On automorphism groups of circulant digraphs of square-free order

Edward Dobson

Department of Mathematics and Statistics, Mississippi State University, PO Drawer MA Mississippi State, MS 39762

Joy Morris [1]

Department of Mathematics and Computer Science, University of Lethbridge, Lethbridge, AB. T1K 6R4. Canada

Abstract

We show that the full automorphism group of a circulant digraph of square-free order is either the intersection of two 2-closed groups, each of which is the wreath product of 2-closed groups of smaller degree, or contains a transitive normal subgroup which is the direct product of two 2-closed groups of smaller degree.

The work in this paper makes contributions to the solutions of two problems in graph theory. The most general, known as the König problem, asks for a concrete characterization of all automorphism groups of graphs. While it is known that every group is isomorphic to the automorphism group of a graph [12], determining the concrete characterization seems intractable. Thus, the natural approach is to consider either certain classes of graphs, or certain classes of groups. The second problem considered in this paper was posed by Elspas and Turner [11], when they asked for a polynomial time algorithm to calculate the full automorphism group of a circulant graph. (Note that it is unclear if a polynomial time algorithm exists.) That is, they essentially asked for an efficient solution to the König problem restricted to the class of graphs consisting of circulant graphs. In this paper, we will consider the class of circulant graphs of square-free order. We will show that the full automorphism group of a circulant digraph of square-free order is either the intersection of two 2-closed groups, each of which is the wreath product of 2-closed groups of smaller degree, or contains a transitive normal subgroup which is the direct

Email addresses: dobson@math.msstate.edu (Edward Dobson), joy@cs.uleth.ca (Joy Morris).

[1] This author gratefully acknowledges support from NSERC grant # 40188

product of two 2-closed groups of smaller degree. Several remarks are now in order. First, in the latter case, the possible over groups of the direct product of the 2-closed groups of smaller degree are found in this paper. Second, although this result in and of itself will not solve Elspas and Turner's original problem for circulant graphs of square-free order, we will show in a subsequent paper [22] that a polynomial time algorithm to calculate the full automorphism group of a circulant digraph of square-free order can be derived using this result. This algorithm is only polynomial time provided that the prime power decomposition on the order of the graph is known. Finally, several results have been previously obtained on Elspas and Turner's problem. The full automorphism groups of circulant digraphs of prime order [2] and [1], prime-squared order [18] (see [10] for another proof of this result), odd prime power order [19], and of a product of two distinct primes [18] have been obtained, and all of these results lead to polynomial time algorithms.

The proof of these results are presented in the four sections that follow. The first section includes preliminaries: primarily results from other sources that are used in this paper, and definitions. The second section looks at the structure of actions on blocks. More specifically, it uses results from the Classification of Finite Simple Groups and the structure of specific groups to prove Lemma 16, showing that faithful doubly-transitive nonsolvable actions on blocks must be equivalent. In the third section, under the hypothesis that a certain kind of block system exists, we prove results about the structure of blocks that are minimal with respect to the partial order defined in the preliminaries. Finally, we use the results of sections 2 and 3 to establish the main results described above.

1 Preliminaries

All groups and graphs in this paper are finite. For permutation group terminology not defined in this paper, see [8], and for graph theory terminology, see [3].

Definition 1. Let $S \subset \mathbb{Z}_n$ such that $0 \notin S$. We define a *circulant digraph* $\Gamma = \Gamma(\mathbb{Z}_n, S)$ by $V(\Gamma) = \mathbb{Z}_n$ and $E(\Gamma) = \{ij : i - j \in S\}$. If $S = -S$, then $\Gamma(\mathbb{Z}_n, S)$ is a *circulant graph*. Note that the function $x \to x + 1$ is contained in $\mathrm{Aut}(\Gamma)$, the *automorphism group of* Γ, so that $\mathrm{Aut}(\Gamma)$ is a transitive group.

While we are motivated by the problem of finding the full automorphism group of a circulant digraph, our results hold for a (perhaps) larger class of groups, which we now define.

Definition 2. Let Ω be a set and $G \leq S_\Omega$ be transitive. Let G act on $\Omega \times \Omega$

by $g(\omega_1, \omega_2) = (g(\omega_1), g(\omega_2))$ for every $g \in G$ and $\omega_1, \omega_2 \in \Omega$. We define the 2-*closure of* G, denoted $G^{(2)}$, to be the largest subgroup of S_Ω whose orbits on $\Omega \times \Omega$ are the same as G's. Let $\mathcal{O}_1, \ldots, \mathcal{O}_r$ be the orbits of G acting on $\Omega \times \Omega$. Define digraphs $\Gamma_1, \ldots, \Gamma_r$ by $V(\Gamma_i) = \Omega$ and $E(\Gamma_i) = \mathcal{O}_i$. Each Γ_i, $1 \leq i \leq r$, is an *orbital digraph of* G, and it is straightforward to show that $G^{(2)} = \cap_{i=1}^{r} \mathrm{Aut}(\Gamma_i)$. Note that $\mathcal{B}$ is a complete block system of G if and only if $\mathcal{B}$ is a complete block system of $G^{(2)}$. A *vertex-transitive graph* is a graph whose automorphism group acts transitively on the vertices of the graph. Clearly the automorphism group of a vertex-transitive graph or digraph is 2-closed.

Definition 3. Let G be a transitive permutation group of degree mk that admits a complete block system $\mathcal{B}$ of m blocks of size k. If $g \in G$, then g permutes the m blocks of $\mathcal{B}$ and hence induces a permutation in S^m, which we denote by $g/\mathcal{B}$. We define $G/\mathcal{B} = \{g/\mathcal{B} : g \in G\}$. Let $\mathrm{fix}_{\mathcal{B}}(G) = \{g \in G : g(B) = B \text{ for every } B \in \mathcal{B}\}$.

Definition 4. If $G \leq \mathrm{Aut}(\Gamma)$, for some vertex-transitive graph Γ, define a graph $\Gamma/\mathcal{B}$ with vertex set $V(\Gamma/\mathcal{B}) = \mathcal{B}$ and edge set

$$E(\Gamma/\mathcal{B}) = \left\{ (B, B') : \begin{array}{l} \text{some vertex of } B \text{ is adjacent} \\ \text{to some vertex of } B', B \neq B' \end{array} \right\}.$$

We observe that $G/\mathcal{B} \leq \mathrm{Aut}(\Gamma/\mathcal{B})$.

The following is a standard construction for obtaining vertex-transitive digraphs of larger order from vertex-transitive digraphs of smaller order.

Definition 5. Let Γ_1 and Γ_2 be vertex-transitive digraphs. Let

$$E = \{((x, x'), (y, y')) : xy \in E(\Gamma_1), x', y' \in V(\Gamma_2) \text{ or } x = y \text{ and } x'y' \in E(\Gamma_2)\}.$$

Define the *wreath* (*or lexicographic*) *product* of Γ_1 and Γ_2, denoted $\Gamma_1 \wr \Gamma_2$, to be the digraph such that $V(\Gamma_1 \wr \Gamma_2) = V(\Gamma_1) \times V(\Gamma_2)$ and $E(\Gamma_1 \wr \Gamma_2) = E$. We remark that the wreath product of a circulant digraph of order m and a circulant digraph of order n is circulant.

Definition 6. Let G and H be groups acting on X and Y, respectively. We define the *wreath product of* X *and* Y, denoted $G \wr H$, to be the permutation group that acts on $X \times Y$ consisting of all permutations of the form $(x, y) \to (g(x), h_x(y))$, where $g \in G$ and $h_g \in H$.

Clearly $\mathrm{Aut}(\Gamma_1) \wr \mathrm{Aut}(\Gamma_2) \leq \mathrm{Aut}(\Gamma_1 \wr \Gamma_2)$. For information about the converse, see [23].

Much of our proof exploits the fact that if G is a transitive permutation group that contains a regular cyclic subgroup R, then every block system of G is formed by the orbits of a normal subgroup of R (see, for example, [25,

Exercise 6.5]). As inclusion induces a natural partial order on the subgroups of a cyclic group, we have a natural partial order on the block systems of R.

Definition 7. Let X be the set of all possible complete block systems of $(\mathbb{Z}_n)_L$. Define a partial order on X by $\mathcal{B} \preceq \mathcal{C}$ if and only if every block of $\mathcal{C}$ is a union of blocks of $\mathcal{B}$.

Although this partial order depends on the value of n, for the purposes of this paper we will be using assuming that n is predetermined, so we can write $\prec$ in place of the more general $\prec_n$.

The following is not necessarily the usual definition of equivalent representations, but is equivalent (see [8, Theorem 1.6B]).

Definition 8. Let G act transitively on the sets Ω and Γ, and let H be the stabilizer of a point in the first action. We say the actions are *equivalent* if H is also the stabilizer of some point in the second action.

With these definitions in hand, we state some results from other publications that will be used in this paper.

Theorem 9. ([13], Theorem 1.49) *If H is a nonsolvable doubly transitive permutation group of degree m that contains an m-cycle, then one of the following holds:*

(i) $H \cong \mathcal{A}_m$ *or* $\mathcal{S}_m$*;*

(ii) $m = 11$ *and* $H = \mathrm{PSL}_2(11)$ *or* M_{11}*;*

(iii) $m = 23$ *and* $H \cong M_{23}$*;*

(iv) $m = (q^d - 1)/(q - 1)$ *for some prime power q and H is isomorphic to a subgroup of* $\mathrm{P\Gamma L}_d(q)$ *containing* $\mathrm{PSL}_d(q)$*.*

Theorem 10. *[8, Theorem 3.5B] Let G be a transitive group of prime degree p. Then either G is non-solvable and doubly transitive or we may relabel the set upon which G acts with elements of $\mathbb{F}_p$ so that $G \leq \mathrm{AGL}(1, p) = \{x \to ax + b : a \in \mathbb{F}_p^*, b \in \mathbb{F}_p\}$.*

Definition 11. Let G be a permutation group acting on the set Ω and $B \subseteq \Omega$ either a block of G or a union of orbits of G. Then for any $g \in G$ and any $x \in \Omega$, $g|_B(x) = g(x)$ if $x \in B$ and $g|_B(x) = x$ if $x \notin B$.

Let G be a transitive permutation group that admits a complete block system $\mathcal{B}$ of m blocks of size k, where $\mathcal{B}$ is formed by the orbits of some normal subgroup $N \triangleleft G$. Furthermore, assume that $\mathrm{fix}_G(\mathcal{B})|_B$ is primitive for every $B \in \mathcal{B}$, and that $\mathrm{fix}_G(\mathcal{B})$ is not faithful. Define an equivalence relation $\equiv$

on $\mathcal{B}$ by $B \equiv B'$ if and only if the subgroups of $\mathrm{fix}_G(\mathcal{B})$ that fix B and B', point-wise respectively, are equal. We denote these subgroups by $\mathrm{fix}_G(\mathcal{B})_B$ and $\mathrm{fix}_G(\mathcal{B})_{B'}$, respectively. Denote the equivalence classes of $\equiv$ by $C_0, \ldots, C_a$ and let $E_i = \cup_{B \in C_i} B$. The following result was proven in [9] in the case where $k = p$. It is straightforward to generalize this result to k being composite provided that $\mathrm{fix}_G(\mathcal{B})|_B$ is primitive for every $B \in \mathcal{B}$ and the action of $\mathrm{fix}_G(\mathcal{B})$ is not faithful.

Lemma 12. (Dobson, [9]) *Let $\vec{X}$ be a vertex-transitive digraph for which $G \leq \mathrm{Aut}(\vec{X})$ as above. Then $\mathrm{fix}_G(\mathcal{B})|_{E_i} \leq \mathrm{Aut}(\vec{X})$ for every $0 \leq i \leq a$. Furthermore, $\{E_i : 0 \leq i \leq a\}$ is a complete block system of G.*

As the 2-closure of a group G is equal to the intersection of the automorphism groups of the orbital digraphs of G, we have the following.

Lemma 13. *Let G be a transitive group as above. Then $\mathrm{fix}_G(\mathcal{B})|_{E_i} \leq G^{(2)}$ for every $0 \leq i \leq a$. Furthermore, $\{E_i : 0 \leq i \leq a\}$ is a complete block system of G.*

Lemma 14 ([17]). *For permutation groups $G \leq \mathcal{S}_X$ and $H \leq \mathcal{S}_Y$, the following hold:*

(1) Let $G \times H$ act canonically on $X \times Y$. Then $(G \times H)^{(2)} = G^{(2)} \times H^{(2)}$,
(2) Let $G \wr H$ act canonically on $X \times Y$. Then $(G \wr H)^{(2)} = G^{(2)} \wr H^{(2)}$.

To conclude our preliminary section, we give a short result that will be used repeatedly in later sections of this paper.

