On automorphism groups of circulant digraphs of square-free order

Edward Dobson\textsuperscript{a}, Joy Morris\textsuperscript{b, 1}

\textsuperscript{a}Department of Mathematics and Statistics, Mississippi State University, PO Drawer MA Mississippi State, MS 39762, USA

\textsuperscript{b}Department of Mathematics and Computer Science, University of Lethbridge, Lethbridge, Canada, AB. T1K 3M4

Received 2 September 2003; received in revised form 14 March 2004; accepted 22 March 2004

Available online 27 July 2005

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.

© 2005 Elsevier B.V. All rights reserved.

Keywords: Automorphisms; Automorphism group; Circulant graphs; Cayley graphs; Graphs; Directed graphs

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 \cite{14}, 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 \cite{13}, 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

\textsuperscript{1}This author gratefully acknowledges support from NSERC grant # 40188.

E-mail addresses: dobson@math.msstate.edu (E. Dobson), joy@cs.uleth.ca (J. Morris).

0012-365X/ - see front matter © 2005 Elsevier B.V. All rights reserved.
doi:10.1016/j.disc.2004.03.018
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 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 [11] 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 [3] and [1], prime-squared order [20] (see [12] for another proof of this result), odd prime power order [21], and of a product of two distinct primes [20] have been obtained, and all of these results lead to polynomial time algorithms.

As was pointed out by an anonymous referee, it may be possible to prove our main result using the classification of Schur rings over cyclic groups obtained by Leung and Ma [22], or the refinement obtained by Muzychuk [25] for cyclic groups of square-free order. This would be a completely different approach to the problem, and would be of value in its own right.

The proofs of these results are presented in the four sections that follow. Section 1 includes preliminaries: primarily results from other sources that are used in this paper, and definitions. Section 2 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 17, showing that faithful doubly-transitive nonsolvable actions on blocks must be equivalent. In Section 3, 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 [9], and for graph theory terminology, see [4].

**Definition 1.** For any set \( \Omega \), we will use \( \mathcal{S}_\Omega \) to denote the symmetric group acting on the elements of the set \( \Omega \), and \( \mathcal{A}_\Omega \) will denote the alternating group on this set. We will also use \( \mathcal{S}_n \) and \( \mathcal{A}_n \) to denote the symmetric and alternating groups (respectively) on an arbitrary set of cardinality \( n \).

**Definition 2.** 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 \( E(\Gamma) = \{(i, j) : i - j \in S\} \). If \( S = -S \), then \( \Gamma(\mathbb{Z}_n, S) \) is a circulant graph.
We observe that \( G/\mathbb{O} \) product of a circulant digraph of order \( n \) is contained in \( \text{Aut}(\Gamma) \), the automorphism group of \( \Gamma \), so that \( \text{Aut}(\Gamma) \) 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 3.** Let \( \Omega \) be a set and \( G \leqslant \mathcal{S}_\Omega \) 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 \( \mathcal{S}_\Omega \) whose orbits on \( \Omega \times \Omega \) are the same as \( G \)'s. Let \( \mathcal{C}_1, \ldots, \mathcal{C}_r \) be the orbits of \( G \) acting on \( \Omega \times \Omega \). Define digraphs \( G_1, \ldots, G_r \) by \( V(G_i) = \Omega \) and \( E(G_i) = \mathcal{C}_i \). Each \( G_i, 1 \leq i \leq r, \) is an orbital digraph of \( G \), and it is straightforward to show that \( G^{(2)} = \bigcap_{i=1}^{r} \text{Aut}(G_i) \). 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 4.** 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 \( \mathcal{S}_m \), which we denote by \( g/\mathcal{B} \). We define \( G/\mathcal{B} = \{ g/\mathcal{B} : g \in G \} \). Let \( \text{fix}_G(\mathcal{B}) = \{ g \in G : g(B) = B \text{ for every } B \in \mathcal{B} \} \).

**Definition 5.** If \( G \leqslant \text{Aut}(\Gamma) \), for some vertex-transitive graph \( \Gamma \), define a graph \( \Gamma/\mathcal{B} \) with vertex set \( V(\Gamma/\mathcal{B}) = \mathcal{B} \) and edge set

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

We observe that \( G/\mathcal{B} \leqslant \text{Aut}(\Gamma/\mathcal{B}) \).

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

**Definition 6.** Let \( \Gamma_1 \) and \( \Gamma_2 \) 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 \( \Gamma_1 \) and \( \Gamma_2 \), denoted \( \Gamma_1 \bowtie \Gamma_2 \), to be the digraph such that \( V(\Gamma_1 \bowtie \Gamma_2) = V(\Gamma_1) \times V(\Gamma_2) \) and \( E(\Gamma_1 \bowtie \Gamma_2) = E \). We remark that the wreath product of a circulant digraph of order \( m \) and a circulant digraph of order \( n \) is circulant.

**Definition 7.** Let \( G \) and \( H \) be groups acting on \( X \) and \( Y \), respectively. We define the **wreath product of \( X \) and \( Y \)**, denoted \( G \bowtie H \), to be the permutation group that acts on \( X \times Y \) consisting of all permutations of the form \( (x, y) \rightarrow (g(x), h_x(y)) \), where \( g \in G \) and \( h_x \in H \).

Clearly, \( \text{Aut}(\Gamma_1) \bowtie \text{Aut}(\Gamma_2) \leqslant \text{Aut}(\Gamma_1 \bowtie \Gamma_2) \). For information about the converse, see [27].
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, [29, 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 8.** Let $X$ be the set of all possible complete block systems of $(\mathbb{Z}_n)_L$. Define a partial order on $X$ by $B \preceq C$ if and only if every block of $C$ is a union of blocks of $B$.

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 [9, Theorem 1.6B]).

**Definition 9.** Let $G$ act transitively on the sets $\Omega$ and $\Gamma$, 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 10 ([15, 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) $H \cong A_m$ or $S_m$;
(ii) $m = 11$ and $H = PSL_2(11)$ 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 $P\Gamma L_d(q)$ containing $PSL_d(q)$.

**Theorem 11** (cf. Burnside [9, Theorem 3.5B]). Let $G$ be a transitive group of prime degree $p$. Then either $G$ is nonsolvable and doubly transitive or we may relabel the set upon which $G$ acts with elements of $\mathbb{F}_p$ so that $G \leq AGL(1, p) = \{ x \mapsto ax + b : a \in \mathbb{F}_p^*, \ b \in \mathbb{F}_p \}$.

**Definition 12.** Let $G$ be a permutation group acting on the set $\Omega$ 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 $\text{fix}_G(\mathcal{B})|_B$ is primitive for every $B \in \mathcal{B}$, and that $\text{fix}_G(\mathcal{B})$ on some $B$ is not faithful. (Since the actions of this group on the blocks of $\mathcal{B}$ are conjugate in $G$, $\text{fix}_G(\mathcal{B})$ is therefore not faithful on any $B \in \mathcal{B}$). Define an equivalence relation $\equiv$ on $\mathcal{B}$ by $B \equiv B'$ if and only if the subgroups of $\text{fix}_G(\mathcal{B})$ that fix $B$ and $B'$, point-wise respectively, are equal. We denote these subgroups by $\text{fix}_G(\mathcal{B})|_B$ and $\text{fix}_G(\mathcal{B})|_{B'}$, respectively. Denote the equivalence
Lemma 15. Let $\equiv$ be a vertex-transitive digraph for which $G \trianglelefteq \text{Aut}(\tilde{X})$ as above. Then $\text{fix}_G(\mathcal{B})|B$ is primitive for every $B \in \mathcal{B}$ and the action of $\text{fix}_G(\mathcal{B})$ is not faithful.

Lemma 13 (Dobson, [10]). Let $\tilde{X}$ be a vertex-transitive digraph for which $G \trianglelefteq \text{Aut}(\tilde{X})$ as above. Then $\text{fix}_G(\mathcal{B})|E_i \leq G^{(2)}$ for every $0 \leq i \leq a$. Furthermore, $\{E_i : 0 \leq i \leq a\}$ is a complete block system of $G$.

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

Lemma 15 (Kalužnin and Klin, [19]). 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. This result is an immediate consequence of Proposition 3.5 of [26], but as the direct proof is short, we include it for completeness.

