CLONES CLOSED UNDER CONJUGATION I: CLONES WITH CONSTANTS

KEITH A. KEARNES AND ÁGNES SZENDREI

ABSTRACT. We show that if $G \leq \mathsf{S}_A$ is a permutation group on a finite set A satisfying $|A| \geq 3$, then the set of G-closed clones on A that contain all constant operations is finite if and only if $G = \mathsf{S}_A$, A_A, $\mathsf{AGL}(1,5)$ ($|A| = 5$), $\mathsf{PSL}(2,5)$ ($|A| = 6$), $\mathsf{PGL}(2,5)$ ($|A| = 6$), $\mathsf{PGL}(2,7)$ ($|A| = 8$), $\mathsf{PGL}(2,8)$ ($|A| = 9$), or $\mathsf{P\Gamma L}(2,8)$ ($|A| = 9$).

1. INTRODUCTION

The group S_A of all permutations of A acts on the relations on A by the rule: if $\rho \subseteq A^n$ and $\gamma \in \mathsf{S}_A$, then $\gamma(\rho) := \{\big(\gamma(a_1), \ldots, \gamma(a_n)\big) : (a_1, \ldots, a_n) \in \rho\} \subseteq A^n$. If ρ is the graph of an operation $f\colon A^k \to A$, then $\gamma(\rho)$ is the graph of the *conjugate operation* $\gamma\big(f(\gamma^{-1}(x_1), \ldots, \gamma^{-1}(x_k))\big)$, which will be denoted by ${}^\gamma f$ in this paper.

A *clone* on A is a collection $\mathfrak{C}$ of operations on A that is closed under composition and contains the projection operations. If $\gamma \in \mathsf{S}_A$ and $\mathfrak{C}$ is a clone on A, then ${}^\gamma\mathfrak{C} := \{{}^\gamma f : f \in \mathfrak{C}\}$ is also a clone on A. We say that $\mathfrak{C}$ is *G-closed* for a subgroup $G \leq \mathsf{S}_A$ if ${}^\gamma\mathfrak{C} = \mathfrak{C}$ for all $\gamma \in G$. This paper is the first of two which together answer the question: for which permutation groups $G \leq \mathsf{S}_A$ on a finite set A are there only finitely many G-closed clones? We not only identify which groups G have this property, but we also identify the corresponding G-closed clones.

Clones arise in algebra. If $\mathbf{A} = (A; F)$ is an algebra, then the closure of F under composition is the *clone of* $\mathbf{A}$, denoted by $\mathrm{Clo}(\mathbf{A})$. Every clone $\mathfrak{C}$ on A arises as the clone of some algebra, e.g. of $(A; \mathfrak{C})$. Two algebras on A that have the same clone are called *term equivalent*. Conjugation by some $\gamma \in \mathsf{S}_A$ fixes $\mathrm{Clo}(\mathbf{A})$ pointwise precisely when γ is an automorphism of $\mathbf{A}$. Therefore it is standard to call γ a *weak automorphism* of $\mathbf{A}$ if conjugation by γ fixes $\mathrm{Clo}(\mathbf{A})$ setwise. In this terminology, $\mathrm{Clo}(\mathbf{A})$ is G-closed precisely when $G \leq \mathrm{WAut}(\mathbf{A})$. From this point of view, our paper may be described in approximate terms as (the first half of) a classification of all finite algebras that have a high degree of homogeneity. Here $\mathbf{A}$ has "a high degree

1991 *Mathematics Subject Classification.* Primary 08A05, Secondary 08A40, 08A35, 03B50.

Key words and phrases. Clone, conjugation, weak automorphism.

This material is based upon work supported by the Hungarian National Foundation for Scientific Research (OTKA) grants no. T 034175 and T 037877.

of homogeneity" if $\mathrm{WAut}(\mathbf{A})$ is so large that only finitely many term inequivalent algebras on A have the same weak automorphism group.

The principal antecedents to this paper in chronological order are:

- [18] by Emil Post, which classifies all clones on a 2-element set. This result allows us to focus exclusively on the cases $|A| \geq 3$ in the present paper.
- [13] by S. S. Marchenkov, which classifies up to term equivalence all finite algebras satisfying $\mathrm{Aut}(\mathbf{A}) = \mathsf{S}_A$.
- [7] by Nguen van Hoa, which proves that there are finitely many S_A-closed clones when $|A| = 3$.
- [8, 9] by Hoa and [14] by Marchenkov, which prove that there are finitely many S_A-closed clones when $4 \leq |A| < \omega$.
- [15, 16] by Marchenkov, which proves that there are finitely many A_A-closed clones when $4 \leq |A| < \omega$.
- [20] by László Szabó, which provides a coarse description of the lattice of G-closed clones ordered by inclusion, when G acts 2-homogeneously on A.

Our results may be viewed as completing the line of research of the last four items on this list.

It follows from the coarse description of the lattice of G-closed clones for 2-homogeneous groups in [20] that almost any such clone contains all constant operations or consists entirely of idempotent operations. Consequently the classification of these clones divides naturally into these two main cases, one of which is handled in this paper while the other will be handled in its successor.

The results of this paper were announced in [23].