Lemma 15. *Let $G \leq \mathcal{S}_{mk}$ contain a regular cyclic subgroup $\langle \rho \rangle$. Assume that G admits a complete block system $\mathcal{B}$ of m blocks of size k formed by the orbits of $\langle \rho^m \rangle$. Furthermore, assume that $\mathrm{fix}_G(\mathcal{B})|_B$ admits a complete block system of r blocks of size s formed by the orbits of $\langle \rho^{mr} \rangle|_B$ for some $B \in \mathcal{B}$ $(rs = k)$. Then G admits a complete block system $\mathcal{C}$ of mr blocks of size s formed by the orbits of $\langle \rho^{mr} \rangle$.*

Proof. If $\mathrm{fix}_G(\mathcal{B})|_B$ admits a complete block system $\mathcal{C}_B$ of r blocks of size s formed by the orbits of $\langle \rho^{mr} \rangle|_B$ for some $B \in \mathcal{B}$, then $g(\mathcal{C}_B)$ is a complete block system of $\mathrm{fix}_G(\mathcal{B})|_{B'}$, where $g(B) = B'$. As $\langle \rho^m \rangle|_{B'} \leq \mathrm{fix}_G(\mathcal{B})|_{B'}$, every complete block system of $\mathrm{fix}_G(\mathcal{B})|_{B'}$ is formed by the orbits of $\langle \rho^{ma} \rangle|_{B'}$ for some $a \in \mathbb{Z}_k$. As for every divisor d of k, there is a unique subgroup of $\langle \rho^m \rangle|_{B'}$ of order d, we conclude that the blocks of $g(\mathcal{C}_B)$ ar e the orbits of $\langle \rho^{mr} \rangle|_{B'}$. Hence for every $B \in \mathcal{B}$, the orbits of $\langle \rho^{mr} \rangle|_B$ form a complete block system $\mathcal{C}_B$ of $\mathrm{fix}_G(\mathcal{B})|_B$. But then if $g \in G$, then $g(\mathcal{C}_B) = \mathcal{C}_{B'}$ for some B' so that $\mathcal{C} = \cup_{B \in \mathcal{B}} \mathcal{C}_B$ is a complete block system of G. □

2 Faithful doubly-transitive nonsolvable actions are equivalent

In this section, we consider a transitive permutation group G that contains a regular cyclic subgroup and admits a complete block system $\mathcal{B}$. We hypothesize that $\mathrm{fix}_G(\mathcal{B})$ acts faithfully, and that $\mathrm{fix}_G(\mathcal{B})|_B$ is doubly transitive and nonsolvable for every $B \in \mathcal{B}$. We use results from the Classification of Finite Simple Groups to determine specific permutation groups that may satisfy these hypotheses, and establish the structure we need on each of these specific permutation groups.

We begin this section with the statement and proof of its main result, even though the proof cites the subsequent results on specific groups. In this way, we are able to demonstrate clearly the motivation for the results on specific groups that follow.

Lemma 16. *Let $G \leq \mathcal{S}_{mk}$ admit a complete block system $\mathcal{B}$ of m blocks of size k, and contain a regular cyclic subgroup $\langle\rho\rangle$. Assume that $\mathrm{fix}_G(\mathcal{B})$ acts faithfully on $B \in \mathcal{B}$ and that $\mathrm{fix}_G(\mathcal{B})|_B$ is doubly transitive and nonsolvable for every $B \in \mathcal{B}$. Then $\mathrm{fix}_G(\mathcal{B})|_B$ is equivalent to $\mathrm{fix}_B(\mathcal{B})|_{B'}$ for every $B, B' \in \mathcal{B}$.*

Proof. Let $H = \langle \mathrm{fix}_G(\mathcal{B}), \rho\rangle$. Then $\mathrm{fix}_H(\mathcal{B}) = \mathrm{fix}_G(\mathcal{B})$. Let $B \in \mathcal{B}$. Perusing the list of doubly transitive groups given in [5, Theorem 5.3], we have (assuming towards a contradiction that there exist B_1, B_2 such that $\mathrm{fix}_G(\mathcal{B})|_{B_1}$ is not equivalent to $\mathrm{fix}_G(\mathcal{B})|_{B_2}$) that since $\mathrm{fix}_H(\mathcal{B})|_B$ has more than one representation, it has exactly two representations. Define an equivalence relation $\equiv$ on the elements permuted by $\mathcal{S}_{mk}$ by $i \equiv j$ if and only if $\mathrm{Stab}_{\mathrm{fix}_H(\mathcal{B})}(i) = \mathrm{Stab}_{\mathrm{fix}_H(\mathcal{B})}(j)$. As $\mathrm{fix}_H(\mathcal{B})|_B$ has two representations, there are $m/2$ elements in each equivalence class of $\equiv$ and these equivalence classes of $\equiv$ form a complete block system $\mathcal{C}$ of $2k$ blocks of size $m/2$ formed by the orbits of $\langle\rho^{2k}\rangle$. Then $H/\mathcal{C}$ admits a complete block system $\mathcal{D}$ of 2 blocks of size k formed by the orbits of $\langle\rho^2\rangle/\mathcal{C}$. Let $\mathcal{D} = \{D_1, D_2\}$. Furthermore, $\mathrm{fix}_{H/\mathcal{C}}(\mathcal{D})|_{D_1}$ is doubly transitive and nonsolvable and $\mathrm{fix}_{H/\mathcal{C}}(\mathcal{D})|_{D_1}$ is not equivalent to $\mathrm{fix}_{H/\mathcal{C}}(\mathcal{D})|_{D_2}$.

As $\rho \in H$, $\mathrm{fix}_{H/\mathcal{C}}(\mathcal{D})|_{D_1}$ contains a k-cycle. Hence $\mathrm{fix}_{H/\mathcal{C}}(\mathcal{D})|_{D_1}$ contains a k-cycle and has two representations. By Theorem 9 and [5, Theorem 5.3], together with k composite, we need only consider the cases where

$$\mathrm{soc}(\mathrm{fix}_{H/\mathcal{C}}(\mathcal{D})|_{D_1}) \cong \mathcal{A}_6 \ (k = 6),$$

$\mathrm{PSL}_d(q)$ ($k = (q^d - 1)/(q - 1)$ and $d > 2$), or $\mathrm{PSL}_2(11)$ (with $k = 11$). If $k = 6$ and $\mathrm{soc}(\mathrm{fix}_{H/\mathcal{C}}(\mathcal{D})|_{D_1}) \cong \mathcal{A}_6$, then as $\mathrm{fix}_{H/\mathcal{C}}(\mathcal{D})|_{D_1}$ contains a 6-cycle,

$$\mathrm{fix}_{H/\mathcal{C}}(\mathcal{D})|_{D_1} \cong \mathcal{S}_6,$$

contradicting Lemma 17 (stated and proven later). If $k = (q^d - 1)/(q - 1)$

and $\mathrm{soc}(\mathrm{fix}_{H/\mathcal{C}}(\mathcal{D})|_{D_1}) \cong \mathrm{PSL}_d(q)$, then by Corollary 22 (stated and proven later) $H/\mathcal{C}$ does not contain a $2k$-cycle, a contradiction. Finally, if $k = 11$ and $\mathrm{soc}(\mathrm{fix}_{H/\mathcal{C}}(\mathcal{D})|_{D_1}) \cong \mathrm{PSL}_2(11)$, then by Lemma 18 (stated and proven later), $H/\mathcal{C}$ does not contains a $2k$-cycle, a contradiction. □

Lemma 17. *Let $G \leq \mathcal{S}_{12}$ admit a complete block system $\mathcal{B}$ of 2 blocks of size 6. Let $\mathcal{B} = \{B_1, B_2\}$. Assume that $\mathrm{fix}_G(\mathcal{B})$ acts faithfully on $B \in \mathcal{B}$ and that $\mathrm{fix}_G(\mathcal{B}) \cong \mathcal{S}_6$ but $\mathrm{fix}_G(\mathcal{B})|_{B_1}$ is not equivalent to $\mathrm{fix}_G(\mathcal{B})|_{B_2}$. Then G does not contain a 12-cycle.*

Proof. Assume that G contains a 12-cycle, $\langle\rho\rangle$. Then $\mathcal{B}$ is formed by the orbits of $\langle\rho^2\rangle$ and $\rho^2 \in \mathrm{fix}_G(\mathcal{B})$. Then conjugation by ρ induces an automorphism α from $\mathrm{fix}_G(\mathcal{B})|_{B_1}$ to $\mathrm{fix}_G(\mathcal{B})|_{B_2}$. As $\mathrm{fix}_G(\mathcal{B})|_{B_1}$ is not equivalent to $\mathrm{fix}_G(\mathcal{B})|_{B_2}$, α is an outer automorphism of $\mathcal{S}_6$.

The group $\mathcal{S}_6$ has two kinds of elements of order 3: (a) 3-cycles, and (b) the product of two disjoint 3-cycles. Any element of type (b) is the square of a 6-cycle, but no element of type (a) is the square of a 6-cycle. It is well-known that there is an outer automorphism of $\mathcal{S}_6$ that interchanges type (a) and type (b) (cf. [24], 11.4.3, pp. 310-311). Thus, this outer automorphism cannot take any 6-cycle to another 6-cycle.

However, modulo inner automorphisms, there is only one outer automorphism of $\mathcal{S}_6$. Hence, as α is an outer automorphism of $\mathcal{S}_6$, $\alpha(\rho^2|_{B_1})$ is not a 6-cycle so that $\rho^{-1}\rho^2\rho \notin \langle\rho\rangle$, a contradiction. □

Lemma 18. *Suppose G admits a complete block system $\mathcal{B} = \{B_1, B_2\}$ of 2 blocks of size 11. Assume that $K = \mathrm{fix}_G(\mathcal{B})$, that $K|_B$ is doubly-transitive for each $B \in \mathcal{B}$, and that $\mathrm{soc}(K) \cong \mathrm{PSL}_2(11)$. Assume G has a transitive, cyclic subgroup $\langle\rho\rangle$. Then the action of $K|_{B_1}$ is equivalent to the action of $K|_{B_2}$.*

Proof. Without loss of generality, assume that $\mathrm{soc}(K) = \mathrm{PSL}_2(11)$. We want to show that if $x \in B_1$, there is some $y \in B_2$ for which $\mathrm{Stab}_K(x) = \mathrm{Stab}_K(y)$.

Define $f : K \to K$ by $f(k) = \rho^{-1}k\rho$. Then f is an automorphism of K, so it is well-known that there is some $a \in \mathrm{PGL}_2(11)$ for which $f(k) = a^{-1}ka$ for all $k \in K$ (cf. [6, p. 7], or the on-line version [7]). Let $P = \langle\rho^2\rangle$, a Sylow 11-subgroup of K. Then ρ centralizes P, so a is in the centralizer in $\mathrm{PGL}_2(11)$ of P, which is P. This means there is some $\rho^{2i} \in P$, such that $a = \rho^{2i}$. Hence $f(k) = \rho^{-1}k\rho = a^{-1}ka = \rho^{-2i}k\rho^{2i}$ for all $k \in K$. Thus, $\rho^{2i-1}k\rho^{1-2i} = k$ for every $k \in K$. So we have $\mathrm{Stab}_K(x) = \rho^{2i-1}\mathrm{Stab}_K(x)\rho^{1-2i} = \mathrm{Stab}_K(\rho^{2i-1}(x))$, completing the proof with $y = \rho^{2i-1}(x)$. □

The rest of this section deals with the group $\mathrm{PSL}_d(q)$ with $d \geq 3$. Several of these results were proven by Dr. Dave Witte, to assist us with this work. Since

they have not appeared elsewhere, the proofs are included here.

Note 1. In the remainder of this section, if V is a vector space, then $\mathbb{P}(V)$ is used to denote the set of all one-dimensional subspaces of the vector space.

Lemma 19. *Let $k = (q^d - 1)/(q - 1)$, with $d \geq 3$, write $q = p^r$ with p prime, and let $k' = k/\gcd(r, k)$. Let ρ' be an element of order k' in $\mathrm{PGL}_d(q)$ that acts semi-regularly on $\mathbb{P}((\mathbb{F}_q)^d)$. Then ρ' is not conjugate to $(\rho')^{-1}$ in $\mathrm{P\Gamma L}_d(q)$.*

Proof. Let $\hat{\rho'}$ be any lift of ρ' to $\mathrm{GL}_d(q)$. The cardinality of the linear span of any $\hat{\rho'}$-orbit is at least $(q-1)k'$, which is greater than q^{d-1}, so we see that $\hat{\rho'}$ is irreducible. Thus, by Schur's Lemma, the centralizer of $\hat{\rho'}$ in $\mathrm{Mat}(d, q)$ is a finite field. ¿From the cardinality, we conclude that the centralizer is isomorphic to $\mathbb{F}_{q^d}$. Abusing notation, we may assume that this centralizer is actually $\mathbb{F}_{q^d}$ itself. Thus, we may assume that $\hat{\rho'} \in \mathbb{F}_{q^d}^{\times}$ and that the centralizer of $\hat{\rho'}$ in $\mathrm{GL}_d(q)$ is $\mathbb{F}_{q^d}^{\times}$.

Suppose $g \in \mathrm{P\Gamma L}_d(q)$ with $g^{-1}\rho' g = (\rho')^{-1}$. Because g inverts ρ', it must normalize $\mathbb{F}_{q^d}^{\times}$, the centralizer of ρ' in $\mathrm{GL}_d(q)$. Therefore, the map $\mathbb{F}_{q^d} \to \mathbb{F}_{q^d}$ defined by $t \mapsto g^{-1}tg$ is clearly a field automorphism (i.e., it is bijective and respects addition and multiplication). So there is a natural number j, such that $g^{-1}tg = t^{p^j}$ for all $t \in \mathbb{F}_{q^d}$. (Because $t^{p^{rd}} = t^{q^d} = t$ for all $t \in \mathbb{F}_{q^d}$, we may and do assume $j \leq rd/2$.) Because $g^{-1}\rho' g = (\rho')^{-1}$, we must have $p^j \equiv -1 \pmod{k'}$, so

$$p^j + 1 \geq k' \geq \frac{p^{rd} - 1}{r(p^r - 1)} = \frac{p^{r(d-1)}}{r} + \frac{p^{r(d-2)}}{r} + \cdots > \frac{p^{r(d-1)}}{r} + \frac{p^{r(d-2)}}{r} > \frac{p^{r(d-1)}}{r} + 1.$$

It therefore suffices to show $p^{r(d-1)}/r \geq p^{rd/2}$, for this implies $j > rd/2$, a contradiction.