Lemma 16. 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 $\text{fix}_G(\mathcal{B})|B$ 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 $\text{fix}_G(\mathcal{B})|B$ admits a complete block system $\mathcal{C}_B$ of $r$ blocks of size $s$ formed by the orbits of $\langle \rho^{mr} \rangle|B$, then $g(\mathcal{C}_B)$ is a complete block system of $\text{fix}_G(\mathcal{B})|B'$, where $g(B) = B'$. As $\langle \rho^m \rangle|B' \leq \text{fix}_G(\mathcal{B})|B'$, every complete block system of $\text{fix}_G(\mathcal{B})|B'$ 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 $g(\mathcal{C}_B)$ are 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 $\text{fix}_G(\mathcal{B})|B$. 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 $\text{fix}_G(\mathcal{B})$ acts
faithfully on each block \( B \in \mathcal{B} \), and that \( \text{fix}_G(\mathcal{B}) \mid_B \) 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 17.** Let \( G \leq S_{mk} \) admit a complete block system \( \mathcal{B} \) of \( m \) blocks of size \( k \), and contain a regular cyclic subgroup \( \langle \rho \rangle \). Assume that \( \text{fix}_G(\mathcal{B}) \) acts faithfully on \( B \in \mathcal{B} \) and that \( \text{fix}_G(\mathcal{B}) \mid_B \) is doubly transitive and nonsolvable for every \( B \in \mathcal{B} \). Then \( \text{fix}_G(\mathcal{B}) \mid_B \) is equivalent to \( \text{fix}_G(\mathcal{B}) \mid_{B'} \) for every \( B, B' \in \mathcal{B} \).

**Proof.** Let \( H = \langle \text{fix}_G(\mathcal{B}), \rho \rangle \). Then \( \text{fix}_H(\mathcal{B}) = \text{fix}_G(\mathcal{B}) \). Let \( B \in \mathcal{B} \). Perusing the list of doubly transitive groups given in [6, Theorem 5.3], we have (assuming towards a contradiction that there exist \( B_1, B_2 \) such that \( \text{fix}_G(\mathcal{B}) \mid_{B_1} \) is not equivalent to \( \text{fix}_G(\mathcal{B}) \mid_{B_2} \) that since \( \text{fix}_H(\mathcal{B}) \mid_B \) has more than one representation, it has exactly two representations. Define an equivalence relation \( \equiv \) on the elements permuted by \( S_{mk} \) from \( \text{fix}_H(\mathcal{B}) \mid_B \) if and only if \( \text{Stab}_{\text{fix}_H(\mathcal{B})}(i) = \text{Stab}_{\text{fix}_H(\mathcal{B})}(j) \). As \( \text{fix}_H(\mathcal{B}) \mid_B \) 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 \( \langle \rho^2 \rangle \). Then \( H/\mathcal{C} \) admits a complete block system \( \mathcal{D} \) of \( 2k \) blocks of size \( k \) formed by the orbits of \( \langle \rho^2 \rangle /\mathcal{C} \). Let \( \mathcal{D} = \{ D_1, D_2 \} \). Furthermore, \( \text{fix}_{H/\mathcal{C}}(\mathcal{D})|_{D_1} \) is doubly transitive and nonsolvable and \( \text{fix}_{H/\mathcal{C}}(\mathcal{D})|_{D_2} \) is not equivalent to \( \text{fix}_{H/\mathcal{C}}(\mathcal{D})|_{D_2} \).

As \( \rho \in H \), \( \text{fix}_{H/\mathcal{C}}(\mathcal{D})|_{D_1} \) contains a \( k \)-cycle. Hence \( \text{fix}_{H/\mathcal{C}}(\mathcal{D})|_{D_1} \) contains a \( k \)-cycle and has two representations. By Theorem 10 and [6, Theorem 5.3], we need only consider the cases where \( \text{soc}(\text{fix}_{H/\mathcal{C}}(\mathcal{D})|_{D_1}) \cong S_6 \) \((k = 6)\), \( \text{PSL}_{d}(q) \) \((k = (q^d - 1)/(q - 1)\) and \( d > 2)\), or \( \text{PSL}_2(11) \) \((k = 11)\). If \( k = 6 \) and \( \text{soc}(\text{fix}_{H/\mathcal{C}}(\mathcal{D})|_{D_1}) \cong S_6 \), then as \( \text{fix}_{H/\mathcal{C}}(\mathcal{D})|_{D_1} \) contains a \( 6 \)-cycle, \( \text{fix}_{H/\mathcal{C}}(\mathcal{D})|_{D_1} \cong S_6 \), contradicting Lemma 18 (stated and proven later). If \( k = (q^d - 1)/(q - 1) \) and \( \text{soc}(\text{fix}_{H/\mathcal{C}}(\mathcal{D})|_{D_1}) \cong \text{PSL}_d(q) \), then by Proposition 20 (stated and proven later) \( H/\mathcal{C} \) does not contain a \( 2k \)-cycle, a contradiction. Finally, if \( k = 11 \) and \( \text{soc}(\text{fix}_{H/\mathcal{C}}(\mathcal{D})|_{D_1}) \cong \text{PSL}_2(11) \), then by Lemma 19 (stated and proven later), \( H/\mathcal{C} \) does not contain a \( 2k \)-cycle, a contradiction. \( \square \)

**Lemma 18.** Let \( G \leq S_6 \) admit a complete block system \( \mathcal{B} \) of \( 2 \) blocks of size \( 6 \). Let \( \mathcal{B} = \{ B_1, B_2 \} \). Assume that \( \text{fix}_G(\mathcal{B}) \) acts faithfully on \( B \in \mathcal{B} \) and that \( \text{fix}_G(\mathcal{B}) \cong S_6 \) but \( \text{fix}_G(\mathcal{B})\mid_{B_1} \) is not equivalent to \( \text{fix}_G(\mathcal{B})\mid_{B_2} \). 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 \( \rho^2 \in \text{fix}_G(\mathcal{B}) \). Then conjugation by \( \rho \) induces an automorphism \( \varphi \) from \( \text{fix}_G(\mathcal{B})\mid_{B_1} \) to \( \text{fix}_G(\mathcal{B})\mid_{B_2} \). As \( \text{fix}_G(\mathcal{B})\mid_{B_1} \) is not equivalent to \( \text{fix}_G(\mathcal{B})\mid_{B_2} \), \( \varphi \) is an outer automorphism of \( S_6 \).

The group \( S_6 \) 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
Therefore, without loss of generality, we identify the points of \( \mathcal{S}_6 \) that interchanges type (a) and type (b) (cf. [28], 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 \( \alpha \) 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. \( \square \)

**Lemma 19.** Suppose \( G \) admits a complete block system \( \mathcal{B} = \{B_1, B_2\} \) of 2 blocks of size 11. Assume that \( K = \text{fix}_G(\mathcal{B}) \), that \( K |_{\mathcal{B}} \) is doubly-transitive for each \( B \in \mathcal{B} \), and that \( \text{soc}(K) \cong \text{PSL}_2(11) \). 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 \( \text{soc}(K) = \text{PSL}_2(11) \). We want to show that if \( x \in B_1 \), there is some \( y \in B_2 \) for which \( \text{Stab}_K(x) = \text{Stab}_K(y) \).

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 \( a \in \text{PGL}_2(11) \) for which \( f(k) = a^{-1}ka \) for all \( k \in K \) (cf. [7, p. 7], or the on-line version [8]). Let \( P = \langle \rho^2 \rangle \), a Sylow 11-subgroup of \( K \). Then \( \rho \) centralizes \( P \), so \( a \) is in the centralizer in \( \text{PGL}_2(11) \) of \( P \), which is \( P \). This means there is some \( \rho^{2i} \in P \), such that \( a = \rho^{2i} \). Hence \( f(k) = \rho^{-1}k \rho = a^{-1}ka = \rho^{-2i} \rho^{2i} = \rho^{1-2i} = k \) for every \( k \in K \). So we have \( \text{Stab}_K(x) = \rho^{2i-1} \text{Stab}_K(x) \rho^{1-2i} = \text{Stab}_K(\rho^{2i-1}(x)) \), completing the proof with \( y = \rho^{2i-1}(x) \). \( \square \)

The last result of this section deals with the group \( \text{PSL}_d(q) \) with \( d \geq 3 \). This result was initially proven by Dr. Dave Witte (now Dave Witte Morris), to assist us with this work. Thanks are due to him and to an anonymous referee, whose suggestions significantly shortened the proof.

