ and $\text{Ly}$. (Note that the last two rows of Table 2 are referred to in the proof of the construction.)

**Construction 4.2.** Let $G$, $p$, $q$, be as in one of the columns of Table 2, and let $P = \langle u \rangle \cong \mathbb{Z}_p$, a Sylow $p$-subgroup of $G$. Then there exists $x \in G$ of order $q$ such that $N_G(\langle x \rangle) \cap N_G(P) = 1$. Let $x$ be such an element, and set $S := x^P \cup (x^{-1})^P$, and $\Gamma := \text{Cay}(G,S)$. Then $\Gamma$ is a connected half-transitive graph of valency $2p$, and $\text{Aut}\Gamma = G : \text{I}(P)$, where $\text{I}(P)$ denotes the subgroup of $\text{Inn}(G)$ induced by conjugation by elements of $P$.

**Proof.** For $G$, $p$, $q$ as in Table 2, and for $P = \langle u \rangle \cong \mathbb{Z}_p$ and $x \in G$ of order $q$, the normalizers $N_G(P) = \langle u \rangle \cdot \langle v \rangle$ and $N_G(\langle x \rangle) = \langle x \rangle \cdot \langle y \rangle$, where $|v|$ and $|y|$ are as in Table 2. Moreover $N_G(P)$ is a maximal subgroup of $G$, and every proper subgroup of $G$ of order divisible by $p$ is conjugate to a subgroup of $N_G(P)$. These assertions follow from [6, pp. 36, 174, 190, 217], [14] and [26]. In particular, $G$ contains no subgroups of order divisible by $4p$.

Suppose that $N_G(\langle x \rangle) \cap N_G(P) \neq 1$. Then by Table 2, it follows that $G \neq \text{BM}$, and for the other groups, this intersection is a subgroup of order 2. Now $N_G(\langle x \rangle)$ and $N_G(P)$ each contain a single conjugacy class of involutions, of size $q$ and $p$ respectively. Thus the involutions of $N_G(\langle x \rangle)$ and $N_G(P)$ belong to the same $G$-conjugacy class, say $c$, and counting pairs $(Q,w)$, where $Q$ is a subgroup of $G$ of order $q$, $w \in c$, and $w \in N_G(Q)$, we see that $|G:N_G(Q)| : q = |c| : s$, where $s$ is the number of subgroups of order $q$ normalized by an involution $w \in c$. Since $N_G(P)$ contains exactly $p$ involutions, the number of subgroups of order $q$ normalized by one of these $p$ involutions is equal to $ps$.

If $|N_G(Q) \cap N_G(P)| = 2$ for each subgroup $Q$ of order $q$, then we have $|G:N_G(Q)|$, and hence $|c| = pq$. Thus, for $w \in c$, $C_G(w)$ has index $pq$ in $G$, which is a contradiction by [6]. Hence there exists $x \in G$ of order $q$ such that $N_G(\langle x \rangle) \cap N_G(P) = 1$. Let $x$ be such an element, and let $S = x^P \cup (x^{-1})^P$.

Let $Y$ be the subgroup of $N_G(P)$ which stabilizes $S$ setwise, in the conjugation action of $N_G(P)$ on $S^G$. Then $Y$ contains $P$, so $Y = P \cdot \langle v' \rangle$ for some divisor $i$ of $|v|$. Since $P$ acts transitively by conjugation on $x^P$ and $(x^{-1})^P$, replacing $v'$ if necessary by a $Y$-conjugate, we may assume that $x^{v'} \in \langle x,x^{-1} \rangle$, and hence that $v' \in N_G(\langle x \rangle)$. However, since $N_G(\langle x \rangle) \cap N_G(P) = 1$, it follows that $v' = 1$, that is, $Y = P$.

Let $H = \langle x^P \rangle$, and suppose that $H \neq G$. Then $|G:H| > p$ (see [6]). Now $P$ normalizes $H$, so $HP$ is a proper subgroup of $G$ of order $|H| \cdot p$ divisible by $p$, contradicting our observations in the first paragraph of this proof. Hence $H = G$. Next we claim that $A(G,S) = \text{I}(P)$. For each group $G$ we have $\text{Out}(G) = 1$, and so $A(G,S) = \text{I}(K)$.