2. The main theorem

Let $G \leq \mathsf{S}_A$ be a permutation group acting on a finite set A. G is *k-homogeneous* if for any k-element subsets C and C' of A there exists $\gamma \in G$ such that $C' = \gamma(C)$; i.e., if the action of G on the k-element subsets of A is transitive.

In this paper we will need a weaker notion. Call G *weakly k-homogeneous* if it has the following property.

(WH_k) For every $(k+1)$-element subset B of A, and for every k-element subset C of B, there exists a k-element subset C' of B such that $C' \neq C$ and $C' = \gamma(C)$ for some $\gamma \in G$.

Call G *weakly homogeneous* if it is weakly k-homogeneous for every k $(1 \leq k < |A|)$.

It is clear that if G is k-homogeneous, then it is also weakly k-homogeneous. The converse is true when $k \leq 2$:

Lemma 2.1. *Let G be a permutation group acting on a finite set A $(|A| \geq 3)$.*

(1) *G is weakly 1-homogeneous if and only if it is 1-homogeneous if and only if it is transitive.*

(2) *G is weakly 2-homogeneous if and only if it is 2-homogeneous.*

Proof. The first statement is an immediate consequence of the definitions. The second statement only has content when $|A| \geq 3$, so assume this and that G is weakly 2-homogeneous. If $B = \{1, 2, 3\}$ is a 3-element subset of A, then by weak 2-homogeneity $\{1, 2\}$ lies in the same G-orbit as some other 2-element subset of B, say $\{1, 3\}$. But the third 2-element subset, $\{2, 3\}$, also lies in the same G-orbit as some different 2-element subset of B, which must be either $\{1, 2\}$ or $\{1, 3\}$. Hence all 2-element subsets of B (or of any 3-element subset of A) lie in the same G-orbit. This shows that if $\{a, b\}$ and $\{c, d\}$ are 2-element subsets of A and $|\{a, b, c, d\}| \neq 4$, then $\{a, b\}$ and $\{c, d\}$ lie in the same G-orbit. On the other hand, if $|\{a, b, c, d\}| = 4$, then $\{a, b\}$ and $\{c, d\}$ are each in the same G-orbit as $\{a, c\}$, so G is indeed 2-homogeneous. □

The main result of this paper is the following theorem.

Theorem 2.2. *For a permutation group G acting on a finite set A ($|A| \geq 3$) the following conditions are equivalent.*

(i) *The number of G-closed clones that contain all constants is finite.*
(ii) *G is weakly homogeneous.*
(iii) *G is one of the following groups:*
- A_n, S_n ($|A| = n \geq 3$),
- $\mathsf{AGL}(1, 5)$ ($|A| = 5$),
- $\mathsf{PSL}(2, 5)$, $\mathsf{PGL}(2, 5)$ ($|A| = 6$),
- $\mathsf{PGL}(2, 7)$ ($|A| = 8$),
- $\mathsf{PGL}(2, 8)$, $\mathsf{P\Gamma L}(2, 8)$ ($|A| = 9$).

Since all groups that are k-homogeneous for every k are weakly homogeneous, the equivalence of conditions (ii) and (iii) in Theorem 2.2 extends the following classical theorem, the main results of [1].

Theorem 2.3. *The permutation groups that act on a finite set A ($|A| \geq 3$) k-homogeneously for every k ($1 \leq k < |A|$) are the following:*
- A_n, S_n ($|A| = n \geq 3$),
- $\mathsf{AGL}(1, 5)$ ($|A| = 5$),
- $\mathsf{PGL}(2, 5)$ ($|A| = 6$),
- $\mathsf{PGL}(2, 8)$, $\mathsf{P\Gamma L}(2, 8)$ ($|A| = 9$).

Theorem 2.2 is concerned only with G-closed clones that contain all constants. Therefore we will now briefly discuss what is known about G-closed clones that don't contain all constants. Throughout this discussion we will assume that $|A| \geq 3$ and that G is 2-homogeneous, a property shared by all groups in Theorem 2.2 (see Lemma 2.1).

We will use the following notation. If F is a set of operations on A, $\langle F \rangle$ will denote the clone generated by F. The set of unary constant operations on A will be denoted

by C_A. For an algebra $\mathbf{A}$, $\mathbf{A}^{\mathrm{c}}$ will stand for the expansion of $\mathbf{A}$ by all constants. If $\mathfrak{C}$ is a clone on A, $\mathfrak{C}^{(n)}$ will denote the set of n-ary operations in $\mathfrak{C}$, and $\mathfrak{C}^{\mathrm{c}}$ the clone generated by $\mathfrak{C} \cup \mathsf{C}_A$. Let $\underline{A}$ be an abelian group. The group of all translations of $\mathbf{A}$ is denoted by $\mathsf{TR}(\underline{A})$. For an R-module ${}_R\underline{A}$ with underlying abelian group $\underline{A}$, ${}_R\underline{A}^{\mathrm{id}}$ will denote the corresponding affine module (whose clone consists of all idempotent term operations of ${}_R\underline{A}$), and ${}_R\underline{A}^{\mathrm{tr}}$ will denote the expansion of ${}_R\underline{A}^{\mathrm{id}}$ by all translations of $\underline{A}$.