Case 1. Assume $(p, r) \neq (2, 3)$. We have $r \leq p^{r/2} \leq p^{(rd/2)-r}$, so

$$\frac{p^{r(d-1)}}{r} \geq \frac{p^{r(d-1)}}{p^{(rd/2)-r}} = p^{rd/2}.$$

Therefore, $j > rd/2$, a contradiction.

Case 2. Assume $(p, r) = (2, 3)$ and $d \geq 4$. We have

$$\frac{p^{r(d-1)}}{r} = \frac{8^{d-1}}{3} > 8^{d-2} \geq 8^{d/2} = p^{rd/2},$$

so $j > rd/2$, a contradiction.

Case 3. Assume $(p, r, d) = (2, 3, 3)$. We have

$$\begin{aligned} p^j + 1 &> \frac{p^{r(d-1)}}{r} + \frac{p^{r(d-2)}}{r} = \frac{2^{3(3-1)}}{3} + \frac{2^{3(3-2)}}{3} \\ &= 24 > 16\sqrt{2} + 1 = 2^{9/2} + 1 = p^{rd/2} + 1. \end{aligned}$$

Therefore, $j > rd/2$, a contradiction. □

Lemma 20. *Let $k = (q^d - 1)/(q - 1)$, with $d \geq 3$, write $q = p^r$ with p prime, let $k' = k/\gcd(r, k)$, and let V be a d-dimensional vector space over $\mathbb{F}_q$. Let ρ' be an element of order k' in $\mathrm{PGL}(V)$ that acts semi-regularly on $\mathbb{P}(V)$, and let $\mathbb{H}(V)$ be the set of all $(d-1)$-dimensional subspaces of V. There is a bijection $f\colon \mathbb{P}(V) \to \mathbb{H}(V)$ and an automorphism α of $\mathrm{P\Gamma L}(V)$, such that $\alpha(\rho') = (\rho')^{-1}$ and, for all $v \in \mathbb{P}(V)$ and all $g \in \mathrm{P\Gamma L}(V)$, we have $f(gv) = \alpha(g)f(v)$.*

Proof. Let $\hat{\rho}'$ be a representative of ρ' in $\mathrm{GL}(V)$. From the beginning of the proof of the preceding lemma, we see that we may assume $V = \mathbb{F}_{q^d}$ and that $\hat{\rho}' \in \mathbb{F}_{q^d}^{\times}$.

Define $\mathrm{tr}\colon \mathbb{F}_{q^d} \to \mathbb{F}_q$ by $\mathrm{tr}(t) = t + t^q + \cdots + t^{q^{d-1}}$ (so tr is the "trace map" from $\mathbb{F}_{q^d}$ to $\mathbb{F}_q$), and define an $\mathbb{F}_q$-bilinear form on $\mathbb{F}_{q^d}$ by $\langle s \mid t \rangle = \mathrm{tr}(st)$. Because $\mathbb{F}_{q^d}$ is a separable extension of $\mathbb{F}_q$, this bilinear form is non-degenerate (i.e., for every nonzero $s \in \mathbb{F}_{q^d}$, there is some $t \in \mathbb{F}_{q^d}$ with $\langle s \mid t \rangle \neq 0$). For each one-dimensional $\mathbb{F}_q$-subspace W of $\mathbb{F}_{q^d}$, define

$$f(W) = \{\, v \in \mathbb{F}_{q^d} \mid \langle v \mid W \rangle = 0 \,\}.$$

Because the bilinear form is non-degenerate, f is a bijection from the set of one-dimensional subspaces of $\mathbb{F}_{q^d}$ onto the set of $(d-1)$-dimensional subspaces.

For each $g \in \mathrm{P\Gamma L}(V)$, let g^T be the transpose of g with respect to the bilinear form (that is, $\langle v \mid gw \rangle = \langle g^T v \mid w \rangle$), and let $\rho(g) = (g^T)^{-1}$.

Because $\langle \rho(g)v, gW \rangle = \langle (g^T)^{-1}v, gW \rangle = \langle g^T(g^T)^{-1}v, W \rangle = \langle v, W \rangle$, it is clear that $f(gW) = \rho(g)f(W)$.

Furthermore, for every $v, w \in \mathbb{F}_{q^n}$, we have $\langle \hat{x}^{-1}v, \hat{x}w \rangle = \mathrm{tr}((\hat{x}^{-1}v)(\hat{x}w)) = \mathrm{tr}(vw)$, so it is clear that $f(\hat{\rho}'W) = \hat{\rho}'^{-1} f(W)$, so $\alpha(\hat{\rho}') = \hat{\rho}'^{-1}$. □

Proposition 21. *Let $k = (q^d - 1)/(q - 1)$, with $d \geq 3$. Suppose $\mathrm{PSL}_d(q) \leq G \leq \mathrm{P\Gamma L}_d(q)$ with $d \geq 3$, and let H be a group that contains G as a normal subgroup. Suppose H acts imprimitively on a set Ω, with a complete block system $\{B_1, B_2\}$ consisting of 2 blocks of cardinality k. Assume $G = \{\, h \in H \mid h(B_1) = B_1,\ h(B_2) = B_2 \,\}$. Assume G acts doubly transitively on B_i for each*

$i = 1, 2$, and that the action of G on B_1 is not equivalent to the action of G on B_2. Then H does not contain a transitive, cyclic subgroup.

Proof. Suppose H does contain a transitive, cyclic subgroup $\langle\rho\rangle$. Then G contains a cyclic subgroup $\langle\rho'\rangle$ that is transitive on each of B_1 and B_2 (and we may assume that $rho' \in \langle\rho\rangle$). Write $q = p^r$ with p prime, and let $k' = k/\gcd(r, k)$, so $(\rho')^r$ is an element of order k' in $\mathrm{PGL}_d(q)$ that acts semi-regularly.

Because the action of G on B_1 is not equivalent to the action of G on B_2, one of the actions (say, the action on B_1), must be isomorphic to the action of G on $\mathbb{P}((\mathbb{F}_q)^d)$; and the other action must be isomorphic to the action of G on $\mathbb{H}((\mathbb{F}_q)^d)$.

Let $G' = \langle\rho'^r\rangle\mathrm{PSL}_d(q) \subset G$. By combining the conclusion of the preceding paragraph with Lemma 20, we see that there is a bijection $f\colon B_1 \to B_2$ and an automorphism α of $\mathrm{P\Gamma L}_d(q)$, such that $\alpha((\rho')^r) = (\rho')^{-r}$ and, for all $v \in B_1$ and all $g \in G'$, we have $f(gv) = \alpha(g)f(v)$.

Note that $\alpha(G') = G'$, because $\alpha((\rho')^r) = (\rho')^{-r}$ and because every automorphism of $\mathrm{P\Gamma L}_d(q)$ normalizes $\mathrm{PSL}_d(q)$. Also note that ρ normalizes G', because ρ centralizes ρ' (recall that $\rho' \in \langle\rho\rangle$) and because $\mathrm{PSL}_d(q)$ is normal in H (since $\mathrm{PSL}_d(q)$ is characteristic in G, and G has index two in H). Therefore, we may define an automorphism α' of G' by $\alpha'(g) = \rho\alpha(g)\rho^{-1}$.

Because $\langle\rho\rangle$ is transitive, we know that $\rho(B_2) = B_1$, so we may define a permutation f' of B_1 by $f'(v) = \rho f(v)$. Then, for all $v \in B_1$ and all $g \in G'$, we have

$$f'(gv) = \rho f(gv) = (\rho\alpha(g)\rho^{-1})\rho f(v) = \alpha'(g)f'(v). \tag{1}$$

Thus, the permutation f' normalizes $G'|_{B_1}$, so f' normalizes $\mathrm{PSL}_d(q)$, from which we conclude that $f' \in \mathrm{P\Gamma L}_d(q)$.

Because $\rho' \in \langle\rho\rangle$, we know that ρ centralizes $(\rho')^r$, so

$$\alpha'((\rho')^r) = \rho\alpha((\rho')^r)\rho^{-1} = \rho(\rho')^{-r}\rho^{-1} = (\rho')^{-r}.$$

Therefore, from (1), we conclude that f' conjugates $(\rho')^r|_{B_1}$ to $(\rho')^{-r}|_{B_1}$. This contradicts the conclusion of Lemma 19. □

Corollary 22. *Let $G \leq \mathcal{S}_{2k}$ admit a complete block system $\mathcal{B}$ of 2 blocks of size k. Assume that $\mathrm{Stab}_G(\mathcal{B})$ acts faithfully on $B \in \mathcal{B}$ and $\mathrm{soc}(\mathrm{Stab}_G(\mathcal{B})) \cong \mathrm{PSL}_d(q)$, where d is an integer, q is a prime power, and $k = (q^d - 1)/(q - 1)$. Let $\mathcal{B} = \{B_1, B_2\}$. If $\mathrm{Stab}_G(\mathcal{B})|_{B_1}$ is not equivalent to $\mathrm{Stab}_G(\mathcal{B})|_{B_2}$, then G does not contain a $2k$-cycle.*

Proof. Most of this result is trivial from Proposition 21. When $d = 2$, we have $\mathrm{PSL}_2(q)$, and this group has only one transitive representation acting on $(q^d - 1)/(q - 1) = q + 1$ points. This is because the stabilizer of a point in such a representation is the normalizer of a Sylow p-subgroup (where p is the prime dividing q), and so by one of the Sylow theorems they are all conjugate. Thus, when $d = 2$, the hypotheses of this lemma cannot arise. □

3 The structure of minimal blocks

We now wish to prove a lemma which will be a crucial tool. If a block system with particular characteristics exists and consists of more than one block, this lemma will establish that there is a complete block system of G, minimal with respect to our partial order, upon which we know something about the action of G or its 2-closure. As the proof of this lemma is quite long, the proof will be broken down into a sequence of lemmas. We now develop the notation and hypotheses which will be used throughout this section.

Hypothesis 23. Let k and m be integers such that km is square-free. Let $G \leq \mathcal{S}_{km}$ be a transitive permutation group that contains a regular cyclic subgroup $\langle \rho \rangle$ and admits a complete block system $\mathcal{B}$ with m blocks of size k. We assume that

- $\mathrm{fix}_G(\mathcal{B})$ is of order k,
- $\mathrm{fix}_G(\mathcal{B}) \leq \mathrm{C}(G)$ (the center of the group G), and
- there exists no complete block system $\mathcal{F} \succ \mathcal{B}$ such that $\mathrm{fix}_G(\mathcal{F})$ is semiregular.

These assumptions will hold throughout this section, and we will assume that all results in this section satisfy the above hypothesis. Additionally, the following conditions will sometimes be assumed and will be referred to as Conditions (1) and (2), respectively:

(1) there exists a complete block system $\mathcal{D}$ of G such that $\mathrm{fix}_G(\mathcal{D})$ is not of order $|D|$, $D \in \mathcal{D}$, and there exists no nontrivial complete block system $\mathcal{E}$ of G such that $\mathcal{E} \prec \mathcal{D}$, or
(2) there exists a prime $p|k$ such that $G^{(2)}$ admits a complete block system $\mathcal{D}'$ of mk/p blocks of size p and p^2 divides $|\mathrm{fix}_{G^{(2)}}(\mathcal{D}')|$.

The next few lemmas involve consideration of a complete block system $\mathcal{C}$ with $\mathcal{C} \succ \mathcal{B}$, and $\mathcal{C}$ consists of $\frac{m}{t}$ blocks of size kt for some $t|m$. Therefore, until further notice, it will be convenient to view $\mathbb{Z}_{mk}$ as $\mathbb{Z}_{\frac{m}{t}} \times \mathbb{Z}_t \times \mathbb{Z}_k$ with $\rho(x, y, z) = (x + 1, y + 1, z + 1)$ (we can assume this, since mk is square-free), where the complete block systems $\mathcal{B}$ and $\mathcal{C}$ are given by $\mathcal{B} = \{\{(x, y, z) : x \in$

$\mathbb{Z}_{\frac{m}{t}}, y \in \mathbb{Z}_t\} : z \in \mathbb{Z}_k\}$, and $\mathcal{C} = \{\{(x, y, z) : x \in \mathbb{Z}_{\frac{m}{t}}\} : y \in \mathbb{Z}_t, z \in \mathbb{Z}_k\}$.

Lemma 24. *Under Hypothesis 23, suppose that $m > 1$ and Condition (1) does not hold. Let $\mathcal{C}$ be any complete block system of G with $\mathcal{C} \succ \mathcal{B}$ that is minimal in the sense that there is no complete block system $\mathcal{C}'$ of G with $\mathcal{B} \prec \mathcal{C}' \prec \mathcal{C}$. Then $(\mathrm{fix}_G(\mathcal{C})|_C)/\mathcal{B}$ is doubly transitive and nonsolvable.*

Proof. Towards a contradiction, suppose that $(\mathrm{fix}_G(\mathcal{C})|_C)/\mathcal{B}$ is not doubly transitive, or is solvable. If t were composite, then since $(\mathrm{fix}_G(\mathcal{C})|_C)/\mathcal{B}$ contains a regular cyclic subgroup of order t and all cyclic groups of composite order are Burnside groups [25, Theorem 25.3], we would have $(\mathrm{fix}_G(\mathcal{C})|_C)/\mathcal{B}$ being doubly transitive. (The minimality of $\mathcal{C}$ means that $(\mathrm{fix}_G(\mathcal{C})|_C)/\mathcal{B}$ cannot be imprimitive.) By [16, Exercise 1, p. 169,], we must have $t = 4$, a contradiction.