**Note 1.** In the proposition that follows, 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. Also, if \( V \) has dimension \( d \), then \( \mathbb{H}(V) \) is used to denote the set of all \( d-1 \)-dimensional subspaces of \( V \).

**Proposition 20.** Let \( H \leq \mathcal{S}_{2k} \) admit a complete block system \( \mathcal{B} \) consisting of 2 blocks of size \( k \). Assume \( \text{fix}_H(\mathcal{B}) \) acts faithfully on \( B \in \mathcal{B} \) and \( \text{soc}(\text{fix}_H(\mathcal{B})) \cong \text{PSL}_d(q) \), where \( d > 2 \), \( q \) is a prime power, and \( k = (q^d - 1)/(q - 1) \). Let \( \mathcal{B} = \{B_1, B_2\} \). If \( \text{fix}_H(\mathcal{B}) |_{B_1} \) is not equivalent to \( \text{fix}_H(\mathcal{B}) |_{B_2} \), then \( H \) does not contain a 2k-cycle.

**Proof.** Because the action of \( \text{fix}_H(\mathcal{B}) \) on \( B_1 \) is not equivalent to the action of \( \text{fix}_H(\mathcal{B}) \) on \( B_2 \), one of the actions (say, the action on \( B_1 \)), must be isomorphic to the action of \( \text{fix}_H(\mathcal{B}) \) on \( \mathbb{P}((\mathbb{F}_q)^d) \); and the other action must be isomorphic to the action of \( \text{fix}_H(\mathcal{B}) \) on \( \mathbb{H}((\mathbb{F}_q)^d) \). Therefore, without loss of generality, we identify the points of \( B_1 \) with the elements of \( \mathbb{P}((\mathbb{F}_q)^d) \), and the points of \( B_2 \) with the elements of \( \mathbb{H}((\mathbb{F}_q)^d) \). We will consider the actions of \( H \) and \( \text{fix}_H(\mathcal{B}) \) on the complete bipartite graph \( \Gamma \) with bipartition sets \( B_1 \) and \( B_2 \).

Let \( \Gamma_1 \) be the graph whose vertices are the elements of \( \mathbb{P}((\mathbb{F}_q)^d) \cup \mathbb{H}((\mathbb{F}_q)^d) \), with an edge between a point and a hyperplane if and only if the point is in the hyperplane. Since \( \text{soc}(\text{fix}_H(\mathcal{B})) \cong \text{PSL}_d(q) \), we have \( \text{fix}_H(\mathcal{B}) \leq \text{PGL}_d(q) \). So \( \text{fix}_H(\mathcal{B}) \) preserves the incidence relation between points and hyperplanes, and hence \( \text{fix}_H(\mathcal{B}) \leq \text{Aut}(\Gamma_1) \). In fact,
it is straightforward to see that $\text{PSL}_d(q)$, and therefore $\text{fix}_H(B)$, acts transitively on the edges of $\Gamma_1$. So the edges of $\Gamma_1$ form an orbit of the action of $\text{fix}_H(B)$ on pairs from $P((F_q^d) \times H((F_q^d)^d))$. Likewise, the non-edges of $\Gamma_1$ that do not lie within either set of the bipartition, form an orbit (the only other orbit) of the action of $\text{fix}_H(B)$ on pairs from $P((F_q^d)^d) \times H((F_q^d)^d)$. Let $\Gamma_2$ be the bipartite graph with $V(\Gamma_2) = V(\Gamma)$ and edge set the non-edges of $\Gamma_1$ that do not lie within either set of the bipartition. Notice that the number of edges of $\Gamma_1$ is $k(q^d-1)/(q-1)$, which is therefore the length of the first of these orbits, while number of edges of $\Gamma_2$ is $k(q^d - q^{d-1})/(q-1)$. Since $q \geq 2$, $q^d - q^{d-1} = q^d(q-1) > q^{d-1} > q^{d-1} - 1$, so the second orbit of $\text{fix}_H(B)$ is longer than the first.

As $\text{fix}_H(B) \leq H$, and $\text{fix}_H(B)$ has exactly two orbits in its action on the edges of $\Gamma$, $H$ has either two orbits or one orbit in its action on the edges of $\Gamma_1$. As $\text{fix}_H(B) \leq H$, by [9, Exercise 1.4.6], if $H$ is transitive on the edges (that is, has one orbit) of $\Gamma$, then there exists $h \in H$ such that $h(\Gamma_1) = \Gamma_2$. However, $\Gamma_2$ has more edges than $\Gamma_1$, so no such $h$ can exist.

Thus $H$ has exactly two orbits in its action on the edges of $\Gamma$, which are also the orbits of $\text{fix}_H(B)$ acting on the edges of $\Gamma$. Thus $H \leq \text{Aut}(\Gamma_1)$.

Now, since $\text{PSL}_d(q) \leq \text{fix}_H(B)$, it is straightforward to verify that $\text{fix}_H(B)$ acts transitively on the set of triples
\[\{(l, h, m) \in P((F_q^d)^d) \times H((F_q^d)^d) \times P((F_q^d)^d) | l \neq m; (l, h), (m, h) \text{ edges of } \Gamma_1\}\]
and on the dual set of triples
\[\{(l, h, m) \in H((F_q^d)^d) \times P((F_q^d)^d) \times H((F_q^d)^d) | l \neq m; (l, h), (m, h) \text{ edges of } \Gamma_1\};\]
these two sets together form the 2-arcs of $\Gamma_1$. Now, towards a contradiction, suppose that $H$ does contain a $2k$-cycle. Then $H$ has elements that interchange $B_1$ and $B_2$, and therefore interchange these sets of triples, so $\Gamma_1$ is a 2-arc-transitive graph. In fact, since $H$ contains $2k$-cycle, $\Gamma_1$ is a 2-arc-transitive circulant graph.

However, 2-arc-transitive circulant graphs have been characterized in [2], and fall into four categories: complete graphs, cycles, complete bipartite graphs, and complete bipartite graphs minus a one-factor. Our graph $\Gamma_1$ is bipartite with degree $(q^d-1)/(q-1)$ on $2(q^d - 1)/(q-1)$ vertices; simple calculations show that this does not fall into any of the given categories. This is the desired contradiction. □

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 21.** Let $k$ and $m$ be integers such that $km$ is square-free. Let $G \leq S_{km}$ 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

- $\text{fix}_{\mathcal{G}}(\mathcal{B})$ is of order $k$,
- $\text{fix}_{\mathcal{G}}(\mathcal{B}) \leq \mathcal{C}(\mathcal{G})$ (the center of the group $\mathcal{G}$), and
- there exists no complete block system $\mathcal{F} > \mathcal{B}$ such that $\text{fix}_{\mathcal{G}}(\mathcal{F})$ 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 $\text{fix}_{\mathcal{G}}(\mathcal{D})$ 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 $|\text{fix}_{\mathcal{G}^{(2)}}(\mathcal{D}')|$.

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

**Lemma 22.** Under Hypothesis 21, suppose that $m > 1$ and Condition (1) does not hold. Let $\mathcal{C}$ be any complete block system of $G$ with $\mathcal{C} > \mathcal{B}$ that is minimal in the sense that there is no complete block system $\mathcal{C}'$ of $G$ with $\mathcal{B} < \mathcal{C}' < \mathcal{C}$. Then $(\text{fix}_{\mathcal{G}}(\mathcal{C})|_\mathcal{B})/\mathcal{B}$ is doubly transitive and nonsolvable.