Lemma 2.4. *Let G be a permutation group acting 2-homogeneously on a finite set A ($|A| \geq 3$). Let $\mathfrak{C}$ be a G-closed clone on A, and let $\mathbf{A} = (A; \mathfrak{C})$.*

(1) $G \leq \mathrm{WAut}(\mathbf{A})$, *hence* $\mathrm{WAut}(\mathbf{A})$ *is 2-homogeneous;*
(2) $\mathfrak{C}^{(1)} \cap \mathsf{S}_A$ *and* $\mathrm{Aut}(\mathbf{A})$ *are normal subgroups of* $\mathrm{WAut}(\mathbf{A})$*;*
(3) *either* $\mathfrak{C}^{(1)} \leq \mathsf{S}_A$ *or* $\mathsf{C}_A \subseteq \mathfrak{C}^{(1)}$*;*
(4) $\mathrm{WAut}(\mathbf{A}) \leq \mathrm{WAut}(\mathbf{A}^{\mathrm{c}})$*;*
(5) *if* $\mathbf{A}$ *is not simple, then* $\mathfrak{C}^{(1)} \subseteq \mathsf{S}_A \cup \mathsf{C}_A$.

Proof. Items (1), (2), and (4) follow from the definition of weak automorphism.

For item (3), assume that $\mathfrak{C}^{(1)} \not\leq \mathsf{S}_A$, and let $f \in \mathfrak{C}^{(1)}$ be a non-permutation, say $f(a) = f(b)$ for some distinct $a, b \in A$. If f is not constant, say $f(c) \neq f(d)$ for some $c, d \in A$, then by 2-homogeneity there exists $\gamma \in G$ such that γ maps $\{a, b\}$ onto $\{f(c), f(d)\}$. Hence ${}^{\gamma}f \circ f$ has smaller range than f. This implies that a non-permutation in $\mathfrak{C}$ with smallest possible range is a constant operation. Since $\mathfrak{C}$ is G-closed and G is transitive on A, it follows that $\mathsf{C}_A \subseteq \mathfrak{C}^{(1)}$.

For (5), the 2-homogeneity of G implies that G acts transitively on the principal congruences $\Theta(a, b)$ ($a, b \in A$, $a \neq b$) of $\mathbf{A}$. Thus all principal congruences are minimal. Assume that $\mathfrak{C}^{(1)}$ contains an operation f that is neither constant nor a permutation. Let B be a kernel class of f with more than one element, and let $C = A - B$; $C \neq \emptyset$ because f is not constant. For any $c \in C$ and distinct $a, b \in B$ we have $f(a) = f(b) \neq f(c)$ and $\Theta(a, c) \cap \Theta(b, c) \supseteq \Theta\big(f(a), f(c)\big) = \Theta\big(f(b), f(c)\big)$. So the minimality of the principal congruences yields that $\Theta(a, c) = \Theta(b, c) = \Theta(a, b)$. Since this holds for arbitrary $c \in C$, we also get that $\Theta(b, d) = \Theta(b, c) = \Theta(c, d)$ for all distinct $c, d \in C$ (if any). This implies that all principal congruences coincide, that is, $\mathbf{A}$ is simple, which contradicts our hypothesis. This completes the proof of the lemma. □

Theorem 2.5. *If G is a permutation group that acts 2-homogeneously on a finite set A ($|A| \geq 3$), then one of the following conditions holds for any G-closed clone $\mathfrak{C}$ on A:*

(a) $\mathfrak{C}^{(1)}$ *contains all constants and an operation that is neither constant nor a permutation; moreover, the algebra $(A; \mathfrak{C})$ is simple;*
(b) $\mathfrak{C}$ *is an idempotent clone such that the algebra $(A; \mathfrak{C})$ is simple;*

(c) $\mathfrak{C}$ *is the clone of a quasiprimal algebra with no proper subalgebras, whose automorphism group is* $\mathsf{TR}(\underline{A})$ *for some elementary abelian group* $\underline{A}$ *on* A*;*
(d) $\mathfrak{C} = \mathrm{Clo}({}_R\underline{A}^{\mathrm{tr}})$ *where* $\underline{A}$ *is an elementary abelian group on* A *and* $R = \mathrm{End}({}_K\underline{A})$ *for a subfield* K *of* $\mathrm{End}(\underline{A})$*;*
(e) $\mathfrak{C} = \mathrm{Clo}({}_K\underline{A}^{\mathrm{id}})$*,* $\mathfrak{C} = \mathrm{Clo}({}_K\underline{A}^{\mathrm{tr}})$*, or* $\mathfrak{C} = \mathrm{Clo}({}_K\underline{A}^{\mathrm{c}}) = \mathrm{Pol}({}_K\underline{A})$ *for a vector space* ${}_K\underline{A}$ *on* A*;*
(f) $\mathfrak{C} = \langle M \rangle$ *or* $\mathfrak{C} = \langle M \cup \mathsf{C}_A \rangle$ *for a permutation group* $M \leq \mathsf{S}_A$ *whose normalizer* $N_{\mathsf{S}_A}(M)$ *is 2-homogeneous.*

In each case (a)–(f) above, G is a subgroup of the weak automorphism group of the algebra $(A; \mathfrak{C})$ (see Lemma 2.4 (1)). In case (c) the weak automorphism group is $\mathsf{AGL}(\mathbb{F}_p\underline{A})$, in cases (d) and (e) it is $\mathsf{AGL}({}_K\underline{A})$, while in case (f) it is $N_{\mathsf{S}_A}(M)$.