---

**Table 2. Sporadic simple groups for Construction 4.2.**

| $p$ | $q$ | $|v|$ | $|y|$ |
|-----|-----|------|------|
| 47  | 31  | 23   | 15   |
| 19  | 11  | 6    | 10   |
| 43  | 37  | 14   | 12   |
| 37  | 67  | 18   | 22   |
| 67  | 37  | 22   | 18   |

<table>
<thead>
<tr>
<th>$G$</th>
<th>$\text{BM}$</th>
<th>$J_1$</th>
<th>$J_4$</th>
<th>$\text{Ly}$</th>
<th>$\text{Ly}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$p$</td>
<td>$q$</td>
<td>$</td>
<td>v</td>
<td>$</td>
<td>$</td>
</tr>
<tr>
<td>47</td>
<td>31</td>
<td>23</td>
<td>6</td>
<td>19</td>
<td>10</td>
</tr>
<tr>
<td>19</td>
<td>11</td>
<td>6</td>
<td>10</td>
<td>43</td>
<td>12</td>
</tr>
<tr>
<td>43</td>
<td>37</td>
<td>14</td>
<td>12</td>
<td>37</td>
<td>22</td>
</tr>
<tr>
<td>37</td>
<td>67</td>
<td>18</td>
<td>22</td>
<td>67</td>
<td>18</td>
</tr>
</tbody>
</table>
\begin{table}[h]
\centering
\begin{tabular}{|c|c|c|}
\hline
Group & Structure & Remarks \\
\hline
P_{1} & \{q^{2}\}; Z_{q-1} & The normalizer of \{q^{2}\} in Ree(q) \\
\hline
P_{2} & (2^{n} \times D_{q+1}/2):3 & The normalizer of a four-group \\
\hline
P_{3} & 2 \times L_{2}(q) & An involution centralizer \\
\hline
P_{4} & Z_{q^{r+1}}; Z_{6} & The normalizer of \Z_{q^{r+1}} \\
\hline
P_{5} & Z_{q^{r+1}}; Z_{6} & The normalizer of \Z_{q^{r+1}} \\
\hline
P_{6} & Ree(3^{r}) & (2n+1)/d prime \\
\hline
P_{7} & Ree(3^{r}) = PSL(2,8) & \\
\hline
\end{tabular}
\caption{Maximal subgroups of Ree(q), q \geq 3.}
\end{table}

As a third application of Theorem 1.3, we construct another infinite family of half-transitive graphs, using groups from the family of Ree simple groups. For the construction we need some information about these groups. The simple Ree group Ree(q) \((q \geq 3)\) constructed in 1960 by R. Ree [24], has order \(q^{3} (q-1) (q^{3} + 1)\), where \(q = 3^{2n+1} \geq 27\). Write \(r := 3^{n+1}\), where \(n \geq 1\), so that \(r^{2} = 3q\). For an integer \(m \geq 1\), let [\(m\)] denote a group of order \(m\). A proof of the following lemma listing all the maximal subgroups of Ree(q) may be found in [12].

\textbf{Lemma 4.3 [12, Theorem C].} \textit{Let \(T\) be a maximal subgroup of Ree(q), where \(q = 3^{2n+1} \geq 27\). Then \(T\) is conjugate to one of the subgroups \(P_{i}\) \((1 \leq i \leq 7)\) in Table 3, and conversely all the subgroups \(P_{i}\) are maximal.}

**Construction 4.4.** Let \(G = Ree(q)\), where \(q = 3^{2n+1} \geq 27\), and let \(p\) be a prime divisor of \(q^{2} - q + 1\), so \(p\) divides \(q + \delta r + 1\) with \(\delta = +1\) or \(\delta = -1\). Let \(P\) be a subgroup of \(G\) of order \(p\). Then there exists \(x \in G\) of order \(q - \delta r + 1\) such that \(C_{\text{Aut}(G)}(x) \cap N_{\text{Aut}(G)}(P) = 1\), and no element of \(N_{\text{Aut}(G)}(P)\) inverts \(x\). Let \(x\) be such an element, and set \(S := x^{P} \cup (x^{-1})^{P}\) and \(\Gamma := \text{Cay}(G,S)\). Then \(\Gamma\) is a connected half-transitive graph of valency \(2p\), and \(\text{Aut}\Gamma = G \cdot I(P)\), where \(I(P)\) denotes the subgroup of \(\text{Ind}(G)\) induced by conjugation by elements of \(P\).
Hence $N_{\text{Aut}(G)}(P)$ contains $q + \delta r + 1$ involutions, and the number of subgroups of order $q - \delta r + 1$ which are normalized by one of the involutions of $N_{\text{Aut}(G)}(P)$ is at most $(q + \delta r + 1)(q^2 - 1)/6$. Thus there exist at least