**Proof.** Towards a contradiction, suppose that $(\text{fix}_{\mathcal{G}}(\mathcal{C})|_\mathcal{B})/\mathcal{B}$ is not doubly transitive, or is solvable. If $t$ were composite, then since $(\text{fix}_{\mathcal{G}}(\mathcal{C})|_\mathcal{B})/\mathcal{B}$ contains a regular cyclic subgroup of order $t$ and all cyclic groups of composite order are Burnside groups [29, Theorem 25.3], we would have $(\text{fix}_{\mathcal{G}}(\mathcal{C})|_\mathcal{B})/\mathcal{B}$ being doubly transitive. (The minimality of $\mathcal{C}$ means that $(\text{fix}_{\mathcal{G}}(\mathcal{C})|_\mathcal{B})/\mathcal{B}$ cannot be imprimitive.) By [18, Exercise 1, p. 169.], we must have $t = 4$, a contradiction.

So $t$ is prime, and by Theorem 11, $(\text{fix}_{\mathcal{G}}(\mathcal{C})|_\mathcal{B})/\mathcal{B} \leq AGL(1, t)$. Let $T$ be a Sylow $t$-subgroup of $\text{fix}_{\mathcal{G}}(\mathcal{C})$ that contains $\langle \rho^{mk/t} \rangle$. Now, $(\text{fix}_{\mathcal{G}}(\mathcal{C})|_\mathcal{B})/\mathcal{B}$ contains a unique Sylow $t$-subgroup, which must be $(T|_\mathcal{B})/\mathcal{B}$. Since $\text{fix}_{\mathcal{G}}(\mathcal{C})/\mathcal{B} \leq AGL(1, t)$, this also contains a unique Sylow $t$-subgroup, which must be $T/\mathcal{B}$. So $T/\mathcal{B}$ is characteristic in $\text{fix}_{\mathcal{G}}(\mathcal{C})/\mathcal{B}$, and is therefore normal in $G/\mathcal{B}$. Now, since $(k, t) = 1$, $\text{fix}_{\mathcal{G}}(\mathcal{B})$ is centralized by $T$ (since $\text{fix}_{\mathcal{G}}(\mathcal{B})$ is central in $G$), and $T/\mathcal{B}$ is normal in $G/\mathcal{B}$, we must have $T < G$. So the orbits of $T$ form a complete block system $\mathcal{D}'$ of $G$.

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


Since \( \text{fix}_G(\mathcal{E}) \) is not cyclic (by Hypothesis 21), there must be some \( \gamma \in \text{fix}_G(\mathcal{E}) \) for which \( \gamma / \mathcal{B} \not\in T / \mathcal{B} \). Then we have
\[
\gamma(x, y, z) = (x, \alpha_x(y) + \alpha_x, \beta_x(z) + b_x), \quad \alpha_x \in \mathbb{Z}_t, \quad \beta_x \in \mathbb{Z}_k, \quad b_x \in \mathbb{Z}_k \text{ as } \gamma \text{ normalizes } (\rho^{m/t}). \]  
As \( (\rho^m) \) is in the center of \( G \), we must have that \( \beta_x = 1 \) for every \( x \in \mathbb{Z}_{m/t} \). Since \( \text{fix}_G(\mathcal{D}') = (\rho^{mk/t}) \triangleleft G \), conjugating \( \rho^{mk/t} \) by \( \gamma \) shows that \( \alpha_x = \alpha'_x = \alpha \) for any \( x, x' \in \mathbb{Z}_{m/t} \).

Choose \( i \) so that \( \rho^{itk}(x, y, z) = (x + 1, y, z) \) for every \( (x, y, z) \in \mathbb{Z}_{m/t} \times \mathbb{Z}_t \times \mathbb{Z}_k \). 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 \( \text{fix}_G(\mathcal{E}) / \mathcal{B} \).

Since \( T = \text{fix}_G(\mathcal{D}') \) has order \( t \), \( T / \mathcal{B} \) has order \( t \), and as \( \rho^{mk/t} \in T / \mathcal{B} \), we must have that \( a_{x+1} - a_x = c \) is constant for every \( x \in \mathbb{Z}_{m/t} \). Then \( a_1 = c + a_0, a_{x+1} = c + a_x \) so that \( a_{x+1} = (x + 1)c + a_0 \). Hence \( a_0 = (m/t)c + a_0 \). Since \( \gcd(m/t, k) = 1 \), \( a_0 = 0 \), and so \( a_{x+1} = a_x = a \) is constant. Without loss of generality, since \( \rho \in G \), we may assume that \( a = 0 \).

Now since \( \gamma^{-1} \rho^{itk}\rho^{itk} / \mathcal{B} = \mathcal{B} \), \( b_{x+1} - b_x \) must be constant. Since \( (m/t, k) = 1 \), this constant must be 0, so \( b_{x+1} = b_x = b \) is constant. Still without loss of generality because of the presence of \( \rho \) in \( G \), we may assume that \( b = 0 \). But now \( \gamma(x, y, z) = (x, \alpha y, z) \), so \( \gamma \in \text{fix}_G(\mathcal{D}') = (\rho^{mk/t}) \), a contradiction. \( \square \)

**Lemma 23.** Under Hypothesis 21, suppose that \( m > 1 \) and Condition (1) does not hold, and let \( \mathcal{E} \) be as in Lemma 22. Let \( L = \{g^{-1} \rho^{mk/t} g : g \in G\} \) and \( H = \langle L \rangle \). Then

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

**Proof.** By Lemma 22, we have that \( (\text{fix}_G(\mathcal{E}) \cap \mathcal{B}) / \mathcal{B} \) is a doubly-transitive nonsolvable group. Note that every element of \( L \) has order \( t \).

1. Any \( \vartheta \in H \) must be of the form \( \vartheta = g_1^{a_1} g_2^{a_2} \cdots g_t^{a_t} \), where \( a_i \in \mathbb{Z}_t \) and \( \gamma_i \in L \) for \( i = 1, \ldots, t \). For any \( g \in G \) we then have
   \[
g^{-1} \vartheta g = g^{-1} g_1^{a_1} g_2^{a_2} \cdots g_t^{a_t} g = (g^{-1} \gamma_1 g)^{a_1} (g^{-1} \gamma_2 g)^{a_2} \cdots (g^{-1} \gamma_t g)^{a_t}.
   \]
   As \( \gamma_i \in L \), we have \( \gamma_i = g_i^{-1} \rho^{kr/t} g_i \) for some \( g_i \in G \). Hence
   \[
g^{-1} \gamma_i g = (g_1 g)^{-1} \rho^{kr/t} (g_1 g) \in L
   \]
   and \( g^{-1} \vartheta g \in H \). Therefore \( H \triangleleft G \).

3. and \( 4. \) Since \( \rho^{mk/t} \in \text{fix}_G(\mathcal{E}) \) and \( \text{fix}_G(\mathcal{E}) \triangleleft G \), we have that \( H \triangleleft \text{fix}_G(\mathcal{E}) \). As \( H \triangleleft \text{fix}_G(\mathcal{E}) \), 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 \( x \in \mathbb{Z}_{m/t} \) and \( y \in \mathbb{Z}_t \). Since \( |\gamma| = t \) and \( \gcd(m, k) = 1 \), we have that \( \sum_{y \in \mathbb{Z}_t} d_{x,y} \equiv 0 \) (mod \( k \)) for every \( x \in \mathbb{Z}_{m/t} \). Therefore every \( \vartheta \in H \), since it is of the form \( g_1^{a_1} g_2^{a_2} \cdots g_t^{a_t} \) for \( \gamma_1, \gamma_1, \ldots, \gamma_t \in L \), acts as \( \vartheta(x, y, z) = (x, e_x(y), z + e_{x,y}) \), where \( \sum_{y \in \mathbb{Z}_t} e_{x,y} \equiv 0 \) (mod \( k \)) for every \( x \in \mathbb{Z}_{m/t} \). It is now clear that \( (\rho^m) \cap H = 1 \) as \( \rho^m(x, y, z) = (x, y, z + m) \) and \( \sum_{i=1}^{t} m \not\equiv 0 \) (mod \( k \)) as \( \gcd(m, k) = 1 \).
2. The orbits of $H$ have length $k'$ for some $k'|k$. Suppose that $k' = 1$. If $|H| = t$ then $H = (p^{mk/k'}) \triangleleft G$, so $((p^{mk/k'})|_{C})/\mathcal{B} \triangleleft \text{fix}_G(\mathcal{C})/\mathcal{B}$, forcing $\text{fix}_G(\mathcal{C})/\mathcal{B} \leq AGL(1, t)$, 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 $(\text{fix}_G(\mathcal{C})/\mathcal{B}$ is doubly transitive. This contradiction shows that we must have $k' \neq 1$. □