So t is prime, and by Theorem 10, $(\mathrm{fix}_G(\mathcal{C})|_C)/\mathcal{B} \leq \mathrm{AGL}(1, t)$. Let T be a Sylow t-subgroup of $\mathrm{fix}_G(\mathcal{C})$ that contains $\langle \rho^{mk/t} \rangle$. Now, $(\mathrm{fix}_G(\mathcal{C})|_C)/\mathcal{B}$ contains a unique Sylow t-subgroup, which must be $(T|_C)/\mathcal{B}$. Since $\mathrm{fix}_G(\mathcal{C})/\mathcal{B} \leq 1_{\mathcal{S}_{m/t}} \wr \mathrm{AGL}(1, t)$, this also contains a unique Sylow t-subgroup, which must be $T/\mathcal{B}$. So $T/\mathcal{B}$ is characteristic in $\mathrm{fix}_G(\mathcal{C})/\mathcal{B}$, and is therefore normal in $G/\mathcal{B}$. Now, since $(k, t) = 1$, $\mathrm{fix}_G(\mathcal{B})$ is centralized by T (since $\mathrm{fix}_G(\mathcal{B})$ is central in G), and $T/\mathcal{B}$ is normal in $G/\mathcal{B}$, we must have $T \triangleleft G$. So the orbits of T form a complete block system $\mathcal{D}'$ of G.

We may also assume $|\mathrm{fix}_G(\mathcal{D}')| = t$, since if this were not the case, Condition (1) would follow, a contradiction (the blocks of $\mathcal{D}'$ have no nontrivial subblocks since t is prime). So $\mathrm{fix}_G(\mathcal{D}') = \langle \rho^{mk/t} \rangle$. As $\mathcal{D}'$ is formed by the orbits of T, we thus have that $T = \mathrm{fix}_G(\mathcal{D}') = \langle \rho^{mk/t} \rangle$. We also can now conclude that $\langle \rho^{m/t} \rangle \triangleleft G$.

Since $\mathrm{fix}_G(\mathcal{C})$ is not cyclic (by Hypothesis 23), there must be some $\gamma \in \mathrm{fix}_G(\mathcal{C})$ for which $\gamma/\mathcal{B} \notin T/\mathcal{B}$. Then we have $\gamma(x, y, z) = (x, \alpha_x(y) + a_x, \beta_x(z) + b_x)$, $\alpha_x \in \mathbb{Z}_t^*$, $a_x \in \mathbb{Z}_t$, $\beta_x \in \mathbb{Z}_k^*$, and $b_x \in \mathbb{Z}_k$ as γ normalizes $\langle \rho^{m/t} \rangle$. As $\langle \rho^m \rangle$ is in the center of G, we must have that $\beta_x = 1$ for every $x \in \mathbb{Z}_{m/t}$. Since $\mathrm{fix}_G(\mathcal{D}') = \langle \rho^{mk/t} \rangle \triangleleft G$, conjugating $\rho^{mk/t}$ by γ shows that $\alpha_x = \alpha'_x = \alpha$ for any $x, x' \in \mathbb{Z}_{\frac{m}{t}}$.

Choose i so that $\rho^{itk}(x, y, z) = (x + 1, y, z)$ for every $(x, y, z) \in \mathbb{Z}_{\frac{m}{t}} \times \mathbb{Z}_t \times \mathbb{Z}_k$. Straightforward calculations show that $\gamma^{-1}\rho^{-itk}\gamma\rho^{itk}(x, y, z) = (x, y + \alpha^{-1}(a_{x+1} - a_x), z + b_{x+1} - b_x)$. Therefore, $\gamma^{-1}\rho^{-itk}\gamma\rho^{itk}/\mathcal{B} \in T/\mathcal{B}$ (the unique Sylow t-subgroup of $\mathrm{fix}_G(\mathcal{C})/\mathcal{B}$). Since $T = \mathrm{fix}_G(\mathcal{D}')$ has order t, $T/\mathcal{B}$ has order t, and as $\rho^{mk/t}/\mathcal{B} \in T/\mathcal{B}$, we must have that $a_{x+1} - a_x = c$ is constant for every $x \in \mathbb{Z}_{\frac{m}{t}}$. Then $a_1 = c + a_0$, $a_{x+1} = c + a_x$ so that $a_{x+1} = (x + 1)c + a_0$. Hence $a_0 = \frac{m}{t} \cdot c + a_0$. Since $\gcd(\frac{m}{t}, t) = 1$, $c = 0$, and so $a_{x+1} = a_x = a$ is constant. Without loss of generality, since $\rho \in G$, we may assume that a is 0. Now since $\gamma^{-1}\rho^{itk}\gamma\rho^{itk} \in \mathrm{fix}_G(\mathcal{B})$, $b_{x+1} - b_x$ must be constant. Since $(\frac{m}{t}, k) = 1$,

this constant must be 0, so $b_{x+1} = b_x = b$ is constant. Still without loss of generality because of the presence of ρ in G, we may assume that b is 0. But now $\gamma(x, y, z) = (x, \alpha y, z)$, so $\gamma \in \mathrm{fix}_G(\mathcal{D}') = \langle \rho^{mk/t} \rangle$, a contradiction. □

Lemma 25. *Under Hypothesis 23, suppose that $m > 1$ and Condition (1) does not hold, and let $\mathcal{C}$ be as in Lemma 24. Let $L = \{g^{-1}\rho^{\frac{mk}{t}}g : g \in G\}$ and $H = \langle L \rangle$. Then*

(1) $H \triangleleft G$,
(2) the orbits of H have order $k't$ for some $k'|k$, $k' \neq 1$,
(3) $\langle \rho^m \rangle \cap H = 1$, and
(4) If $h \in H$ has the form $h(x, y, z) = (x, \sigma_x(y), z + b_{x,y})$ then $\sum_{y=0}^{t-1} b_{x,y} \equiv 0 \pmod{k}$ for every x.

Proof. By Lemma 24, we have that $(\mathrm{fix}_G(\mathcal{C})|_C)/\mathcal{B}$ is a doubly-transitive non-solvable group. Note that every element of L has order t.

1. Any $\vartheta \in H$ must be of the form $\vartheta = \gamma_1^{a_1}\gamma_2^{a_2}\cdots\gamma_\ell^{a_\ell}$, where $a_i \in \mathbb{Z}_t$ and $\gamma_i \in L$ for $i = 1, \ldots, \ell$. For any $g \in G$ we then have

$$\begin{aligned} g^{-1}\vartheta g &= g^{-1}\gamma_1^{a_1}\gamma_2^{a_2}\cdots\gamma_\ell^{a_\ell}g \\ &= (g^{-1}\gamma_1 g)^{a_1}(g^{-1}\gamma_2 g)^{a_2}\cdots(g^{-1}\gamma_\ell g)^{a_\ell}. \end{aligned}$$

As $\gamma_i \in L$, we have $\gamma_i = g_i^{-1}\rho^{\frac{kr}{t}}g_i$ for some $g_i \in G$. Hence

$$g^{-1}\gamma_i g = (g_i g)^{-1}\rho^{\frac{kr}{t}}(g_i g) \in L$$

and $g^{-1}\vartheta g \in H$. Therefore $H \triangleleft G$.

3 and 4. Since $\rho^{\frac{mk}{t}} \in \mathrm{fix}_G(\mathcal{C})$ and $\mathrm{fix}_G(\mathcal{C}) \triangleleft G$, we have that $H \leq \mathrm{fix}_G(\mathcal{C})$. As $H \leq \mathrm{fix}_G(\mathcal{C})$, any $\gamma \in L$ acts as $\gamma(x, y, z) = (x, \delta_x(y), z + d_{x,y})$ where $\delta_x \in \mathcal{S}_t$ is of order t and $d_{x,y} \in \mathbb{Z}_k$ for every $x \in \mathbb{Z}_{\frac{m}{t}}$ and $y \in \mathbb{Z}_t$. Since $|\gamma| = t$ and $\gcd(m, k) = 1$, we have that $\sum_{y\in\mathbb{Z}_t} d_{x,y} \equiv 0 \pmod{k}$ for every $x \in \mathbb{Z}_{\frac{m}{t}}$. Therefore every $\vartheta \in H$, since it is of the form $\gamma_1^{a_1}\gamma_2^{a_2}\cdots\gamma_\ell^{a_\ell}$ for $\gamma_1, \gamma_1, \ldots, \gamma_\ell \in L$, acts as $\vartheta(x, y, z) = (x, \varepsilon_x(y), z + e_{x,y})$, where $\sum_{y\in\mathbb{Z}_t} e_{x,y} \equiv 0 \pmod{k}$ for every $x \in \mathbb{Z}_{\frac{m}{t}}$. It is now clear that $\langle \rho^m \rangle \cap H = 1$ as $\rho^m(x, y, z) = (x, y, z + m)$ and $\sum_{i=1}^{t} m \not\equiv 0 \pmod{k}$ as $\gcd(m, k) = 1$.

2. The orbits of H have length $k't$ for some $k'|k$. Suppose that $k' = 1$. If $|H| = t$ then $H = \langle \rho^{mk/t} \rangle \triangleleft G$, so $(\langle \rho^{mk/t} \rangle|_C)/\mathcal{B} \triangleleft (\mathrm{fix}_G(\mathcal{C})|_C)/\mathcal{B}$, forcing $(\mathrm{fix}_G(\mathcal{C})|_C)/\mathcal{B} \leq \mathrm{AGL}(1, t)$, which is solvable, a contradiction. So $|H| > t$. Now, the orbits of H form a nontrivial block system $\mathcal{D}$ of G (since $H \triangleleft G$), and since Condition (1) does not hold, there must be a nontrivial block system $\mathcal{D}'$ of G with

$\mathcal{D}' \prec \mathcal{D}$. But this is not possible since $(\mathrm{fix}_G(\mathcal{C})|_C)/\mathcal{B}$ is doubly transitive. This contradiction shows that we must have $k' \neq 1$. □

Lemma 26. *Under Hypothesis 23, suppose that $m > 1$ and Condition (1) does not hold, and let $\mathcal{C}$ be as in Lemma 24, and H as in Lemma 25. For each prime $p|k'$, there exists $h = h_p \in H$ such that $h(x, y, z) = (x, \sigma_x(y), z + b_{x,y})$ and for some $x^* \in \mathbb{Z}_{\frac{m}{t}}$ and some $y^* \in \mathbb{Z}_t$, $\sigma_{x^*}(y^*) = y^*$ and $b_{x^*,y^*} \equiv 1 \pmod p$. Furthermore, h satisfies the following additional properties:*

(1) $|h|$ is a power of p,
(2) $\sum_{y\in\mathcal{O}} b_{x,y} \equiv 0 \pmod p$ for every non-singleton orbit $\mathcal{O}$ of σ_x,
(3) $h|_{C_{x^*}}/\mathcal{B}$ has at least two fixed points,
(4) there is at least one $b_{x^*,\ell^*} \not\equiv 1 \pmod p$ and $\sigma_{x^*}(\ell^*) = \ell^*$, and
(5) h fixes some block of $\mathcal{B}$ contained in any block of $\mathcal{C}$.

Proof. Since the orbits of H have length $k't$ and H admits $\mathcal{B}$ as a complete block system, for any chosen block $B \in \mathcal{B}$, $\mathrm{Stab}_H(B)$, the set-wise stabilizer of the block B, is transitive on each orbit of $\langle \rho^{\frac{mk}{k'}} \rangle|_B$. Let $p|k'$ be prime. As $|B| = k$, for each block $B \in \mathcal{B}$ there exists $h \in H$ such that $h|_B$ is of order p, and so is cyclic and semiregular (semiregularity follows from the fact that ρ^m is in the center of G). That is, for every $x^* \in \mathbb{Z}_{\frac{m}{t}}$ and every $y^* \in \mathbb{Z}_t$ there exists $h \in H$ such that $h(x, y, z) = (x, \sigma_x(y), z + b_{x,y})$ with $\sigma_{x^*}(y^*) = y^*$ and $b_{x^*,y^*} \equiv 1 \pmod p$. This then implies that p divides $|h|$. By raising h to an appropriate power relatively prime to p, we may assume without loss of generality that h has order a power of p (so that (1) holds). Note then that $h/\mathcal{B} \neq 1$, as otherwise $1 \neq h \in \mathrm{fix}_G(\mathcal{B}) = \langle \rho^m \rangle$, but by Lemma 25, $\langle \rho^m \rangle \cap H = 1$. We may also assume that h is of minimal order while preserving the property that $\sigma_{x^*}(y^*) = y^*$ and $b_{x^*,y^*} \equiv 1 \pmod p$ for some $y^* \in \mathbb{Z}_{\frac{m}{t}}$ and $y^* \in \mathbb{Z}_t$. Fix these x^*, y^*, and h.