Proof of Theorem 2.5. Let $\mathbf{A}$ denote the algebra $(A; \mathfrak{C})$. Then $\mathrm{Clo}(\mathbf{A}) = \mathfrak{C}$ and $\mathrm{Clo}(\mathbf{A}^{\mathrm{c}}) = \mathfrak{C}^{\mathrm{c}}$. By assumption $\mathfrak{C}$ is G-closed, that is, $G \leq \mathrm{WAut}(\mathbf{A})$. Therefore by Lemma 2.4 (4), $\mathfrak{C}^{\mathrm{c}}$ is also G-closed. We also know from Lemma 2.4 (2) that $M = \mathfrak{C}^{(1)} \cap \mathsf{S}_A$ is a normal subgroup of $\mathrm{WAut}(\mathbf{A})$. Since $\mathrm{WAut}(\mathbf{A})$ acts 2-homogeneously on A, it follows that either M is the trivial group $\{\mathrm{id}\}$ or M acts transitively on A.

Assume first that $(\mathfrak{C}^{\mathrm{c}})^{(1)} \subseteq \mathsf{S}_A \cup \mathsf{C}_A$. Then, by Pálfy's Theorem [17], either $\mathfrak{C}^{\mathrm{c}} = \mathrm{Pol}({}_K\underline{A})$, the polynomial clone of a vector space ${}_K\underline{A}$ on A, or else $\mathfrak{C}$ is the polynomial clone of a unary algebra on A; in the latter case $\mathfrak{C} = \langle \mathfrak{C}^{(1)} \rangle$ and $\mathfrak{C}^{(1)} \subseteq (\mathfrak{C}^{\mathrm{c}})^{(1)}$, hence $\mathfrak{C}^{(1)} \subseteq M \cup \mathsf{C}_A$ and $\mathfrak{C}^{\mathrm{c}} = \langle \mathfrak{C}^{(1)} \cup \mathsf{C}_A \rangle = \langle M \cup \mathsf{C}_A \rangle$. According to Lemma 2.4 (3), we will distinguish two cases. First let $\mathsf{C}_A \subseteq \mathfrak{C}^{(1)}$. Then $\mathfrak{C}^{\mathrm{c}} = \mathfrak{C}$, hence it follows from the facts established so far that $\mathfrak{C}$ is one of the clones in (e) or (f). Now let $\mathfrak{C}^{(1)} \leq \mathsf{S}_A$, that is, $\mathfrak{C}^{(1)} = M$. If $\mathfrak{C}^{\mathrm{c}} = \langle M \cup \mathsf{C}_A \rangle$, then $\mathfrak{C} = \langle \mathfrak{C}^{(1)} \rangle = \langle M \rangle$, so $\mathfrak{C}$ is among the clones in (f). If $\mathfrak{C}^{\mathrm{c}} = \mathrm{Pol}({}_K\underline{A})$, then the description of the subclones of $\mathrm{Pol}({}_K\underline{A})$ in [21] (Proposition 2.9) yields that $\mathrm{Clo}({}_K\underline{A}^{\mathrm{id}}) \subseteq \mathfrak{C} \subseteq \mathrm{Pol}({}_K\underline{A})$; moreover, if $M = \{\mathrm{id}\}$ then $\mathfrak{C} = \mathrm{Clo}({}_K\underline{A}^{\mathrm{id}})$, while if M is a transitive permutation group on A then $M = \mathsf{TR}(\underline{A})$ and $\mathfrak{C} = \mathrm{Clo}({}_K\underline{A}^{\mathrm{tr}})$. In both cases $\mathfrak{C}$ is among the clones listed in (e).

Now assume that $(\mathfrak{C}^{\mathrm{c}})^{(1)} \not\subseteq \mathsf{S}_A \cup \mathsf{C}_A$. By Lemma 2.4 (5) the algebra $\mathbf{A}^{\mathrm{c}} = (A; \mathfrak{C}^{\mathrm{c}})$ must be simple. Hence $\mathbf{A} = (A; \mathfrak{C})$ is also simple. Again, we distinguish two cases according to Lemma 2.4 (3). If $\mathsf{C}_A \subseteq \mathfrak{C}^{(1)}$, then the conditions in (a) hold for $\mathfrak{C}$. Now let $\mathfrak{C}^{(1)} \leq \mathsf{S}_A$, that is, $\mathfrak{C}^{(1)} = M$. If $M = \{\mathrm{id}\}$ then $\mathfrak{C}$ satisfies condition (b). Finally, if M is a transitive permutation group on A, then the simple algebra $\mathbf{A} = (A; \mathfrak{C})$ has no proper subalgebras, and $\mathrm{Clo}^{(1)}(\mathbf{A}) = M$ is a permutation group. It was proved in [22] (Corollary 3.7 and Claims 3.8–3.9) that in this case either

— $\mathbf{A}$ is essentially unary and hence $\mathfrak{C} = \langle \mathfrak{C}^{(1)} \rangle = \langle M \rangle$ satisfies condition (f), or
— $\mathfrak{C} = \mathrm{Clo}(\mathbf{A}) = \mathrm{Clo}({}_R\underline{A}^{\mathrm{tr}})$ for an R-module ${}_R\underline{A}$ as in (d), or else
— $\mathbf{A}$ is a quasiprimal algebra such that $\mathrm{Aut}(\mathbf{A})$ acts regularly on A.