$$t := \frac{|G|}{6(q - \delta r + 1)} - \frac{(q + \delta r + 1)(q^2 - 1)}{6}$$

subgroups $\langle x_1 \rangle, \ldots, \langle x_t \rangle$ of order $q - \delta r + 1$ which are normalized by no involution of $N_{\text{Aut}(G)}(P)$. Note that, for each $\langle x_i \rangle$, no element of $N_{\text{Aut}(G)}(P)$ inverts $x_i$; for if $y \in N_{\text{Aut}(G)}(P)$ and $x_i^y = x_i^{-1}$ then $|y|$ is even. Since $|N_{\text{Aut}(G)}(P)|$ is not divisible by 4, $|y| = 2m$ with $m$ odd, and $y^m$ is an involution in $N_{\text{Aut}(G)}(P)$ which inverts $x_i$ and hence normalizes $\langle x_i \rangle$, which is a contradiction.

Next we show that, for at least one $i \leq t$, we have $C_{\text{Aut}(G)}(x_i) \cap N_{\text{Aut}(G)}(P) = 1$. For each $i$, since $C_G(x_i) = \langle x_i \rangle$ we have $C_{\text{Aut}(G)}(x_i) \cap N_{\text{Aut}(G)}(P) = 1$. Also $N_{\text{Aut}(G)}(P) = N_{G(P)}Z_{2n+1}$. Hence $C_{\text{Aut}(G)}(x_i) \cap N_{\text{Aut}(G)}(P) = \langle y \rangle$ where $|y|$ divides $2n + 1$ and $\langle y \rangle \cap G = 1$. There are $|N_{\text{Aut}(G)}(P)| - |N_{G(P)}| = 12n(q + \delta r + 1)$ elements $y \in N_{\text{Aut}(G)}(P)/N_{G(P)}$. If one of these elements $y$ centralizes at least two of $x_1, \ldots, x_t$, say $x_i$ and $x_j$ with $i \neq j$, then $y$ would centralize $\langle x_i, x_j \rangle$. However it follows from Lemma 4.3 that $\langle x_i, x_j \rangle = G$, and hence $y$ would centralize $G$, which is a contradiction. Hence each of these elements $y$ centralizes at most one of the $x_i$, and so there are at most $12n(q + \delta r + 1)$ of the $x_i$ centralised by some element of $N_{\text{Aut}(G)}(P)/N_{G(P)}$. Since $12n(q + \delta r + 1) < t$, it follows that there exists $i \leq t$ such that $C_{\text{Aut}(G)}(x_i) \cap N_{\text{Aut}(G)}(P) = 1$.

Let $x$ be one of these elements, set $S = x^P \cup (x^{-1})^P$ and $\Gamma = \text{Cay}(G, S)$. By Lemma 4.3, $N_{G(P)}(\langle u \rangle : \langle x \rangle)$ where $|u| = q + \delta r + 1$ and $|\langle x \rangle| = 6$. Moreover, $N_{G(P)}$ is conjugate to one of $P_4$ or $P_5$, and $N_{G(\langle x \rangle)}$ is conjugate to the other, and both $\langle u \rangle$ and $\langle x \rangle$ are self-centralizing in $G$. We claim that $x^P$ and $(x^{-1})^P$ are disjoint subsets of each order $p$. If this is not so then we would have $x = x^u$ or $(x^{-1})^u$, for some $u \neq 1$. In either case $u$ normalizes $\langle x \rangle$, and since $p$ does not divide $|N_{G(\langle x \rangle)}|$ we have a contradiction. Thus $|S| = |x^P| + |(x^{-1})^P| = 2p$.

Next we show that $\langle x^P \rangle = G$. Let $H = \langle x^P \rangle$. Then $|H|$ is divisible by $q - \delta r + 1$, and so by Lemma 4.3, either $H = G$ or $H \leq N_G(\langle x \rangle)$. In the latter case, since $H$ is normalized by $P$, the subgroup $HP$ has order dividing $6(q^2 - q - 1)$ and divisible by $|H||P| = pq(q - \delta r + 1)$. By Lemma 4.3 there is no subgroup with this property. Hence $H = G$.