2) Choose any $x \in \mathbb{Z}_{\frac{m}{t}}$ and let $\mathcal{O}$ be a non-singleton orbit of σ_x. Let p^ℓ be the maximum length of the orbits of σ_x for all $x \in \mathbb{Z}_{\frac{m}{t}}$. If $\mathcal{O}$ is an orbit of σ_x of length p^ℓ, then $h^{p^\ell} \in \mathrm{fix}_H(\mathcal{B}) = \{1\}$. We conclude that for such orbits $\sum_{y\in\mathcal{O}} b_{x,y} \equiv 0 \pmod p$. If $\mathcal{O}$ is an orbit of σ_x of length $p^r < p^\ell$, then $h^{p^r}/\mathcal{B} \neq 1$. Now h^{p^r} acts as $h^{p^r}(x, y, z) = (x, \sigma_x^{p^r}(y), z + c_{x,y})$ for some $c_{x,y} \in \mathbb{Z}_k$. If $\sum_{y\in\mathcal{O}} b_{x,y} \not\equiv 0 \pmod p$, then for $y \in \mathcal{O}$, $\sigma_x^{p^r}(y) = y$ and $c_{x,y} \not\equiv 0 \pmod p$. Hence some power of h^{p^r} relatively prime to p has all the properties required of h but with smaller order, contradicting our choice of h. Thus $\sum_{y\in\mathcal{O}} b_{x,y} \equiv 0 \pmod p$ for every non-singleton orbit of σ_x.

3 - 5) As the order of h, and hence of each σ_x, is a power of p, $b_{x^*,y^*} \equiv 1 \pmod p$, and $\sum_{y=0}^{t-1} b_{x^*,y} \equiv 0 \pmod p$, (by Lemma 25), $h|_{C_{x^*}}/\mathcal{B}$ must have at least two fixed points. Furthermore, there is at least one $b_{x^*,\ell^*} \not\equiv 1 \pmod p$ and $\sigma_{x^*}(\ell^*) = \ell^*$, since $p \not| t$. Finally, observe that h must fix some block of $\mathcal{B}$ contained in any block of $\mathcal{C}$, again since $p \not| t$ and the length of any orbit of h

is a power of p. $\square$

Lemma 27. *Under Hypothesis 23, suppose that $m > 1$ and Conditions (1) and (2) do not hold, and let $\mathcal{C}$ be as in Lemma 24. Then there is a complete block system $\mathcal{F} \succ \mathcal{B}$ of G, consisting of t blocks of size $\frac{mk}{t}$, where each block is an orbit of $\langle \rho^{mk/t} \rangle$.*

Proof. By Lemma 24, we have that $(\mathrm{fix}_G(\mathcal{C})|_C)/\mathcal{B}$ is doubly transitive and nonsolvable for each $C \in \mathcal{C}$. Define H as in Lemma 25. By Lemma 25, $H \triangleleft G$, the orbits of H have order $k't$ for some $k'|k$, $k' \neq 1$, and $\langle \rho^m \rangle \cap H = 1$. By Lemma 26, for each $p|k'$ there exists $h = h_p \in H$ such that $h(x, y, z) = (x, \sigma_x(y), z + b_{x,y})$ and for some $x^* \in \mathbb{Z}_{\frac{m}{t}}$ and some $y^* \in \mathbb{Z}_t$, $\sigma_{x^*}(y^*) = y^*$ and $b_{x^*,y^*} \equiv 1 \pmod{p}$. Furthermore, h satisfies the following additional properties:

(1) $|h|$ is a power of p,
(2) $\sum_{y \in \mathcal{O}} b_{x,y} \equiv 0 \pmod{p}$ for every non-singleton orbit $\mathcal{O}$ of σ_x,
(3) $h|_{C_{x^*}}/\mathcal{B}$ has at least two fixed points,
(4) there is at least one $b_{x^*,\ell^*} \not\equiv 1 \pmod{p}$ and $\sigma_{x^*}(\ell^*) = \ell^*$, and
(5) h fixes some block of $\mathcal{B}$ contained in any block of $\mathcal{C}$.

For each $x \in \mathbb{Z}_{\frac{m}{t}}$ define a homomorphism $\pi_x : \mathrm{fix}_G(\mathcal{C}) \to \mathcal{S}_t$ by $\pi_x(g) = (g|_{C_x})/\mathcal{B}$. Define an equivalence relation $\equiv$ on $\mathcal{C}$ by $C_{x_1} \equiv C_{x_2}$ if and only if $\mathrm{Ker}(\pi_{x_1})/\mathcal{B} = \mathrm{Ker}(\pi_{x_2})/\mathcal{B}$. As in the proof of Lemma 13, it is not difficult to see that the unions of the equivalence classes of $\equiv$ form a complete block system $\mathcal{E}$ of G. Let $\mathcal{D}'$ be the complete block system of G formed by the orbits of $\langle \rho^{mk/p} \rangle$ (these orbits are blocks of G because of Lemma 15 and the fact that $\mathrm{fix}_G(\mathcal{B}) = \langle \rho^m \rangle$).

Let X be a circulant digraph with $G \leq \mathrm{Aut}(X)$, and let $G' \leq \mathrm{Aut}(X)$ be largest subgroup of $\mathrm{Aut}(X)$ that admits $\mathcal{B}$, $\mathcal{D}'$, and $\mathcal{E}$ as complete block systems. Note then that G' is 2-closed, as any block systems of a group are also block systems of its 2-closure. With the help of the automorphism h, we'll show that either the desired block system $\mathcal{F}$ exists, or $\rho^{mk/p}|_E \in G'$. The latter would imply that $\rho^{mk/p}|_E \in G^{(2)}$, contradicting the fact that Condition (2) does not hold.

First assume that there is more than one equivalence class of $\equiv$. Suppose there is an edge e between E and E_r, where $E, E_r \in \mathcal{E}$. Then there exists $C, C_r \in \mathcal{C}$ such that e is an edge between C and C_r. Then there exists $D', D'_r \in \mathcal{D}'$ such that e is an edge between D' and D'_r. We will show that every vertex of D' is adjacent to every vertex of D'_r. This will then imply that $\rho^{mk/p}|_E \in G'$ for every $E \in \mathcal{E}$ as required. Since $\langle \rho \rangle / \mathcal{E}$ is regular, we may without loss of generality, by replacing e with $\rho^a(e)$ for an appropriate a, assume that $D' \subseteq C_{x^*}$ (so that $C = C_{x^*}$).

Recall that σ_r has a fixed point, so that h fixes some block $B_{r,n} \in \mathcal{B}$. As $b_{x^*,y^*} \not\equiv b_{x^*,\ell^*} \pmod{p}$, h has a fixed block B_{x^*,n^*} such that $b_{x^*,n^*} \not\equiv b_{r,n} \pmod{p}$. By replacing e with $\rho^{bm/t}(e)$, for some appropriate b, we may also assume that $D' \subseteq B_{x^*,n^*}$. Note that as $\rho^{bm/t} \in \mathrm{fix}_G(\mathcal{C})$, we still have that $C = C_{x^*}$. As $C_{x^*} \not\equiv C_r$, we have that $(\mathrm{Ker}(\pi_{x^*})|_{C_r})/\mathcal{B} \neq \{1\}$. As $\mathrm{Ker}(\pi_{x^*}) \lhd \mathrm{fix}_G(\mathcal{C})$ and $(\mathrm{fix}_G(\mathcal{C})|_{C_r})/\mathcal{B}$ is primitive, we have that $(\mathrm{Ker}(\pi_{x^*})|_{C_r})/\mathcal{B}$ is transitive, since otherwise the orbits of $(\mathrm{Ker}(\pi_{x^*})|_{C_r})/\mathcal{B} \lhd (\mathrm{fix}_G(\mathcal{C})|_{C_r})/\mathcal{B}$ would form a complete block system of $(\mathrm{fix}_G(\mathcal{C})|_{C_r})/\mathcal{B}$. This implies that we may assume without loss of generality that $D'_r \subseteq B_{r,n}$. Now the action of h on this edge gives all possible edges between D' and D'_r as required.

It remains to consider the case when there is just one equivalence class of $\equiv$. Define an equivalence relation $\equiv'$ on $\mathcal{B}$ by $B \equiv' B'$ if and only if

$$\mathrm{Stab}_{\mathrm{fix}_G(\mathcal{C})/\mathcal{B}}(B) = \mathrm{Stab}_{\mathrm{fix}_G(\mathcal{C})/\mathcal{B}}(B'),$$

and let $\mathcal{F}$ be the collection of the unions of the equivalence classes of $\equiv'$. It is not difficult to see that $\mathcal{F}$ is a complete block system of G. As $(\mathrm{fix}_G(\mathcal{C})|_C)/\mathcal{B}$ is doubly transitive, each equivalence class of $\equiv'$ can contain at most one block of $\mathcal{B}|_C$ for each $C \in \mathcal{C}$. Thus the number of blocks of $\mathcal{B}$ in each equivalence class of $\equiv'$ is a divisor of $\frac{m}{t}$. As $\mathrm{Ker}(\pi_x)/\mathcal{B} = \mathrm{Ker}(\pi_{x'})/\mathcal{B}$ for all $x, x' \in \mathbb{Z}_{\frac{m}{t}}$, we have that $\pi_x(\mathrm{fix}_G(\mathcal{C})) = (\mathrm{fix}_G(\mathcal{C})|_{C_x})/\mathcal{B}$ is a faithful representation of $\mathrm{fix}_G(\mathcal{C})/\mathcal{B}$ for all $x \in \mathbb{Z}_{\frac{m}{t}}$. By Lemma 16, the representations $\pi_x(\mathrm{fix}_G(\mathcal{C}))$ and $\pi_{x'}(\mathrm{fix}_G(\mathcal{C}))$ are equivalent for all $x, x' \in \mathbb{Z}_{\frac{m}{t}}$. Thus each equivalence class of $\equiv'$ contains $\frac{m}{t}$ blocks of $\mathcal{B}$. Since $\mathcal{F}$ is a complete block system of G, and $\langle\rho\rangle \leq G$, the blocks of $\mathcal{F}$ must be the orbits of $\langle\rho^{mk/t}\rangle$. □

Lemma 28. *Under Hypothesis 23, suppose that $m > 1$ and Conditions (1) and (2) do not hold. Then for every prime $p|m$, there is a complete block system $\mathcal{C}$ that satisfies the following properties:*

(1) $\mathcal{C} \succ \mathcal{B}$;
(2) there is no complete block system $\mathcal{B}'$ for which $\mathcal{B} \prec \mathcal{B}' \prec \mathcal{C}$; and
(3) $\mathcal{C}$ consists of m/t blocks of size kt, where $p|t$.

Proof. Let $\mathcal{C}'$ be a complete block system of G consisting of $\frac{m}{r}$ blocks of size rk, that is minimal with respect to the property that $p|r$. That is, for any complete block system $\mathcal{B}'$ with $\mathcal{B} \prec \mathcal{B}' \prec \mathcal{C}'$, pk does not divide the size of the blocks of $\mathcal{B}'$. Such a $\mathcal{C}'$ certainly exists, since we could choose $r = m$.

If there is no complete block system $\mathcal{B}'$ for which $\mathcal{B} \prec \mathcal{B}' \prec \mathcal{C}'$, then we let $\mathcal{C} = \mathcal{C}'$ and we are done. So let $\mathcal{B}'$ be a complete block system whose block sizes are as small as possible while preserving the property that $\mathcal{B} \prec \mathcal{B}' \prec \mathcal{C}'$, and say that $\mathcal{B}'$ consists of $\frac{m}{t'}$ blocks of size kt', where $t' > 1$. Notice that $t'|r$. By our choice of $\mathcal{C}'$, we must have $p \not| t'$. By Lemma 27, with $\mathcal{B}'$ taking the

role of $\mathcal{C}$, there is a complete block system $\mathcal{F}$ of G consisting of t' blocks of size $\frac{mk}{t'}$.

Let $\mathcal{C}''$ be the complete block system of G whose blocks are all of the nonempty intersections of blocks of $\mathcal{F}$ with blocks of $\mathcal{C}'$. Since the nonempty intersections of any block of $\mathcal{F}$ with any block of $\mathcal{B}'$ consist of single blocks of $\mathcal{B}$, and since any block is an orbit of $\langle \rho^i \rangle$ for some i, the nonempty intersections of any block of $\mathcal{F}$ with any block of $\mathcal{C}'$ must each consist of precisely $\frac{r}{t'}$ blocks of $\mathcal{B}$. Hence $\mathcal{C}''$ consists of $t' \cdot \frac{m}{r}$ blocks of size $k \cdot \frac{r}{t'}$. But $t' > 1$ and $p|r$ but $p \not| t'$, so $p|\frac{r}{t'}$, contradicting our choice of $\mathcal{C}'$. □

Lemma 29. *Let k and m be integers such that mk is square-free. Let $G \leq \mathcal{S}_{mk}$ be a transitive permutation group that contains a regular cyclic subgroup $\langle \rho \rangle$ and admits a complete block system $\mathcal{B}$ with m blocks of size k. If $\mathrm{fix}_G(\mathcal{B})$ is of order k, $\mathrm{fix}_G(\mathcal{B}) \leq \mathrm{C}(G)$, and there exists no complete block system $\mathcal{F} \succ \mathcal{B}$ such that $\mathrm{fix}_G(\mathcal{F})$ is semiregular, then one of the following is true:*

(1) $m = 1$,
(2) there exists a complete block system $\mathcal{D}$ of G such that $\mathrm{fix}_G(\mathcal{D})$ is not of order $|D|$, $D \in \mathcal{D}$, and there exists no nontrivial complete block system $\mathcal{E}$ of G such that $\mathcal{E} \prec \mathcal{D}$, or
(3) there exists a prime $p|k$ such that $G^{(2)}$ admits a complete block system $\mathcal{D}'$ of n/p blocks of size p and p^2 divides $|\mathrm{fix}_{G^{(2)}}(\mathcal{D})|$.