In the last case $\mathrm{Aut}(\mathbf{A})$ is a normal subgroup of $\mathrm{WAut}(\mathbf{A})$ by Lemma 2.4 (2), and $\mathrm{WAut}(\mathbf{A})$ acts 2-homogeneously on A as $G \leq \mathrm{WAut}(\mathbf{A})$. By Burnside's Theorem (see Theorem 4.2) a minimal normal subgroup of a finite 2-homogeneous permutation group is either elementary abelian and regular, or simple and primitive. This conclusion holds, in particular, for a minimal normal subgroup N of $\mathrm{WAut}(\mathbf{A})$ that is contained in $\mathrm{Aut}(\mathbf{A})$. Since $\mathrm{Aut}(\mathbf{A})$ is regular and $N \leq \mathrm{Aut}(\mathbf{A})$, therefore N must be regular. Hence we get that $N = \mathrm{Aut}(\mathbf{A})$ and $\mathrm{Aut}(\mathbf{A})$ is elementary abelian. Thus $\mathrm{Aut}(\mathbf{A}) = \mathsf{TR}(\underline{A})$ for some elementary abelian group $\underline{A}$ with universe A. This concludes the proof that $\mathfrak{C}$ satisfies condition (c).

The proof of Theorem 2.5 is complete. □

The result in Theorem 2.5 on G-closed clones for 2-homogeneous G will be sufficient for our purposes, but it is not the sharpest result known about these clones. In [20] Szabó describes the coarse structure of the lattice of G-closed clones on a finite set A ($|A| \geq 3$) under the weaker assumption that G acts primitively on A. For the case when G is 2-homogeneous, his description yields that in addition to what is stated in Theorem 2.5, if $\mathfrak{C}$ is a G-closed clone that belongs to class (a), then one of the following conditions holds:

- (a)$_1$ $\mathfrak{C}$ is the clone of all operations, or
- (a)$_2$ $\mathfrak{C} = \mathrm{Clo}({}_R\underline{A}^{\mathrm{c}}) = \mathrm{Pol}({}_R\underline{A})$ where $\underline{A}$ is an elementary abelian group on A and $R = \mathrm{End}({}_K\underline{A})$ for a subfield K of $\mathrm{End}(\underline{A})$, or
- (a)$_3$ $\mathfrak{C}$ is contained in the Słupecki clone $\mathfrak{R}_{|A|-1} \cup \langle \mathsf{T}_A \rangle$ (see notation in Section 6).

It is easy to see that for each 2-homogeneous permutation group G on a finite set A there are only finitely many G-closed clones $\mathfrak{C}$ that satisfy any one of conditions (c)–(f) in Theorem 2.5. Therefore the lattice of G-closed clones is finite if and only if

- the lattice of G-closed clones containing all constants, and
- the lattice of idempotent G-closed clones

are both finite.

Since all weakly homogeneous groups are 2-homogeneous (see Lemma 2.1), the observation in the preceding paragraph yields that the assumption in Theorem 2.2 that the clones contain all constants can be replaced by the weaker condition that the clones are non-idempotent:

Corollary 2.6. *For a permutation group G acting on a finite set A ($|A| \geq 3$) the following conditions are equivalent.*

- (i) *There are only finitely many non-idempotent G-closed clones.*
- (ii) *G is weakly homogeneous.*
- (iii) *G is one of the groups listed in Theorem 2.2 (iii).*

The idempotent G-closed clones for weakly homogeneous groups G will be discussed in a forthcoming paper.

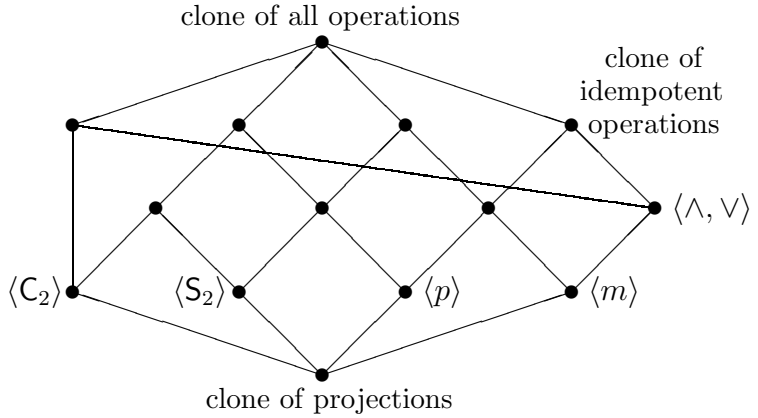

FIGURE 1. S_2-closed clones on $\{0,1\}$

Since the case $|A| = 2$ is excluded by the assumptions in Theorem 2.2 as well as in Corollary 2.6, let us mention the analogues of these statements for the case when the base set A has only two elements. Note first that among the two permutation groups on A the two-element group S_2 is weakly homogeneous, while the one-element group A_2 is not weakly homogeneous.