** Lemma 24.** Under Hypothesis 21, suppose that $m > 1$ and Condition (1) does not hold, and let $\mathcal{C}$ be as in Lemma 22, and $H$ as in Lemma 23. 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 $x^* \in \mathbb{Z}_{m/t}$ 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. $\sum_{y \in \mathcal{C}} b_{x,y} \equiv 0 \pmod{p}$ for every non-singleton orbit $\mathcal{C}$ of $\sigma_x$,
3. $h|_{\mathcal{C}_x/\mathcal{B}}$ 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 $k'$ and $H$ admits $\mathcal{B}$ as a complete block system, for any chosen block $B \in \mathcal{B}$, Stab$_H(B)$, the set-wise stabilizer of the block $B$, is transitive on each orbit of $(p^{mk/k'})|_{B}$. 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 $p^m$ is in the center of $G$). That is, for every $x^* \in \mathbb{Z}_{m/t}$ 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 $h|/B \neq 1$, as otherwise $1 \neq h \in \text{fix}_G(\mathcal{B}) = (p^m)$, but by Lemma 23, $(p^m) \cap H = 1$. 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 $y^* \in \mathbb{Z}_{m/t}$ and $y^* \in \mathbb{Z}_t$. Fix these $x^*, y^*$, and $h$.

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

(3–5) As the order of $h$, and hence of each $\sigma_x$, 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 23), $h|_{\mathcal{C}_x/\mathcal{B}}$ must have at least two fixed points. Furthermore, there is at least one $h|\mathcal{C}_x|\mathcal{B} \not\equiv 1 \pmod{p}$ and $\sigma_{x^*}(\ell^*) = \ell^*$, since $p|t$. Finally, observe that $h$ must fix some block of $\mathcal{B}$ contained in any block of $\mathcal{C}$, again since $p|t$ and the length of any orbit of $h$ is a power of $p$. □
Lemma 25. Under Hypothesis 21, suppose that \( m > 1 \) and Conditions (1) and (2) do not hold, and let \( \mathcal{G} \) be as in Lemma 22. Then there is a complete block system \( \mathcal{F} > \mathcal{B} \) of \( G \), consisting of \( t \) blocks of size \( mk/t \), where each block is an orbit of \( \langle \rho^{mk/t} \rangle \).

Proof. By Lemma 22, we have that \( (\text{fix}_G(\mathcal{G})|_C)/\mathcal{B} \) is doubly transitive and nonsolvable for each \( C \in \mathcal{G} \). Define \( H \) as in Lemma 23. By Lemma 23, \( H < G \), the orbits of \( H \) have order \( k' \) for some \( k' | k, k' \neq 1 \), and \( \langle \rho^n \rangle \cap H = 1 \). By Lemma 24, 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 \( x^* \in \mathbb{Z}_{m/t} \) and some \( y^* \in \mathbb{Z}_t \), \( \sigma_x(y^*) = y^* \) and \( b_{x^*,y^*} \equiv 1 \mod p \). Furthermore, \( h \) satisfies the following additional properties:

1. \(|h| \) is a power of \( p \),
2. \( \sum_{y \in \mathcal{E}} b_{x,y} \equiv 0 \mod p \) for every non-singleton orbit \( \mathcal{E} \) of \( \sigma_x \),
3. \( h|_{C_{x^*}}/\mathcal{B} \) has at least two fixed points,
4. there is at least one \( b_{x^*,\ell^*} \neq 1 \mod p \) and \( \sigma_{x^*}(\ell^*) = \ell^* \), and
5. \( h \) fixes some block of \( \mathcal{B} \) contained in any block of \( \mathcal{G} \).

For each \( x \in \mathbb{Z}_{m/t} \) define a homomorphism \( \pi_x : \text{fix}_G(\mathcal{G}) \rightarrow \mathcal{S}_1 \) by \( \pi_x(g) = (g|_{C_x})/\mathcal{B} \). Define an equivalence relation \( \equiv \) on \( \mathcal{G} \) by \( \mathcal{C}_x \equiv \mathcal{C}_y \) if and only if \( \text{Ker}(\pi_x)/\mathcal{B} = \text{Ker}(\pi_y)/\mathcal{B} \). As in the proof of Lemma 14, 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 16 and the fact that \( \text{fix}_G(\mathcal{B}) = \langle \rho^m \rangle \)).

Let \( X \) be a circulant digraph with \( G \leq \text{Aut}(X) \), and let \( G' \leq \text{Aut}(X) \) be largest subgroup of \( \text{Aut}(X) \) 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 exist \( C, C_r \in \mathcal{G} \) such that \( e \) is an edge between \( C \) and \( C_r \). Then there exists \( \mathcal{D}', \mathcal{D}'_r \in \mathcal{D}' \) such that \( e \) is an edge between \( \mathcal{D}' \) and \( \mathcal{D}'_r \). We will show that every vertex of \( \mathcal{D}' \) is adjacent to every vertex of \( \mathcal{D}'_r \). 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 \( \mathcal{D}' \subseteq \mathcal{C}_{x^*} \) (so that \( C = \mathcal{C}_{x^*} \)).

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

$$\text{Stab}_{\fix_G(\equiv')}/\mathcal{B}(B) = \text{Stab}_{\fix_G(\equiv')}/\mathcal{B}(B'),$$

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 $(\fix_G(\equiv')_C)/\mathcal{B}$ 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 $m/t$. As $\ker(\pi_x)/\mathcal{B} = \ker(\pi_x')/\mathcal{B}$ for all $x, x' \in \mathbb{Z}_{m/t}$, we have that $\pi_x(\fix_G(\equiv')) = (\fix_G(\equiv'))_C/\mathcal{B}$ is a faithful representation of $\fix_G(\equiv')/\mathcal{B}$ for all $x \in \mathbb{Z}_{m/t}$. By Lemma 17, the representations $\pi_x(\fix_G(\equiv'))$ and $\pi_x'(\fix_G(\equiv'))$ are equivalent for all $x, x' \in \mathbb{Z}_{m/t}$. Thus each equivalence class of $\equiv'$ contains $m/t$ blocks of $\mathcal{B}$. Since $\mathcal{F}$ is a complete block system of $G$, and $(\rho) \leq G$, the blocks of $\mathcal{F}$ must be the orbits of $(\rho^{mk/t})$. □

**Lemma 26.** Under Hypothesis 21, 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. $\mathcal{C} \supset \mathcal{B}$;
2. there is no complete block system $\mathcal{B}'$ for which $\mathcal{B} < \mathcal{B}' < \mathcal{C}$; 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 $m/r$ 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 $\mathcal{B} < \mathcal{B}' < \mathcal{C}'$, $pk$ 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 $\mathcal{B} < \mathcal{B}' < \mathcal{C}'$, 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 $\mathcal{B} < \mathcal{B}' < \mathcal{C}'$, and say that $\mathcal{B}'$ consists of $m/t'$ blocks of size $kt'$, where $t' > 1$. Notice that $t' | r$. By our choice of $\mathcal{C}'$, we must have $p | t'$. By Lemma 25, 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 $mk/t'$.

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 $r/t'$ blocks of $\mathcal{B}$. Hence $\mathcal{C}''$ consists of $t' \cdot m/r$ blocks of size $k \cdot r/t'$. But $t' > 1$ and $p | t'$, but $p | t'$, so $p | r/t'$, contradicting our choice of $\mathcal{C}'$. □

**Lemma 27.** Let $k$ and $m$ be integers such that $mk$ is square-free. Let $G \leq S_{mk}$ 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 $\fix_G(\mathcal{B})$ is of order $k$, $\fix_G(\mathcal{B}) \leq C(G)$, and there exists no complete block system $\mathcal{F} > \mathcal{B}$ such that $\fix_G(\mathcal{F})$ is semiregular, then one of the
There exists a complete block system \( \mathcal{D} \) of \( G \) such that \( \text{fix}_G(\mathcal{D}) \) 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 \( |\text{fix}_G^{(2)}(\mathcal{D})| \).