Proof. By Lemma 28, we may assume that if $2|m$, then we can choose $\mathcal{C}$ with $\frac{m}{t}$ blocks of size kt as in Lemma 24, with $2|t$. Let $\mathcal{F}$ be a complete block system consisting of t blocks of size $\frac{mk}{t}$, as found in Lemma 27. Since $(\mathrm{fix}_G(\mathcal{C})|_C)/\mathcal{B}$ is doubly transitive (by Lemma 24) and $\mathcal{F}$ is a complete block system, we must have $\mathrm{Stab}_{\mathrm{fix}_G(\mathcal{C})/\mathcal{B}}(B) = \mathrm{Stab}_{\mathrm{fix}_G(\mathcal{C})/\mathcal{B}}(B')$ if and only if there is some $F \in \mathcal{F}$ for which $B, B' \subseteq F$.

Obtain h from Lemma 26. Since $h|_{C_{x^*}}$ has at least two fixed blocks, so must $h|_C$ for every $C \in \mathcal{C}$. Recall that $h(x, y, z) = (x, \sigma_x(y), z + b_{x,y})$. Since $\mathcal{F}$ is a complete block system, we must have $\sigma_x = \sigma_{x'}$ for every $x, x' \in \mathbb{Z}_{m/t}$; henceforth we will denote this by σ.

As in the proof of Lemma 27, let $\mathcal{D}'$ be the complete block system of G formed by the orbits of $\langle \rho^{mk/p} \rangle$, let X be a circulant digraph with $G \leq \mathrm{Aut}(X)$, and let $G' \leq \mathrm{Aut}(X)$ be the largest subgroup of $\mathrm{Aut}(X)$ that admits $\mathcal{B}$ and $\mathcal{D}'$ as complete block systems. Note again that G' is 2-closed.

Let $F_{x^*} \in \mathcal{F}$ be the block of $\mathcal{F}$ that contains B_{x^*,y^*}. We now show that either $\rho^{mk/p}|_{F_{x^*}} \in \mathrm{Aut}(X)$, which will then imply Condition (2) as before, or $\frac{m}{t}$ is even, a contradiction since $2|t$ and $4 \not| mk$.

Suppose that there is an edge e between a vertex of F_{x^*} and a vertex of F_r, where $F_r \in \mathcal{F}$ and $F_r \neq F_{x^*}$. Arguing as in Lemma 27, we have that there exists $D', D'_r \in \mathcal{D}'$, $C_r \in \mathcal{C}$ and $B_{r,z} \in \mathcal{B}$ such that $D' \subseteq B_{x^*,y^*} \subseteq F_{x^*}$, $D'_r \subseteq B_{r,z} \subseteq F_r$, $B_{r,z} \subseteq C_r$, and there is an edge e between some vertex of D' and some vertex of D'_r.

We show that every vertex of D' is adjacent to every vertex of D'_r, or that $\frac{m}{t}$ is even. Suppose there exists $u, v \in \mathbb{Z}_{m/t}$ such that $u \neq v$, $\sigma(u) = u$, $\sigma(v) = v$, and $b_{x^*,u} \not\equiv b_{r,v} \pmod{p}$. As $(\mathrm{fix}_G(\mathcal{C}))|_C/\mathcal{B}$ is doubly transitive for $C \in \mathcal{C}$, we may assume without loss of generality that $D' \subseteq B_{x^*,u}$ and $D'_r \subseteq B_{r,v}$. Now the action of h on the edge e gives all possible edges between D' and D'_r as required. Thus $\rho^{mk/p}|_F \in G'$ as required. We now assume that no such u and v exist.

Assume for the moment that $h|_C$ fixes at least three blocks of $\mathcal{B}$ set-wise. Recall that $\sigma(y^*) = y^*$ and $\sigma(\ell^*) = \ell^*$. As $h|_C$ fixes at least three blocks of $\mathcal{B}$ set-wise, there exists $n \in \mathbb{Z}_{m/t}$ such that $\sigma(n) = n$, $y^* \neq n \neq \ell^*$. As $b_{x^*,y^*} \not\equiv b_{x^*,\ell^*} \pmod{p}$, $b_{r,n}$ cannot be congruent modulo p to both. Thus appropriate u and v as above exist. We now assume that σ fixes exactly two blocks set-wise and that no appropriate u and v as above exist.

As $\sum_{y=0}^{t-1} b_{x,y} \equiv 0 \pmod{p}$, for every $x \in \mathbb{Z}_{m/t}$, $\sigma(y^*) = y^*$, $\sigma(\ell^*) = \ell^*$ and for every non-singleton orbit $\mathcal{O}$ of σ we have that $\sum_{y \in \mathcal{O}} b_{x,y} \equiv 0 \pmod{p}$, we must have that $b_{x,y^*} + b_{x,\ell^*} \equiv 0 \pmod{p}$ for every $x \in \mathbb{Z}_{m/t}$. Thus $b_{x^*,\ell^*} \equiv -1 \pmod{p}$, $b_{r,y^*} \equiv -1 \pmod{p}$, and $b_{r,\ell^*} \equiv 1 \pmod{p}$, as otherwise appropriate u and v as above exist. Let $q = r - y^*$. Similarly, $b_{r+q,y^*} \equiv 1 \pmod{p}$ and $b_{r+q,\ell^*} \equiv -1 \pmod{p}$ or we may conjugate h by an appropriate power of ρ to map r to x^* and $r+q$ to r, and again obtain appropriate u and v as above. Continuing inductively, we have that either appropriate u and v as above exist or $\frac{m}{t}$ is even, which as previously mentioned is a contradiction. □

4 Main Result

With the results of sections 2 and 3 established, we are approaching the main result of this paper. Two more major lemmas and several short technical results are required to complete the proof.

Lemma 30. *Let $G \leq \mathcal{S}_{mk}$ be 2-closed and contain a regular cyclic subgroup, $\langle \rho \rangle$. If G admits a nontrivial complete block system $\mathcal{B}$ consisting of m blocks of size k such that $\mathrm{fix}_G(\mathcal{B})|_B$ is primitive and $\mathrm{fix}_G(\mathcal{B})$ does not act faithfully on $B \in \mathcal{B}$, then $G = G_1 \cap G_2$, where $G_1 = \mathcal{S}_r \wr H_1$ and $G_2 = H_2 \wr \mathcal{S}_k$, H_1 is a 2-closed group of degree mk/r, H_2 is a 2-closed group of order m, and $r|m$.*

Proof. Define an equivalence relation $\equiv$ on $\mathcal{B}$ by $B \equiv B'$ if and only if the subgroups of $\mathrm{fix}_G(\mathcal{B})$ that fix B and B', point-wise respectively, are equal. Denote the equivalence classes of $\equiv$ by $C_0, \ldots, C_{r-1}$ and let $E_i = \cup_{B \in C_i} B$. By Lemma 13, $\mathrm{fix}_G(\mathcal{B})|_{E_i} \leq G$ for every $0 \leq i \leq r-1$ and $\mathcal{E} = \{E_i : 0 \leq i \leq r-1\}$ is a complete block system of G. As $\mathcal{E}$ is a complete block system of G and $\langle \rho \rangle \leq G$, $\mathcal{E}$ consists of all cosets of some subgroup $\langle rho^a \rangle$. Since $\mathrm{fix}_G(\mathcal{B})$ is not faithful, we have $r > 1$. We first show that every orbital digraph of G can be written as a nontrivial wreath product.

Let $\{\Gamma_\ell : \ell \in L\}$ be the set of all orbital digraphs of G. Let $e = (i, j)$ and Γ_ℓ the orbital digraph of G that contains the edge e. If $i, j \in E \in \mathcal{E}$, then, as $\mathcal{E}$ is a complete block system of G, we have that Γ_ℓ is disconnected. Then Γ_ℓ is trivially a wreath product and it is easy to see that $\mathrm{Aut}(\Gamma_\ell) \leq \mathcal{S}_{r_\ell} \wr \mathcal{S}_{mk/r_\ell}$, where $r | r_\ell$. If $i \in E$ and $j \in E'$, $E, E' \in \mathcal{E}$ and $E \neq E'$, then let $B, B' \in \mathcal{B}$ such that $i \in B$ and $j \in B'$. As $\mathrm{fix}_G(\mathcal{B})|_{E'} \in \mathrm{Aut}(\Gamma_\ell)$, we have that $(i, j') \in E(\Gamma_\ell)$ for every $j' \in B'$. As $\langle \rho \rangle \leq G$, we also have that $(i', j') \in E(\Gamma_\ell)$ for every $i' \in B$ and $j' \in B'$. Then $\Gamma_\ell = \Gamma'_\ell \wr \bar{K}_k$ for some Γ'_ℓ a circulant digraph of order m. Thus every orbital digraph of G can be written as a nontrivial wreath product as claimed.

Now, as G is 2-closed, $G = \cap_{\ell \in L} \mathrm{Aut}(\Gamma_\ell)$. Define a color digraph D whose underlying simple graph is K_n by $V(D) = \mathbb{Z}_n$ and each directed edge (i, j) is given color ℓ, where $(i, j) \in E(\Gamma_\ell)$. Note then that $\mathrm{Aut}(D) = G$. Let $J \subseteq L$ such that if $l \in J$, then Γ_l is a disconnected orbital digraph of G such that the vertex set of every component of Γ_l is contained in some $E \in \mathcal{E}$. Let D_1 be the spanning sub-digraph of D consisting of all edges of D colored with a color contained in J. Then D_1 has r components, so that $\mathrm{Aut}(D_1) = \mathcal{S}_r \wr H_1$, where H_1 is permutation isomorphic to $\mathrm{Aut}(D_1[E])$, for $E \in \mathcal{E}$. Thus H_1 is 2-closed of degree mk/r as H_1 is the automorphism group of a color-digraph. Let D_2 be the spanning sub-digraph of D given by $E(D_2) = E(D) - E(D_1)$. As for each $\ell \in L - J$, we have established that $\Gamma_\ell = \Gamma'_l \wr \bar{K}_k$, we have that $D_2 = D'_2 \wr \bar{K}_k$, where $D'_2 = D_2/\mathcal{B}$. Let $K \leq \mathrm{Aut}(D_2)$ be the maximal subgroup of $\mathrm{Aut}(D_2)$ that admits $\mathcal{E}$ as a complete block system. Then $K = \mathrm{Aut}(D'_2) \wr S_k$ and $\mathrm{Aut}(D_2) \cap \mathrm{Aut}(D_1) = K \cap \mathrm{Aut}(D_1)$ as $\mathrm{Aut}(D_1)$ admits $\mathcal{E}$ as a complete block system. We let $H_2 = \mathrm{Aut}(D'_2)$. Let $g \in G$. As G admits $\mathcal{B}$ and $\mathcal{E}$ as complete block systems, $g \in \mathrm{Aut}(D_1)$ and $g \in \mathrm{Aut}(D_2)$. Conversely, if $g \in \mathrm{Aut}(D_1) \cap \mathrm{Aut}(D_2)$, then $g(e) \in E(D)$ for every $e \in E(D_1)$ and $g(e) \in E(D_2)$ for every $e \in E(D_2)$. As $E(D_1) \cup E(D_2) = E(D)$, $g \in \mathrm{Aut}(D)$. Thus $G = \mathrm{Aut}(D) = (\mathcal{S}_r \wr H_1) \cap (H_2 \wr \mathcal{S}_k)$. Finally, as $\mathcal{B} \preceq \mathcal{E}$, we have that $r | m$. $\square$

Lemma 31. *Let $G \leq \mathcal{S}_{mk}$ be 2-closed and contain a regular cyclic subgroup $\langle \rho \rangle$. Let $\mathcal{B}$ be a nontrivial complete block system of G with m blocks of size k with the property that there exists no nontrivial complete block system $\mathcal{C}$ of G such that $\mathcal{C} \prec \mathcal{B}$. If $|\mathrm{fix}_G(\mathcal{B})| > k$, then one of the following is true:*

(1) $G = G_1 \cap G_2$, *where* $G_1 = \mathcal{S}_r \wr H_1$ *and* $G_2 = H_2 \wr \mathcal{S}_k$, *where* H_1 *is a* 2*-closed group of degree* mk/r, H_2 *is a* 2*-closed group of order* m, *and* $r|m$; *or*

(2) there exists a complete block system $\mathcal{B}$ *of* G *consisting of* k *blocks of size* m, *and there exists* $H \triangleleft G$ *such that* H *is transitive,* 2*-closed, and* $\langle \rho \rangle \leq H = H_1 \times H_2$ *(with the canonical action), where* $H_1 \leq \mathcal{S}_m$ *is* 2*-closed and* $H_2 \leq \mathcal{S}_k$ *is* 2*-closed and primitive.*

Proof. As there exists no nontrivial complete block system $\mathcal{C}$ of G such that $\mathcal{C} \prec \mathcal{B}$, it follows by Lemma 15 that $\mathrm{fix}_G(\mathcal{B})|_B$ is primitive. If $\mathrm{fix}_G(\mathcal{B})$ does not act faithfully on $B \in \mathcal{B}$, then by Lemma 30 1) holds. We thus assume that $\mathrm{fix}_G(\mathcal{B})$ acts faithfully on each $B \in \mathcal{B}$. Define an equivalence relation $\equiv'$ on $\mathbb{Z}_{mk}$ by $i \equiv' j$ if and only if $\mathrm{Stab}_{\mathrm{fix}_G(\mathcal{B})}(i) = \mathrm{Stab}_{\mathrm{fix}_G(\mathcal{B})}(j)$.