Post's classification of all clones on a 2-element set (see [18]) yields that there are only fourteen S_2-closed clones on $A = \{0,1\}$. Figure 1 shows the lattice of all these clones. In the diagram $\wedge, \vee$ denote the lattice operations, $m(x,y,z) = (x \wedge y) \vee (x \wedge z) \vee (y \wedge z)$ is the unique majority operation, and $p(x,y,z) = x + y + z$ is the unique minority operation on $\{0,1\}$. It is easily seen from Figure 1 that there are eight non-idempotent S_2-closed clones on $\{0,1\}$. On the other hand, there are infinitely many non-idempotent A_2-closed clones on $\{0,1\}$. This shows that the equivalence of conditions (i) and (ii) in Corollary 2.6 remains true for $|A| = 2$.

However, conditions (i) and (ii) in Theorem 2.2 are not equivalent if $|A| = 2$. The reason is that there are only seven clones on $\{0,1\}$ that contain both constants. Figure 2 shows the lattice of these clones. All these clones are G-closed for the 1-element group $G = \mathsf{A}_2$, and the ones denoted by bullets rather than black triangles (i.e. those that also appear in Figure 1) are G-closed for $G = \mathsf{S}_2$ as well.

The rest of the paper is devoted to the proof of Theorem 2.2. In Sections 3, 4, and 6 we will prove the implications (i) $\Rightarrow$ (ii), (ii) $\Leftrightarrow$ (iii), and (iii) $\Rightarrow$ (i), respectively. In particular, the implication (iii) $\Rightarrow$ (i) will be proved by explicitly describing, for each weakly homogeneous group G acting on a finite set A ($|A| \geq 3$), all G-closed clones $\mathfrak{C}$ that contain all constants. For all such G, this description can be combined with the description of the clones in Theorem 2.5 (c)–(f) to get a description of all non-idempotent G-closed clones as well.

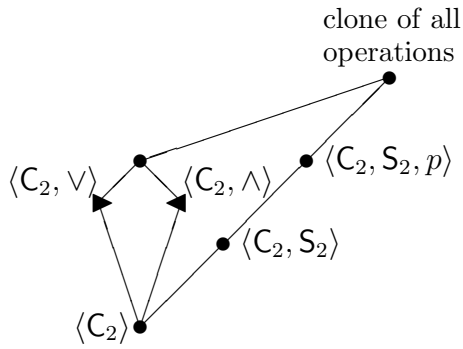

FIGURE 2. Clones on $\{0,1\}$ that contain both constants

3. The necessity of weak homogeneity

In this section we establish the implication (i)⇒(ii) in Theorem 2.2 by proving the following theorem.

Theorem 3.1. *Let G be a permutation group acting on a finite set A ($|A| \geq 3$). If G is not weakly homogeneous, then there exists an infinite descending chain of G-closed clones on A that contain all constants.*

Proof. For an arbitrary relation ρ on A let $\mathfrak{C}(\rho)$ denote the set of all operations f on A such that f preserves the relation ρ (that is, ρ is a subalgebra of the algebra $(A; f)^n$ where n is the arity of ρ).

Claim 3.2. *Let ρ be a relation on A. Then*

(1) *$\mathfrak{C}(\rho)$ is a clone on A, and*
(2) *${}^{\gamma}\big(\mathfrak{C}(\rho)\big) = \mathfrak{C}\big(\gamma(\rho)\big)$ holds for each permutation γ on A.*

It is straightforward to check that $\mathfrak{C}(\rho)$ contains the projection operations and is closed under composition; therefore it is a clone, proving (1). Now let γ be a permutation on A. For every operation f on A, ${}^{\gamma}f$ preserves $\gamma(\sigma)$ if and only if f preserves ρ. Therefore

$$ {}^{\gamma}\big(\mathfrak{C}(\rho)\big) = \{{}^{\gamma}f : f \text{ preserves } \rho\} = \{{}^{\gamma}f : {}^{\gamma}f \text{ preserves } \gamma(\rho)\} = \mathfrak{C}\big(\gamma(\rho)\big), $$

since every operation is of the form ${}^{\gamma}f$ for some operation f. This completes the proof of (2).

Now assume that G is not weakly homogeneous. This means that there is some number $1 \leq k < |A|$ such that (WH_k) fails. In fact, since every weakly 2-homogeneous group is 2-homogeneous (Lemma 2.1), every 2-homogeneous group on a set A of size at least 3 is transitive, and every transitive group is weakly 1-homogeneous, there must exist such a k satisfying $2 \leq k < |A|$. Fix a witness of the failure of (WH_k) for

such a k, i.e., fix a k-element subset C of A, and a $(k+1)$-element subset $B = C \cup \{0\}$ of A so that $\gamma(C) \neq C'$ for every $\gamma \in G$ and for every k-element subset C' of B that contains 0. For notational simplicity let us assume that $C = \{1, 2, \ldots, k\}$.