Now we prove that conditions (1)–(3) of Hypothesis 1.2 hold. It follows from Lemma 4.3 that $G$ has no subgroups of order $2^ip$ for $i \geq 2$, and also that condition (3) holds. To examine $A(G, S)$, let $I(G, S) = A(G, S) \cap I(G)$, the subgroup of inner automorphisms of $G$ contained in $A(G, S)$. Then $I(G, S)$ contains $I(P)$, so by Lemma 4.3, $I(G, S) = I(K)$ where either $K = G$ or $P \leq K \leq N_{G(P)}$. In the former case, $S$ contains $x^P(K) = x^P$, and this is impossible since $|x^P| = |G|/(q - \delta r + 1) > 2p$. Hence $P \leq K \leq N_{G(P)}$, and so $A(G, S) \leq N_{\text{Aut}(G)}(P)$. If $A(G, S)$ is transitive on $S$, then some element $z \in A(G, S)$ conjugates $x$ to $x^{-1}$. However this is not possible by our choice of $x$. Hence $A(G, S)$ has two orbits in $S$, namely $x^P$ and $(x^{-1})^P$. Let $B$
denote the stabilizer in $A(G,S)$ of $x$ in this action. Since $I(P)$ is transitive on $x^P$, we have $A(G,S) = I(P)B$. However

$$B = C_{A(G,S)}(x) \subseteq C_{Aut(G)}(x) \cap N_{Aut(G)}(P) = 1$$

by our choice of $x$. Hence $B = 1$ and so $A(G,S) = I(P)$.

Finally suppose that $L$ is an almost simple group which has a factorization $L = AB$ such that neither $A$ nor $B$ contains $soc(L)$, $A$ is maximal in $L$, $A \cong G$ or $G \times Z_p$, and $A \cap B = Z_p$. Let $B \leq B_1 < L$ with $B_1$ maximal such that $soc(L) \nsubseteq B_1$. Then by [15, Tables 1–6] and [16] we have either (i) $soc(L) = G_2(q)$, $soc(L) \cap A = G$, $soc(L) \cap B_1 = SL_2(q)$ or $SL_2(q)$-2, or (ii) $soc(L) = A_x$, $A$ is $k$-homogeneous of degree $c$, and $A_{c-k} \leq B \leq S_{c-k} \times S_k$, for some $k$ with $1 \leq k \leq 5$. In case (i), $G$ is self-centralizing in $L$ and hence $A \cong G$ and $A \leq soc(L)$. Since $A$ is maximal in $L$, we have $L = soc(L)$. However in this case $|A \cap B_1| = q - 1$ or $2(q - 1)$ and so $A \cap B \nsubseteq Z_p$. Thus we are in case (ii). If $k \geq 2$ then $A \cong G$, $c = q^3 + 1$, and $k = 2$. Thus $A_{c-k} \leq B \leq S_{c-k} \times S_2$. Therefore $A \cap B$ is the stabilizer of an unordered pair of points in the action of $G$ of degree $q^3 + 1$, and so $A \cap B \nsubseteq Z_p$, which is a contradiction. Hence $k = 1$, so $B = A_{c-1} \text{ or } S_{c-1}$, and $A$ is transitive of degree $c$, and maximal in $L$. Since $A \cong G$ or $G \times Z_p$, $A$ is not a maximal imprimitive subgroup of $L$, so $A$ is primitive of degree $c$ and hence $A \cong G$. Hence $A \cap B = Z_p$ is a point stabilizer in the primitive action of $A$ of degree $c$, so $A \cap B$ is a maximal subgroup of $A$, which contradicts Lemma 4.3.

Thus all parts of Hypothesis 1.2 hold and so the result follows from Theorem 1.3.

**Remark 4.5.** Typically we obtain several possibilities for the prime $p$ for each $q = 3^{2n+1} \geq 27$. We list a few small examples in Table 4. The possibilities for $p$ include in particular each primitive prime divisor of $3^{6(2n+1)} - 1$. (A *primitive prime divisor* of $3^m - 1$ is a prime dividing $3^m - 1$ which does not divide $3^i - 1$ for any $i < m$. Such primes exist for all $m \geq 3$ by [28].) Each primitive prime divisor of $3^{6(2n+1)} - 1$ is at least $6(2n + 1) + 1$ and hence this family contains graphs of arbitrarily large valency.

**Acknowledgements.** The authors thank Dr R. A. Wilson for helpful information about the subgroup structure of certain of the sporadic simple groups.

**References**


Xin Gui Fang
Jie Wang

Key Laboratory of Pure and Applied Mathematics
School of Mathematical Sciences
Peking University
Beijing 100871
China
xgfang@sxx0.math.pku.edu.cn
wangj@pku.edu.cn

Cheryl E. Praeger
Department of Mathematics and Statistics
University of Western Australia
35 Stirling Highway
Crawley
WA 6009
Australia
praeger@maths.uwa.edu.au