We demonstrate that $\mathrm{fix}_G(\mathcal{B})|_B$ is equivalent to $\mathrm{fix}_G(\mathcal{B})|_{B'}$ for every $B, B' \in \mathcal{B}$. First, if $\mathrm{fix}_G(\mathcal{B})|_B$ is doubly transitive and nonsolvable for every $B \in \mathcal{B}$, Lemma 16 tells us that $\mathrm{fix}_G(\mathcal{B})|_B$ is equivalent to $\mathrm{fix}_G(\mathcal{B})|_{B'}$ for every $B, B' \in \mathcal{B}$. If k were composite, then by the same argument used in the first paragraph of the proof of Lemma 24, since $\mathrm{fix}_G(\mathcal{B})|_B$ is primitive, $\mathrm{fix}_G(\mathcal{B})|_B$ must be doubly transitive, and since $k \neq 4$ $\mathrm{fix}_G(\mathcal{B})|_B$ must be nonsolvable, and therefore the actions are equivalent by the argument of the previous sentence. The remaining possibility is that $\mathrm{fix}_G(\mathcal{B})|_B$ is not doubly transitive or is solvable, and $k = p$ is prime. By Burnside's Theorem (Theorem 10), $\mathrm{fix}_G(\mathcal{B})|_B$ is doubly transitive if $\mathrm{fix}_G(\mathcal{B})|_B$ is nonsolvable. We conclude that $\mathrm{fix}_G(\mathcal{B})|_B$ is solvable for every $B \in \mathcal{B}$, so that $\mathrm{fix}_G(\mathcal{B})|_B \leq \mathrm{AGL}(1, p)$. Let $|\mathrm{fix}_G(\mathcal{B})|_B| = pr$, $r|(p-1)$. Conjugating $\mathrm{Stab}_{\mathrm{fix}_G(\mathcal{B})}(i)$ by any element of $\mathrm{fix}_G(\mathcal{B})$ gives $\mathrm{Stab}_{\mathrm{fix}_G(\mathcal{B})}(i')$ for some i' for which $i, i' \in B \in \mathcal{B}$, so if we can show that $\mathrm{Stab}_{\mathrm{fix}_G(\mathcal{B})}(i)$ and $\mathrm{Stab}_{\mathrm{fix}_G(\mathcal{B})}(j)$ are conjugate in $\mathrm{fix}_G(\mathcal{B})$ whenever i and j are in different blocks of $\mathcal{B}$, we will have shown that the actions are equivalent, as desired. Since $\mathrm{AGL}(1, p)$ and hence $\mathrm{fix}_G(\mathcal{B})$ is solvable, $\mathrm{Stab}_{\mathrm{fix}_G(\mathcal{B})}(i)$ is in some Hall subgroup of $\mathrm{fix}_G(\mathcal{B})$ that is conjugate in $\mathrm{fix}_G(\mathcal{B})$ to the Hall subgroup that contains $\mathrm{Stab}_{\mathrm{fix}_G(\mathcal{B})}(j)$. Since $\mathrm{AGL}(1, p)/P$ is cyclic, where P is the Sylow p-subgroup of $\mathrm{AGL}(1, p)$, it contains a unique subgroup of order r. This shows that, in fact, $\mathrm{Stab}_{\mathrm{fix}_G(\mathcal{B})}(i)$ and $\mathrm{Stab}_{\mathrm{fix}_G(\mathcal{B})}(j)$ are conjugate in $\mathrm{fix}_G(\mathcal{B})$. We conclude that the actions of $\mathrm{fix}_G(\mathcal{B})|_B$ and $\mathrm{fix}_G(\mathcal{B})|_{B'}$ are equivalent for every $B, B' \in \mathcal{B}$.

It now follows that each equivalence class of $\equiv'$ contains at least m elements. Furthermore, since the intersections of equivalence classes of $\equiv'$ with blocks of $\mathcal{B}$ are blocks of G, and there is no nontrivial complete block system $\mathcal{C}$ of G with $\mathcal{C} \prec \mathcal{B}$, these intersections must be trivial blocks. That is, each block of $\mathcal{B}$ contains exactly one element of each equivalence class of $\equiv'$. As conjugation by an element of G permutes the stabilizers of points in $\mathbb{Z}_{mk}$, we have that the equivalence classes of $\equiv'$ form a complete block system $\mathcal{B}'$ of k blocks of size m. As $\langle \rho \rangle \leq G$, $\mathcal{B}'$ must be formed by the orbits of $\langle \rho^k \rangle$. Then $\mathrm{fix}_G(\mathcal{B}) \triangleleft G$, $\mathrm{fix}_G(\mathcal{B}') \triangleleft G$, and $\mathrm{fix}_G(\mathcal{B}) \cap \mathrm{fix}_G(\mathcal{B}') = 1$. Let H be the internal direct product of $H_1 = \mathrm{fix}_G(\mathcal{B}')$ and $H_2 = \mathrm{fix}_G(\mathcal{B})$ (so that $H \cong \mathrm{fix}_G(\mathcal{B}') \times \mathrm{fix}_G(\mathcal{B})$). Then

$H \triangleleft G$. Since $(m,k)=1$, $\rho^m \in \mathrm{fix}_G(\mathcal{B})$ and $\rho^k \in \mathrm{fix}_G(\mathcal{B}')$, we also have $\langle \rho \rangle \leq H$.

Now, consider $H^{(2)}$. By Lemma 14, $H^{(2)} = \mathrm{fix}_G(\mathcal{B}')^{(2)} \times \mathrm{fix}_G(\mathcal{B})^{(2)}$. As $H \leq G$, $H^{(2)} \leq G$. Hence $\mathrm{fix}_{H^{(2)}}(\mathcal{B}) \leq \mathrm{fix}_G(\mathcal{B})$ and $\mathrm{fix}_{H^{(2)}}(\mathcal{B}') \leq \mathrm{fix}_G(\mathcal{B}')$. As $H^{(2)} = \mathrm{fix}_G(\mathcal{B}')^{(2)} \times \mathrm{fix}_G(\mathcal{B})^{(2)}$, $\mathrm{fix}_{H^{(2)}}(\mathcal{B}') = \mathrm{fix}_G(\mathcal{B}')^{(2)}$ and $\mathrm{fix}_{H^{(2)}}(\mathcal{B}) = \mathrm{fix}_G(\mathcal{B})^{(2)}$. Thus $\mathrm{fix}_G(\mathcal{B}) = \mathrm{fix}_{H^{(2)}}(\mathcal{B}) \leq \mathrm{fix}_G(\mathcal{B})^{(2)}$ so that $\mathrm{fix}_G(\mathcal{B})$ is 2-closed. Similarly, $\mathrm{fix}_G(\mathcal{B}')$ is 2-closed. Hence

$$H^{(2)} = \mathrm{fix}_G(\mathcal{B}')^{(2)} \times \mathrm{fix}_G(\mathcal{B})^{(2)} = \mathrm{fix}_G(\mathcal{B}) \times \mathrm{fix}_G(\mathcal{B}') = H.$$

Then 2) follows with the observation that as $\mathrm{fix}_G(\mathcal{B})|_B$ is primitive for every $B \in \mathcal{B}$, we have that H_2 is primitive in its action on $B \in \mathcal{B}$. □

We now only need technical lemmas before the proof of the main theorem.

Lemma 32. *Let $H \triangleleft G$ such that H contains a regular cyclic subgroup. If $\mathcal{B}$ is a complete block system of H, then $\mathcal{B}$ is a complete block system of G.*

Proof. Clearly $\mathrm{fix}_H(\mathcal{B}) \triangleleft H$. Furthermore, if $g \in G$, then $g^{-1}\mathrm{fix}_H(\mathcal{B})g \triangleleft H$. As H contains a regular cyclic subgroup, the complete block system $\mathcal{B}$ is the unique complete block system of H with blocks of size $|B|$, $B \in \mathcal{B}$. As $g^{-1}\mathrm{fix}_H(\mathcal{B})g \triangleleft H$ and has orbits of the same size as $B \in \mathcal{B}$, the orbits of $g^{-1}\mathrm{fix}_H(\mathcal{B})g$ are the same as those of $\mathrm{fix}_H(\mathcal{B})$. Hence $g^{-1}\mathrm{fix}_H(\mathcal{B})g = \mathrm{fix}_H(\mathcal{B})$, so that $\mathrm{fix}_H(\mathcal{B}) \triangleleft G$. Thus the orbits of $\mathrm{fix}_H(\mathcal{B})$ form the complete block system $\mathcal{B}$ of G. □

Definition 33. For a positive integer n, we define $N(n) = \{x \to ax + b : a \in \mathbb{Z}_n^*, b \in \mathbb{Z}_n\}$. Note that $N(n)$ is the normalizer of the left regular representation of $\mathbb{Z}_n$, and if n is prime, then $N(n) = \mathrm{AGL}(1,n)$. We let $\langle \rho \rangle$ be the cyclic subgroup of $N(n)$ defined by $\rho(x) = x + 1$.

Lemma 34. *Let $H \leq N(mk)$, mk square-free and suppose that H is transitive. If $\mathcal{B}$ is a complete block system of H consisting of m blocks of size k, then $\langle \rho^m \rangle$ is the unique minimal subgroup of $\mathrm{fix}_H(\mathcal{B})$ whose action on any block of $B \in \mathcal{B}$ is transitive.*

Proof. Let $k = p_1 \cdots p_r$, where each p_i is prime. Note that $\langle \rho \rangle$ contains a unique Sylow p_i-subgroup of order p_i, $1 \leq i \leq r$. Hence for each i, $N(mk)$ (and thus H) admits a complete block system $\mathcal{C}_i \preceq \mathcal{B}$ consisting of mk/p_i blocks of size p_i formed by the orbits of $\langle \rho^{mk/p_i} \rangle$. We may thus view $N(mk)$ (and so H) as acting on $\mathbb{Z}_m \times \Pi_{i=1}^r \mathbb{Z}_{p_i}$ in the canonical fashion by viewing $N(mk)$ as $N(m) \times \Pi_{i=1}^r \mathrm{AGL}(1,p)$. Let $K \leq \mathrm{fix}_H(\mathcal{B})$ be such that $K|_B$ is transitive on some $B \in \mathcal{B}$ and K has no proper subgroup K' such that $K'|_B$ is transitive on some block of $B \in \mathcal{B}$. Then for any $b \in \mathcal{B}$, $K|_B$ is transitive on B. Define $\pi_i : K \to \mathrm{AGL}(1,p_i)$ to be projection onto the $(i+1)^{st}$-coordinate (viewing $K \leq N(m) \times \Pi_{i=1}^r \mathrm{AGL}(1,p_i)$). Then $\pi_i(K)$ is transitive for every

$1 \leq i \leq r$. Furthermore, as $\mathrm{AGL}(1, p_i)$ contains a unique transitive subgroup (namely, its unique Sylow p_i-subgroup), $\pi_i(K)$ must contain the unique Sylow p_i-subgroup of $\mathrm{AGL}(1, p_i)$. Now, observe that $\pi_i(\langle \rho^m \rangle)$ is also the unique Sylow p_i-subgroup of $\mathrm{AGL}(1, p_i)$ so that $\pi_i(\langle \rho^m \rangle) \leq \pi_i(K)$. Suppose that $K \neq \langle \rho^m \rangle$. Then there exists $\delta \in K$ such that $\delta \notin \langle \rho^m \rangle$, and hence for some $1 \leq i \leq r$, $\pi_i(\delta) \notin \pi_i(\langle \rho^m \rangle)$. Let P_i be the unique Sylow p_i-subgroup of $\mathrm{AGL}(1, p_i)$. Then $\pi_i^{-1}(P_i)|_B$ is transitive, but $\delta \notin \pi_i^{-1}(P_i)$, a contradiction. □

Lemma 35. *Let mk be a square-free integer, and let $G \leq S_{mk}$ contain a regular cyclic subgroup $\langle \rho \rangle \leq G$ and admit a complete block system $\mathcal{B}$ of m blocks of size k such that $\mathrm{fix}_G(\mathcal{B}) \leq N(mk)$. Then there exists $H \triangleleft G$ such that*

(1) $\langle \rho \rangle \leq H$,
(2) $\mathrm{fix}_H(\mathcal{B})$ is semiregular, and
(3) $\mathrm{fix}_H(\mathcal{B}) \leq \mathrm{C}(H)$.