Using these sets we define an infinite sequence ρ_n $(n = 2, 3, \ldots)$ of relations and an infinite sequence f_n $(n = 3, 4, \ldots)$ of operations on A as follows:

- ρ_n is the $(n + k - 1)$-ary relation consisting of all tuples
$$(a_1, \ldots, a_n, b_1, \ldots, b_{k-1}) \in A^{n+k-1}$$
such that
  - $|\{a_1, \ldots, a_n, b_1, \ldots, b_{k-1}\}| \leq k + 1$ and
  - $|\{a_1, \ldots, a_n\}| \geq 2$ if $\{a_1, \ldots, a_n, b_1, \ldots, b_{k-1}\} = \gamma(C)$ for some $\gamma \in G$;
- f_n is the n-ary operation on A such that
$$\begin{aligned} f_n(1, \ldots, 1, \overbrace{0}^{j\text{th position}}, 1, \ldots, 1) &= 1 \quad \text{for every } j \ (1 \leq j \leq n), \\ f_n(c, \ldots, c) &= c \quad \text{for } c = 2, \ldots, k, \text{ and} \\ f_n(x_1, \ldots, x_n) &= 0 \quad \text{for all remaining arguments.} \end{aligned}$$

Claim 3.3. *$\mathfrak{C}(\rho_n)$ is a G-closed clone for each $n \geq 2$, and it contains all constants.*

Let $n \geq 2$. Since $\gamma(\rho_n) = \rho_n$ for all $\gamma \in G$, it follows immediately from Claim 3.2 that $\mathfrak{C}(\rho_n)$ is a clone on A such that ${}^{\gamma}\big(\mathfrak{C}(\rho_n)\big) = \mathfrak{C}(\rho_n)$ for all $\gamma \in G$. Thus $\mathfrak{C}(\rho_n)$ is a G-closed clone. The fact that the relation ρ_n is reflexive yields that $\mathfrak{C}(\rho_n)$ contains all constants.

Claim 3.4. *$\mathfrak{C}(\rho_{n-1}) \supseteq \mathfrak{C}(\rho_n)$ for all $n \geq 3$.*

Using the definitions of ρ_{n-1} and ρ_n one can easily check that

$$(a_1, \ldots, a_{n-1}, b_1, \ldots, b_{k-1}) \in \rho_{n-1} \quad \Leftrightarrow \quad (a_1, \ldots, a_{n-1}, a_{n-1}, b_1, \ldots, b_{k-1}) \in \rho_n.$$

This implies that every operation that preserves ρ_n also preserves ρ_{n-1}, completing the proof of Claim 3.4.

Claim 3.5. *$f_n \in \mathfrak{C}(\rho_{n-1}) - \mathfrak{C}(\rho_n)$ for all $n \geq 3$.*

To see that $f_n \notin \mathfrak{C}(\rho_n)$ notice the following: the $(n + k - 1)$-tuples

$$e_j = (\underbrace{1, \ldots, 1, \overbrace{0}^{j\text{th position}}, 1, \ldots, 1}_{\text{first } n \text{ positions}}, \underbrace{2, 3, \ldots, k}_{\text{last } k-1 \text{ positions}}) \qquad (1 \leq j \leq n)$$

all belong to ρ_n; however, f_n applied to these elements of ρ_n yields the $(n+k-1)$-tuple

$$f_n(e_1, \ldots, e_n) = (\underbrace{1, \ldots, 1}_{\text{first } n \text{ positions}}, \underbrace{2, 3, \ldots, k}_{\text{last } k-1 \text{ positions}})$$

which fails to belong to ρ_n, since the set of components is $\{1, 2, \dots, k\} = C = \gamma(C)$ for $\gamma = \mathrm{id}$, but the set of the first n components is a singleton. Thus f_n fails to preserve ρ_n, so $f_n \notin \mathfrak{C}(\rho_n)$.

It remains to show that f_n preserves ρ_{n-1}, and hence $f_n \in \mathfrak{C}(\rho_{n-1})$. Let $v_1, \dots, v_n$ be arbitrary $(n-1+k-1)$-tuples such that $f_n(v_1, \dots, v_n) \notin \rho_{n-1}$. We have to verify that at least one of $v_1, \dots, v_n$ fails to belong to ρ_{n-1}. Let

$$f_n(v_1, \dots, v_n) = (a_1, \dots, a_{n-1}, b_1, \dots, b_{k-1}).$$

Since the range of f_n is the $(k+1)$-element set $\{0, 1, 2, \dots, k\} = B = C \cup \{0\}$, we have

$$\{a_1, \dots, a_{n-1}, b_1, \dots, b_{k-1}\} \subseteq C \cup \{0\}.$$

Thus $f_n(v_1, \dots, v_n) \notin \rho_{n-1}$ implies that

$$a_1 = \cdots = a_{n-1} \qquad \text{and} \qquad \{a_1, \dots, a_{n-1}, b_1, \dots, b_{k-1}\} = \gamma(C)$$

for some $\gamma \in G$. By our choice of B and C we have $\gamma(C) \neq C'$ for every $\gamma \in G$ and for every k-element subset C' of B that contains 0. Hence