**Proof.** By Lemma 26, we may assume that if \( 2|m \), then we can choose \( \mathcal{C} \) with \( m/t \) blocks of size \( kt \) as in Lemma 22, with \( 2|t \). Let \( \mathcal{F} \) be a complete block system consisting of \( t \) blocks of size \( mk/t \), as found in Lemma 25. Since \( (\text{fix}_G(\mathcal{C}))/\mathcal{B} \) is doubly transitive (by Lemma 22) and \( \mathcal{F} \) is a complete block system, we must have \( \text{Stab}_{\text{fix}_G(\mathcal{C})/\mathcal{B}}(B) = \text{Stab}_{\text{fix}_G(\mathcal{C})/\mathcal{B}}(B') \) if and only if there is some \( F \in \mathcal{F} \) for which \( B, B' \subseteq F \).

Obtain \( h \) from Lemma 24. Since \( h|_{G_{x}} \) has at least two fixed blocks, so must \( h|_{G} \) 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 \( \sigma \).

As in the proof of Lemma 25, let \( \mathcal{D}' \) be the complete block system of \( G \) formed by the orbits of \( (\rho^{mk/p}) \), let \( X \) be a circulant digraph with \( G \leq Aut(X) \), and let \( G' \leq Aut(X) \) be the largest subgroup of \( Aut(X) \) that admits \( \mathcal{B} \) and \( \mathcal{D}' \) as complete block systems. Note again that \( G' \) is 2-closed.

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

Suppose that there is an edge \( e \) between a vertex of \( F_{x,v} \) and a vertex of \( F_{r} \), where \( F_{r} \in \mathcal{F} \) and \( F_{x,v} \neq F_{r} \). Arguing as in Lemma 25, we have that there exists \( D', D' \in \mathcal{D}' \), \( C \in \mathcal{C} \) and \( B_{r,z} \in \mathcal{B} \) such that \( D' \subseteq B_{x,v} \) and \( D' \subseteq F_{x,v} \), \( D' \subseteq C \), \( B_{r,z} \subseteq C \), 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 \( m/t \) is even. Suppose there exists \( u, v \in \mathbb{Z}/m/t \) such that \( u \neq v \), \( \sigma(u) = u \), \( \sigma(v) = v \), and \( b_{x,v} \neq b_{r,v} \) (mod \( p \)). As \( (\text{fix}_G(\mathcal{C}))/\mathcal{B} \) is doubly transitive for \( C \in \mathcal{C} \), we may assume without loss of generality that \( D' \subseteq B_{x,v} \) and \( D' \subseteq B_{r,v} \). 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 \( n \in \mathbb{Z}/m \) such that \( n = n \), \( y^{*} = y^{*} \). As \( b_{x,v} \neq b_{r,v} \) (mod \( p \)), \( b_{r,n} \) cannot be congruent modulo \( p \) to both. Thus appropriate \( u \) and \( v \) as above exist. We now assume that \( \sigma \) fixes exactly two blocks set-wise and that no appropriate \( u \) and \( v \) as above exist.

As \( \sum_{y \in \mathcal{C}} b_{x,y} \equiv 0 \) (mod \( p \)), for every \( x \in \mathbb{Z}/m/t \), \( \sigma(y^{*}) = y^{*} \), \( \sigma(\ell^{*}) = \ell^{*} \) and for every non-singleton orbit \( \mathcal{C} \) of \( \sigma \) we have that \( \sum_{y \in \mathcal{C}} b_{x,y} \equiv 0 \) (mod \( p \), \( b_{r,n} \) we must have that \( b_{x,y} + b_{x,\ell} \equiv 0 \) (mod \( p \)) for every \( x \in \mathbb{Z}/m/t \). Thus \( b_{x,v} \equiv 1 \) (mod \( p \)), \( b_{r,y} \equiv 1 \) (mod \( p \)), as otherwise appropriate \( u \) and \( v \) as above exist. Let \( q = r - y^{*} \). Similarly, \( b_{r+q,y} \equiv 1 \) (mod \( p \)) and \( b_{r+q,\ell} \equiv 1 \) (mod \( p \)) or we may conjugate \( h \) by an appropriate power of \( \rho \) 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 \(m/t\) is even, which as previously mentioned is a contradiction.

\[ \Box \]

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 28.** Let \( G \leq S_{mk} \) 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 \( \text{fix}_G(\mathcal{B}) \) is primitive and \( \text{fix}_G(\mathcal{B}) \) does not act faithfully on \( B \in \mathcal{B} \), then \( G = G_1 \cap G_2 \), where \( G_1 = S(\mathcal{B}) \cap H_1 \) and \( G_2 = H_2 \cap S(\mathcal{B}) \), \( H_1 \) 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 \( \text{fix}_G(\mathcal{B}) \) that fix \( B \) and \( B' \), point-wise respectively, are equal. Denote the equivalence classes of \( \equiv \) by \( C_0, \ldots, C_r \) and let \( E_i = \bigcup_{B \in C_i} B \). By Lemma 14, \( \text{fix}_G(\mathcal{B})|_{E_i} \leq G \) 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 orbits of some subgroup \( \langle \rho^a \rangle \). Since \( \text{fix}_G(\mathcal{B}) \) 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 \( \Gamma_{\ell} \) be 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 \( \Gamma_{\ell} \) is disconnected. Then \( \Gamma_{\ell} \) is trivially a wreath product and it is easy to see that \( \text{Aut}(\Gamma_{\ell}) \leq S(\mathcal{B}) \cap S_{mk/r} \), where \( r|\ell \). 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 \( \text{fix}_G(\mathcal{B})|_{E_i} \in \text{Aut}(\Gamma_{\ell}) \), 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 \( \Gamma_{\ell} = \Gamma_{\ell}' \cdot \tilde{K}_k \) for some \( \Gamma_{\ell}' \) 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, \( G = \cap_{\ell \in L} \text{Aut}(\Gamma_{\ell}) \). 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 \( \ell \), where \( (i, j) \in E(\Gamma_{\ell}) \). Note then that \( \text{Aut}(D) = G \). Let \( J \subseteq L \) such that if \( l \in J \), then \( \Gamma_{\ell} \) is a disconnected orbit digraph of \( G \) such that the vertex set of every component of \( \Gamma_{\ell} \) 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 \( \text{Aut}(D_1) = S(\mathcal{B}) \cap H_1 \), where \( H_1 \) is permutation isomorphic to \( \text{Aut}(D_1[E]) \), 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 \( \Gamma_{\ell} = \Gamma_{\ell}' \cdot \tilde{K}_k \), we have that \( D_2 = D_2' \cdot \tilde{K}_k \), where \( D_2' = D_2 / \mathcal{B} \). Let \( K \leq \text{Aut}(D_2) \) be the maximal subgroup of \( \text{Aut}(D_2) \) that admits \( \mathcal{E} \) as a complete block system. Then \( K = \text{Aut}(D_2') \cdot \mathcal{B} \) and \( \text{Aut}(D_2) \cap \text{Aut}(D_1) = K \cap \text{Aut}(D_1) \) as \( \text{Aut}(D_1) \) admits \( \mathcal{E} \) as a complete block system. We let \( H_2 = \text{Aut}(D_2') \). Let \( g \in G \). As \( G \) admits \( \mathcal{B} \) and \( \mathcal{E} \) as complete block systems, \( g \in \text{Aut}(D_1) \) and \( g \in \text{Aut}(D_2) \). Conversely, if \( g \in \text{Aut}(D_1) \cap \text{Aut}(D_2) \),
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 $E(D_1) \cup E(D_2) = E(D)$, $g \in \text{Aut}(D)$. Thus $G = \text{Aut}(D) = (\mathcal{F}_r : H_1) \cap (H_2 : \mathcal{F}_k)$. Finally, as $\mathcal{B} \leq \mathcal{E}$, we have that $r|m$. □

Lemma 29. Let $G \leq \mathcal{S}_m$ be 2-closed and contain a regular cyclic subgroup $\langle p \rangle$. 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 $\mathcal{C} < \mathcal{B}$. If $|\text{fix}_G(\mathcal{B})| > k$, then one of the following is true:

1. $G = G_1 \cap G_2$, where $G_1 = \mathcal{S}_r : H_1$ and $G_2 = H_2 : \mathcal{S}_k$, 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 $\langle in \rangle H = H_1 \times H_2$ (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 $\mathcal{C} < \mathcal{B}$, it follows by Lemma 16 that $\text{fix}_G(\mathcal{B})|_B$ is primitive. If $\text{fix}_G(\mathcal{B})$ does not act faithfully on $B \in \mathcal{B}$, then by Lemma 28 (1) holds. We thus assume that $\text{fix}_G(\mathcal{B})$ acts faithfully on each $B \in \mathcal{B}$. Define an equivalence relation $\equiv'$ on $\mathbb{Z}_m$ by $i \equiv' j$ if and only if $\text{Stab}_{\text{fix}_G(\mathcal{B})}(i) = \text{Stab}_{\text{fix}_G(\mathcal{B})}(j)$.