Proof. For convenience, we will view G as acting on $\mathbb{Z}_m \times \mathbb{Z}_k$ so that $\rho(i, j) = (i + 1, j + 1)$, and the blocks of $\mathcal{B}$ are the sets $\{i\} \times \mathbb{Z}_k$, where $i \in \mathbb{Z}_m$. Then $\langle \rho^m \rangle \leq \mathrm{fix}_G(\mathcal{B})$, and by Lemma 34, $\langle \rho^m \rangle$ is the unique minimal subgroup of $\mathrm{fix}_G(\mathcal{B})$ whose action on some block of $\mathcal{B}$ is transitive. We then have that if $g \in G$, then $g^{-1}\langle \rho^m \rangle g = \langle \rho^m \rangle$ as $g^{-1}\langle \rho^m \rangle g$ is transitive on some block of $B \in \mathcal{B}$. Whence if $g \in G$, then $g(i, j) = (\delta(i), \beta_i(j))$, where $\delta \in \mathcal{S}_n$ and $\beta_i \in N(k)$. Thus $\beta_i(j) = \alpha_i j + b_i$, where $\alpha_i \in \mathbb{Z}_k^*$, $b_i \in \mathbb{Z}_k$. As $\langle \rho^m \rangle \triangleleft G$, $\alpha_i = \alpha_{i'}$ for every $i, i' \in \mathbb{Z}_m$. Thus $g(i, j) = (\delta(i), \alpha j + b_i)$. Let $H = \langle \rho \rangle^G = \{g^{-1}\rho^\ell g : g \in G, \ell \in \mathbb{Z}_{mk}\}$, the normal closure of $\langle \rho \rangle$ in G. As every $g \in G$ has the form $g(i, j) = (\delta(i), \alpha j + b_i)$, a straightforward computation will show that if $h \in H$, then $h(i, j) = (\gamma(i), j + c_i)$, $\gamma \in \mathcal{S}_m$, $c_i \in \mathbb{Z}_k$. Clearly $\rho \in H$ so that 1) follows. Furthermore, elements of $\langle \rho^m \rangle$ are the only elements of $\mathrm{fix}_G(\mathcal{B})$ of the form $(i, j) \to (\gamma(i), j + b_i)$, so that $\mathrm{fix}_H(\mathcal{B}) = \langle \rho^m \rangle$ and 2) follows. As $\rho^m(i, j) = (i, j + c)$, for some $c \in \mathbb{Z}_k$, it is now easy to see that ρ^m commutes with every element of H so that $\langle \rho^m \rangle \leq \mathrm{C}(H)$ and 3) follows. □

Lemma 36. *Let $G \leq S_{mk}$, mk square-free with $H \triangleleft G$ such that $\langle \rho \rangle \leq H$ is a regular cyclic subgroup. Assume that H admits a complete block system $\mathcal{B}$ of m blocks of size k. If $\mathrm{fix}_H(\mathcal{B}) \leq N(mk)$, then $\mathrm{fix}_G(\mathcal{B}) \leq N(mk)$.*

Proof. By Lemma 32, $\mathcal{B}$ is also a complete block system of G. Let $g \in \mathrm{fix}_G(\mathcal{B})$. Then $g^{-1}\rho g\rho^{-1}/\mathcal{B} = 1$ so that $g^{-1}\rho g\rho^{-1} \in \mathrm{fix}_G(\mathcal{B})$. Furthermore, $\rho \in H$ so that $g^{-1}\rho g \in H$. Whence $g^{-1}\rho g\rho^{-1} \in \mathrm{fix}_H(\mathcal{B}) \leq N(mk)$. As $\rho^{-1} \in N(mk)$, we have that $g^{-1}\rho g \in N(mk)$ and $\langle g^{-1}\rho g \rangle$ is transitive. By Lemma 34, we have that $g^{-1}\rho g \in \langle \rho \rangle$ so that $g \in N(mk)$ as required. □

Theorem 37. *Let mk be a square-free integer and $G \leq \mathcal{S}_{mk}$ be 2-closed and contain a regular cyclic subgroup, $\langle \rho \rangle$. Then one of the following is true:*

(1) $G = G_1 \cap G_2$, *where* $G_1 = \mathcal{S}_r \wr H_1$ *and* $G_2 = H_2 \wr \mathcal{S}_k$, *where* H_1 *is a* 2*-closed group of degree* mk/r, H_2 *is a* 2*-closed group of order* m, *and* $r|m$; *or*

(2) there exists a complete block system $\mathcal{B}$ *of* G *consisting of* m *blocks of size* k, *and there exists* $H \triangleleft G$ *such that* H *is transitive,* 2*-closed, and* $\langle \rho \rangle \leq H = H_1 \times H_2$ *(with the canonical action), where* $H_1 \leq \mathcal{S}_m$ *is* 2*-closed and* $H_2 \leq \mathcal{S}_k$ *is* 2*-closed and primitive.*

Proof. Choose k as large as possible so that there exists $H \triangleleft G$ such that $\langle \rho \rangle \leq H$, $\mathrm{fix}_H(\mathcal{B})$ is semiregular of order k, where $\mathcal{B}$ is a complete block system consisting of m blocks of size k, and $\langle \rho^m \rangle \leq \mathrm{C}(H)$. Suppose that there exists a complete block system $\mathcal{C}$ with $\mathcal{B} \prec \mathcal{C}$ and $H' \triangleleft H$ such that $\langle \rho \rangle \leq H'$ and $\mathrm{fix}_{H'}(\mathcal{C})$ is semiregular of order, say k', where $k|k'$. Note then that $\mathrm{fix}_{H'}(\mathcal{C}) = \langle \rho^{mk/k'} \rangle \leq N(mk)$. By Lemma 36, $\mathrm{fix}_H(\mathcal{C}) \leq N(mk)$, and again by Lemma 36, $\mathrm{fix}_G(\mathcal{C}) \leq N(mk)$. But then by Lemma 35 there exists $H'' \triangleleft G$ such that $\langle \rho \rangle \leq H''$, $\mathrm{fix}_{H''}(\mathcal{C})$ is semiregular, and $\mathrm{fix}_{H''}(\mathcal{C}) = \langle \rho^{mk/k'} \rangle \leq \mathrm{C}(H'')$, contradicting our original choice of k. Hence if $\mathcal{C} \succ \mathcal{B}$ and $H' \triangleleft H$ with $\langle \rho \rangle \leq H'$, then $\mathrm{fix}_{H'}(\mathcal{C})$ is not semiregular.

We have now established the conditions of Lemma 29 for the group H, which allows us to conclude one of the following:

(1) $m = 1$;
(2) there exists a complete block system $\mathcal{D}$ of H such that $\mathrm{fix}_H(\mathcal{D})$ is not of order $|D|$, $D \in \mathcal{D}$, and there exists no nontrivial block system $\mathcal{E}$ of H such that $\mathcal{E} \prec \mathcal{D}$; or
(3) there exists a prime $q|k$ such that $H^{(2)}$ admits a complete block system $\mathcal{D}'$ of mk/q blocks of size q and q^2 divides $|\mathrm{fix}_{H^{(2)}}(\mathcal{D}')|$.

In the first case, we have just one trivial block, so $\mathrm{fix}_G(\mathcal{B}) = G = \langle \rho \rangle$ and conclusion 2) of this theorem is true (possibly vacuously if $mk = k$ is prime).

In the second case, by Lemma 32, $\mathcal{D}$ is a complete block system of G. Since H has no nontrivial complete block system $\mathcal{E}$ such that $\mathcal{E} \prec \mathcal{D}$ and every complete block system of G is also a complete block system of H, G has no nontrivial complete block system $\mathcal{E}$ such that $\mathcal{E} \prec \mathcal{D}$. Thus $|\mathrm{fix}_G(\mathcal{D})| > |D|$, $D \in \mathcal{D}$. Now by Lemma 31, one of the conclusions of this theorem holds.

In the third case, since G is 2-closed and $H \leq G$, we have $H^{(2)} \leq G$, so q^2 divides $|\mathrm{fix}_G(\mathcal{D}')|$. Since $\mathrm{fix}_H(\mathcal{D}') \leq \mathrm{fix}_H(\mathcal{B}) = \langle \rho^m \rangle \leq N(mk)$, Lemma 36 gives $\mathrm{fix}_G(\mathcal{D}') \leq N(mk)$, a contradiction. □

This is the main result that was described in the abstract. As mentioned in our introductory remarks, we can determine more precisely which groups satisfy (2) of Theorem 37.

For a positive integer n, let $M(n) = \{x \to ax : a \in \mathbb{Z}_n^*\}$.

Corollary 38. *Let G be a 2-closed group of square-free degree mk that contains a regular cyclic subgroup $\langle\rho\rangle$, such that there exists $H \triangleleft G$ such that H is transitive, 2-closed, and there exists a complete block system $\mathcal{B}$ of G consisting of m blocks of size k, such that $H = H_1 \times H_2$ (with the canonical action), where $H_1 \leq \mathcal{S}_m$ is 2-closed and $H_2 \leq \mathcal{S}_k$ is 2-closed and primitive. Then there exists $A \leq M(mk)$ such that $G = A \cdot H$.*

Proof. We must show that $g = rh$, where $h \in H$ and $r \in M$. As $\mathbb{Z}_{mk}$ is a CI-group with respect to binary relational structures [21] and $\langle\rho\rangle = (\mathbb{Z}_{mk})_L \leq H$, there exists $h_1 \in H$ such that $h_1^{-1}g^{-1}\langle\rho\rangle g h_1 = \langle\rho\rangle$. Thus $gh_1 = \omega \in N(mk)$. Let $\omega(i) = ai+b$, $a \in \mathbb{Z}_{mk}^*$, $b \in \mathbb{Z}_{mk}$. Define $h_2 : \mathbb{Z}_{mk} \to \mathbb{Z}_{mk}$ by $h_2(i) = i - a^{-1}b$. Then $gh_1h_2(i) = ai$, where $a \in \mathbb{Z}_{mk}^*$. Let $r \in M(n)$ such that $r(i) = ai$. Then $gh_1h_2 = r$ so that $g = rh_2^{-1}h_1^{-1}$, and the result follows. □

References

[1] Alspach, B., Point-symmetric graphs and digraphs of prime order and transitive permutation groups of prime degree, *J. Combin. Theory* **15** 1973, 12–17.

[2] Berggren, J. L., An algebraic characterization of symmetric graphs with p points, p an odd prime, *Bull. Austral. Math. Soc.* **7** 1972, 131-134.

[3] Bollobás, B., *Graph Theory*, Springer-Verlag New York, 1979.

[4] Burnside, W., On some properties of groups of odd order, *J. London Math. Soc.* 33 (1901) 162–185.

[5] Cameron, P.J.,Finite Permutation groups and finite simple groups, *Bull. London Math. Soc.* **13** 1981, 1-22.

[6] Conway, J. H., Curtis, R. T., Norton, S. P., Parker, R. A., and Wilson. R. A., *Atlas of Finite Groups*, Oxford University Press, New York, 1985.

[7] Conway, J. H., Curtis, R. T., Norton, S. P., Parker, R. A., and Wilson. R. A., *Atlas of Finite Groups*, web version,

http://web.mat.bham.ac.uk/atlas/html/L211.html.

[8] Dixon, J.D., and Mortimer, B., *Permutation Groups*, Springer-Verlag New York, Berlin, Heidelberg, Graduate Texts in Mathematics, **163**, 1996.

[9] Dobson, E., Isomorphism problem for Cayley graphs of $\mathbb{Z}_p^3$, *Discrete Math.* **147** 1995, 87-94.

[10] Dobson, E., and Witte, D., Transitive permutation groups of prime-squared degree, submitted.

[11] Elspas, B., and Turner, J., Graphs with circulant adjacency matrices, *J. Comb. Theory Ser. B* **9** 1970, 297-307.

[12] Frucht, R., Herstellung von Graphen mit vorgegebener abstrakter Gruppe, *Composito Math.*, **6** (1938), 239-250.

[13] Gorenstein, D., *Finite Groups*, Chelsea Publishing Co., New York, 1968.

[14] Gorenstein, D., *Finite Simple Groups*, Plenum Press, New York, London, University Series in Mathematics, 1982.

[15] Hall, M., *The Theory of Groups*, Chelsea Publishing Co., New York, 1976.

[16] Huppert, B., *Endliche Gruppen I*, Springer, Berlin, 1967.

[17] Kalužnin, L. A., and Klin, M. H., On some numerical invariants of permutation groups, *Latv. Math. Ežegodnik*, **18** (1976), 81-99, (in Russian).

[18] Klin, M. H., and Pöschel, R., The König problem, the isomorphism problem for cyclic graphs and the method of Schur, Proceedings of the Inter. Coll. on Algebraic methods in graph theory, Szeged 1978, *Coll. Mat. Soc. János Bolyai* **27**.

[19] Klin, M. Ch., and Pöschel, R., The isomorphism problem for circulant graphs with p^n vertices, Preprint P-34/80 ZIMM, Berlin 1980.

[20] Meldrum, J. D. P., *Wreath Products of Groups and Semigroups*, Pitman Monographs and Surveys in Pure and Applied Mathematics, **74**, Longman, Harlow, 1995.

[21] Muzychuk, M., Ádám's conjecture is true in the square-free case, *J. Comb. Theory Ser. A* **72** 1995, 118-134.

[22] Dobson, E., and Morris, J., A polynomial time algorithm to compute the full automorphism group of a circulant graph of square-free order, in preparation.

[23] Sabidussi, G., The composition of graphs, *Duke Math J.* **26** (1959), 693-696.

[24] Scott, W.R., *Group Theory*, Dover Press, New York, 1987.

[25] H. Wielandt, *Finite Permutation Groups*, Academic Press, New York, 1964.

[26] Wielandt, H., Permutation groups through invariant relations and invariant functions, lectures given at The Ohio State University, Columbus, Ohio, 1969.

[27] Wielandt, H., Mathematische Werke/Mathematical works. Vol. 1. Group theory, edited and with a preface by Bertram Huppert and Hans Schneider, Walter de Gruyter & Co., Berlin, 1994.