We demonstrate that $\text{fix}_G(\mathcal{B})|_B$ is equivalent to $\text{fix}_G(\mathcal{B})|_{B'}$ for every $B, B' \in \mathcal{B}$. First, if $\text{fix}_G(\mathcal{B})|_B$ is doubly transitive and nonsolvable for every $B \in \mathcal{B}$, Lemma 17 tells us that $\text{fix}_G(\mathcal{B})|_B$ is equivalent to $\text{fix}_G(\mathcal{B})|_{B'}$ 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 22, since $\text{fix}_G(\mathcal{B})|_B$ is primitive, $\text{fix}_G(\mathcal{B})|_B$ must be doubly transitive, and since $k \neq 4 \text{fix}_G(\mathcal{B})|_B$ must be nonsolvable, and therefore the actions are equivalent by the argument of the previous sentence. The remaining possibility is that $\text{fix}_G(\mathcal{B})|_B$ is not doubly transitive or is solvable, and $k = p$ is prime. By Burnside’s Theorem (Theorem 11), $\text{fix}_G(\mathcal{B})|_B$ is doubly transitive if $\text{fix}_G(\mathcal{B})|_B$ is nonsolvable. We conclude that $\text{fix}_G(\mathcal{B})|_B$ is solvable for every $B \in \mathcal{B}$, so that $\text{fix}_G(\mathcal{B})|_B \leq \text{AGL}(1, p)$. Let $[\text{fix}_G(\mathcal{B})|_B] = pr, r|(p - 1)$. Conjugating $\text{Stab}_{\text{fix}_G(\mathcal{B})}(i)$ by any element of $\text{fix}_G(\mathcal{B})$ gives $\text{Stab}_{\text{fix}_G(\mathcal{B})}(i')$ for some $i'$ for which $i, i' \in B \in \mathcal{B}$, so if we can show that $\text{Stab}_{\text{fix}_G(\mathcal{B})}(i)$ and $\text{Stab}_{\text{fix}_G(\mathcal{B})}(j)$ are conjugate in $\text{fix}_G(\mathcal{B})$ whenever $i$ and $j$ are in different blocks of $\mathcal{B}$, we will have shown that the actions are equivalent, as desired.

Since $\text{AGL}(1, p)$ and hence $\text{fix}_G(\mathcal{B})$ is solvable, $\text{Stab}_{\text{fix}_G(\mathcal{B})}(i)$ is in some Hall subgroup of $\text{fix}_G(\mathcal{B})$ that is conjugate in $\text{fix}_G(\mathcal{B})$ to the Hall subgroup that contains $\text{Stab}_{\text{fix}_G(\mathcal{B})}(j)$. Since $\text{AGL}(1, p)/p$ is cyclic, where $P$ is the Sylow $p$-subgroup of $\text{AGL}(1, p)$, it contains a unique subgroup of order $r$. This shows that, in fact, $\text{Stab}_{\text{fix}_G(\mathcal{B})}(i)$ and $\text{Stab}_{\text{fix}_G(\mathcal{B})}(j)$ are conjugate in $\text{fix}_G(\mathcal{B})$. We conclude that the actions of $\text{fix}_G(\mathcal{B})|_B$ and $\text{fix}_G(\mathcal{B})|_{B'}$ 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 $\mathcal{C} < \mathcal{B}$, 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 $\mathbb{Z}_m$, we have that the equivalence classes of $\equiv'$ form a complete block system $\mathcal{B}'$ of $k$ blocks of size
As \( \rho \leq G \), \( \mathcal{B} \) must be formed by the orbits of \( \langle \rho^k \rangle \). Then \( \text{fix}_G(\mathcal{B}) \triangleleft G \), \( \text{fix}_G(\mathcal{B}') \triangleleft G \), and \( \text{fix}_G(\mathcal{B}) \cap \text{fix}_G(\mathcal{B}') = 1 \). Let \( H \) be the internal direct product of \( H_1 = \text{fix}_G(\mathcal{B}) \) and \( H_2 = \text{fix}_G(\mathcal{B}') \) (so that \( H \cong \text{fix}_G(\mathcal{B}) \times \text{fix}_G(\mathcal{B}') \)). Then \( H \triangleleft G \). Since \( (m, k) = 1 \), \( \rho^m \in \text{fix}_G(\mathcal{B}) \) and \( \rho^k \in \text{fix}_G(\mathcal{B}') \), we also have \( \langle \rho \rangle \leq H \).

Now, consider \( H^{(2)} \). By Lemma 15, \( H^{(2)} = \text{fix}_G(\mathcal{B})^{(2)} \times \text{fix}_G(\mathcal{B}')^{(2)} \). As \( H \leq G \), \( H^{(2)} \leq G \). Hence \( \text{fix}_{H^{(2)}}(\mathcal{B}) \leq \text{fix}_G(\mathcal{B}) \) and \( \text{fix}_{H^{(2)}}(\mathcal{B}') \leq \text{fix}_G(\mathcal{B}') \). As \( H^{(2)} = \text{fix}_G(\mathcal{B})^{(2)} \times \text{fix}_G(\mathcal{B}')^{(2)} \), \( \text{fix}_{H^{(2)}}(\mathcal{B}) = \text{fix}_G(\mathcal{B})^{(2)} \) and \( \text{fix}_{H^{(2)}}(\mathcal{B}') = \text{fix}_G(\mathcal{B}')^{(2)} \). Thus \( \text{fix}_G(\mathcal{B}) = \text{fix}_{H^{(2)}}(\mathcal{B}) \leq \text{fix}_G(\mathcal{B})^{(2)} \) so that \( \text{fix}_G(\mathcal{B}) \) is 2-closed. Similarly, \( \text{fix}_G(\mathcal{B}') \) is 2-closed. Hence

\[
H^{(2)} = \text{fix}_G(\mathcal{B})^{(2)} \times \text{fix}_G(\mathcal{B}')^{(2)} = \text{fix}_G(\mathcal{B}) \times \text{fix}_G(\mathcal{B}') = H.
\]

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

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

**Lemma 30.** 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 \( \text{fix}_H(\mathcal{B}) \triangleleft H \). Furthermore, if \( g \in G \), then \( g^{-1} \text{fix}_H(\mathcal{B})g \triangleleft H \). 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 \( g^{-1} \text{fix}_H(\mathcal{B})g \triangleleft H \) and has orbits of the same size as \( B \in \mathcal{B} \), the orbits of \( g^{-1} \text{fix}_H(\mathcal{B})g \) are the same as those of \( \text{fix}_H(\mathcal{B}) \). Hence \( g^{-1} \text{fix}_H(\mathcal{B})g = \text{fix}_H(\mathcal{B}) \), so that \( \text{fix}_H(\mathcal{B}) \triangleleft H \). Thus the orbits of \( \text{fix}_H(\mathcal{B}) \) form the complete block system \( \mathcal{B} \) of \( G \). \( \square \)

**Definition 31.** For a positive integer \( n \), we define \( N(n) = \{x \rightarrow ax + b : a \in \mathbb{Z}_n^*, b \in \mathbb{Z}_n\} \). Note that \( N(n) \) is the normalizer of the left regular representation of \( \mathbb{Z}_n \), and if \( n \) is prime, then \( N(n) = \text{AGL}(1, n) \). We let \( (\rho) \) be the cyclic subgroup of \( N(n) \) defined by \( \rho(x) = x + 1 \).

**Lemma 32.** Let \( H \trianglelefteq N(mk) \), \( mk \) 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 \( (\rho^m) \) is the unique minimal subgroup of \( \text{fix}_H(\mathcal{B}) \) 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 \( (\rho) \) 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 \( G_i \leq \mathcal{B} \) consisting of \( mk/p_i \) blocks of size \( p_i \) formed by the orbits of \( (\rho^{mk/p_i}) \). We may thus view \( N(mk) \) (and so \( H \)) as acting on \( \mathbb{Z}_m \times \prod_{i=1}^r \mathbb{Z}_{p_i} \) in the canonical fashion by viewing \( N(mk) \) as \( N(m) \times \prod_{i=1}^r \text{AGL}(1, p_i) \). Let \( K \leq \text{fix}_H(\mathcal{B}) \) 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 \( \pi_i : K \rightarrow \text{AGL}(1, p_i) \) to be projection onto the \( (i + 1)^{th} \)-coordinate (viewing \( K \cong N(m) \times \prod_{i=1}^r \text{AGL}(1, p_i) \)). Then \( \pi_i(K) \) is transitive for every \( 1 \leq i \leq r \). Furthermore, as \( \text{AGL}(1, p_i) \) contains a unique transitive subgroup (namely, its unique Sylow \( p_i \)-subgroup), \( \pi_i(K) \) must contain the unique Sylow \( p_i \)-subgroup of \( \text{AGL}(1, p_i) \). Now, observe that \( \pi_i((\rho^m)) \) is also the unique Sylow \( p_i \)-subgroup of \( \text{AGL}(1, p_i) \) so that \( \pi_i((\rho^m)) \leq \pi_i(K) \).
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 $AGL(1, p_i)$. Then $\pi_i^{-1}(P_i)_B$ is transitive, but $\delta \notin \pi_i^{-1}(P_i)$, a contradiction. □

**Lemma 33.** Let $mk$ be a square-free integer, and let $G \leq \mathcal{S}_{mk}$ 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 $\text{fix}_G(\mathcal{B}) \leq N(mk)$. Then there exists $H \triangleleft G$ such that

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

**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 $\langle \rho^m \rangle \leq \text{fix}_G(\mathcal{B})$, and by Lemma 32, $\langle \rho^m \rangle$ is the unique minimal subgroup of $\text{fix}_G(\mathcal{B})$ 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 $\beta_i(j) = x_i \cdot j + b_i$, where $x_i \in \mathbb{Z}_k^\times, b_i \in \mathbb{Z}_k$. As $\langle \rho^m \rangle \leq G, x_i = x_j$ for every $i, i' \in \mathbb{Z}_m$. Thus $g(i, j) = (\delta(i), x_j \cdot j + b_i)$. Let $H = \langle \rho \rangle^G = \{g^{-1}\rho g : g \in G, \ell \in \mathbb{Z}_{mk}\}$, the normal closure of $\langle \rho \rangle$ in $G$. As every $g \in G$ has the form $g(i, j) = (\delta(i), x_j \cdot j + b_i)$, 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 $\text{fix}_G(\mathcal{B})$ of the form $(i, j) \rightarrow (\gamma(i), j + b_i)$, so that $\text{fix}_H(\mathcal{B}) = \langle \rho^m \rangle$ 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 $\rho^m$ commutes with every element of $H$ so that $\langle \rho^m \rangle \leq C(H)$ and (3) follows. □

**Lemma 34.** Let $G \leq \mathcal{S}_{mk}, mk$ 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 $\text{fix}_H(\mathcal{B}) \leq N(mk)$, then $\text{fix}_H(\mathcal{B}) \leq N(mk)$.

**Proof.** By Lemma 30, $\mathcal{B}$ is also a complete block system of $G$. Let $g \in \text{fix}_G(\mathcal{B})$. Then $g^{-1}\rho g \rho^{-1}/\mathcal{B} = 1$ so that $g^{-1}\rho g \rho^{-1} \in \text{fix}_G(\mathcal{B})$. Furthermore, $\rho \in H$ so that $g^{-1}\rho g \in H$. Whence $g^{-1}\rho g \rho^{-1} / \mathcal{B} \in \text{fix}_H(\mathcal{B}) \leq N(mk)$. As $\rho^{-1} \in N(mk)$, we have that $g^{-1}\rho g \in N(mk)$ and $(g^{-1}\rho g)$ is transitive. By Lemma 32, we have that $g^{-1}\rho g \in \langle \rho \rangle$ so that $g \in N(mk)$ as required. □

**Theorem 35.** 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 $G_1 = \mathcal{S}_r \cap H_1$ and $G_2 = H_2 \cap \mathcal{S}_k$, 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 \( \langle \rho \rangle \leq H \), \( \text{fix}_H(\mathcal{B}) \) is semiregular of order \( k \), where \( \mathcal{B} \) is a complete block system consisting of \( m \) blocks of size \( k \), and \( \langle \rho^m \rangle \leq C(H) \). Suppose that there exists a complete block system \( \mathcal{E} \) with \( \mathcal{B} \triangleleft \mathcal{E} \) and \( H' \triangleleft H' \) such that \( \langle \rho \rangle \leq H' \) and \( \text{fix}_{H'}(\mathcal{E}) \) is semiregular of order, say \( k' \), where \( k | k' \). Note then that \( \text{fix}_{H'}(\mathcal{E}) = \langle \rho^{mk/k'} \rangle \leq N(mk) \). By Lemma 34, \( \text{fix}_H(\mathcal{E}) \leq N(mk) \), and again by Lemma 34, \( \text{fix}_G(\mathcal{E}) \leq N(mk) \). But then by Lemma 33 there exists \( H'' \triangleleft G \) such that \( \langle \rho \rangle \leq H'' \), \( \text{fix}_{H''}(\mathcal{E}) \) is semiregular, and \( \text{fix}_{H''}(\mathcal{E}) = \langle \rho^{mk/k} \rangle \leq C(H'') \), contradicting our original choice of \( k \). Hence if \( \mathcal{E} \triangleleft \mathcal{B} \) and \( H' \triangleleft H \) with \( \langle \rho \rangle \leq H' \), then \( \text{fix}_{H'}(\mathcal{E}) \) is not semiregular.

We have now established the conditions of Lemma 27 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 \( \text{fix}_H(\mathcal{D}) \) is not of order \( |D| \), \( D \in \mathcal{D} \), and there exists no nontrivial block system \( \mathcal{E} \) of \( H \) such that \( \mathcal{E} \triangleleft \mathcal{D} \); 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 \( |\text{fix}_{H^{(2)}}(\mathcal{D}')| \).

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

In the second case, by Lemma 30, \( \mathcal{D} \) is a complete block system of \( G \). Since \( H \) has no nontrivial complete block system \( \mathcal{E} \) such that \( \mathcal{E} \triangleleft \mathcal{D} \) 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 \( \mathcal{E} \triangleleft \mathcal{D} \). Thus \( |\text{fix}_G(\mathcal{D})| > |D| \), \( D \in \mathcal{D} \). Now by Lemma 29, one of the conclusions of this theorem holds.

In the third case, since \( G \) is 2-closed and \( H \triangleleft G \), we have \( H^{(2)} \leq G \), so \( q^2 \) divides \( |\text{fix}_G(\mathcal{D}')| \). Since \( \text{fix}_H(\mathcal{D}') \leq \text{fix}_H(\mathcal{B}) = \langle \rho^m \rangle \leq N(mk) \), Lemma 34 gives \( \text{fix}_G(\mathcal{D}') \leq N(mk) \), a contradiction. \( \square \)

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 35.

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

**Corollary 36.** 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 \( H_1 \triangleleft \mathcal{F}_m \) is 2-closed and \( H_2 \triangleleft \mathcal{F}_k \) 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 [24] and \( \langle \rho \rangle = (\mathbb{Z}_{mk})_L \leq H \), there exists \( h_1 \in H \) such that \( h_1^{-1}g^{-1}(\rho)gh_1 = (\rho) \). 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. \( \square \)
References