$$\{a_1, \dots, a_{n-1}, b_1, \dots, b_{k-1}\} = C = \{1, 2, \dots, k\}.$$

Thus $f_n(v_1, \dots, v_n) = (a, \dots, a, b_1, \dots, b_{k-1})$ where $1 \leq a \leq k$ and $b_1, \dots, b_{k-1}$ is a permutation of the elements $1, \dots, a-1, a+1, \dots, k$. Since the roles of $2, \dots, k$ are symmetric in the operation f_n, and ρ_n is invariant under permuting its last $k-1$ coordinates, we may assume without loss of generality that

$$f_n(v_1, \dots, v_n) = (\underbrace{1, \dots, 1}_{\text{first } n-1 \text{ positions}}, \underbrace{2, 3, \dots, k}_{\text{last } k-1 \text{ positions}}) \tag{3.1}$$

or

$$f_n(v_1, \dots, v_n) = (\underbrace{2, \dots, 2}_{\text{first } n-1 \text{ positions}}, \underbrace{1, 3, \dots, k}_{\text{last } k-1 \text{ positions}}). \tag{3.2}$$

Recall from the definition of f_n that for $2 \leq c \leq k$, $f_n(x_1, \dots, x_n) = c$ implies that $x_1 = \cdots = x_n = c$, while $f_n(x_1, \dots, x_n) = 1$ implies that exactly one of $x_1, \dots, x_n$ equals 0 and the others equal 1. Thus, if (3.1) holds, then each $(n-1+k-1)$-tuple $v_1, \dots, v_n$ has last $k-1$ coordinates $2, \dots, k$, and for each $i = 1, \dots, n-1$ exactly one of $v_1, \dots, v_n$ has i-th coordinate 0, all others have i-th coordinate 1. Thus at least one of the $(n-1+k-1)$-tuples $v_1, \dots, v_n$ is $(1, \dots, 1, 2, \dots, k)$, and hence fails to belong to ρ_{n-1}. If (3.2) holds, the argument is similar. In that case each $(n-1+k-1)$-tuple $v_1, \dots, v_n$ has first $n-1$ coordinates $2, \dots, 2$ and last $k-2$ coordinates $3, \dots, k$. Furthermore, exactly one of $v_1, \dots, v_n$ has n-th coordinate 0, all others have n-th coordinates 1. Thus all $v_1, \dots, v_n$ but one is equal to $(2, \dots, 2, 1, 3, \dots, k)$, and hence fails to belong to ρ_{n-1}.

This completes the proof of Claim 3.5.

Claims 3.3–3.5 show that $\mathfrak{C}(\rho_2) \supsetneq \mathfrak{C}(\rho_3) \supsetneq \cdots \supsetneq \mathfrak{C}(\rho_{n-1}) \supsetneq \mathfrak{C}(\rho_n) \supsetneq \cdots$ is an infinite descending chain of G-closed clones that contain all constants. This completes the proof of Theorem 3.1. □

4. Weakly homogeneous permutation groups

The following theorem proves that conditions (ii) and (iii) in Theorem 2.2 are equivalent. The proof begins after the theorem statement, and spans the entire section.

Theorem 4.1. *A permutation group acting on a finite set A ($|A| \geq 3$) is weakly homogeneous if and only if it is one of the following groups:*

- A_n, S_n ($|A| = n \geq 3$),
- $\mathsf{AGL}(1,5)$ ($|A| = 5$),
- $\mathsf{PSL}(2,5)$, $\mathsf{PGL}(2,5)$ ($|A| = 6$),
- $\mathsf{PGL}(2,7)$ ($|A| = 8$),
- $\mathsf{PGL}(2,8)$, $\mathsf{P\Gamma L}(2,8)$ ($|A| = 9$).

Proof. Let G be a permutation group acting on A ($|A| \geq 3$). We will first prove that if G is weakly homogeneous, then it is one of the groups listed in the theorem. Recall from Lemma 2.1 that under the assumption $|A| \geq 3$ which we will adopt, every weakly homogeneous group is 2-homogeneous.

We will use the classification of 2-homogeneous groups. The first step of the classification is based on the following theorem of Burnside.

Theorem 4.2. *If S is a minimal normal subgroup of a 2-homogeneous group $G \leq \mathsf{S}_A$ (A finite), then S is either elementary abelian and regular, or simple and primitive.*

The proof of Burnside's Theorem, under the slightly stronger assumption that G is 2-transitive, can be found in [3] (Theorem 4.3). The proof easily extends to 2-homogeneous groups.

Now let $G \leq \mathsf{S}_A$ be a 2-homogeneous group, and let S be a minimal normal subgroup of G. Then G normalizes S, hence

$$S \leq G \leq \widehat{S} \qquad \text{where } \widehat{S} = N_{\mathsf{S}_A}(S) \text{ is the normalizer of } S \text{ in } \mathsf{S}_A. \tag{4.1}$$

If S is simple and primitive, then a group G satisfying this condition is called *almost simple*.

If S is regular and elementary abelian, then $S = \mathsf{TR}(\underline{A}) = \mathsf{TR}({}_{\mathbb{F}_p}\underline{A})$ for an elementary abelian p-group $\underline{A}$, or equivalently, for a vector space ${}_{\mathbb{F}_p}\underline{A}$ over a prime field. Let $d = \dim {}_{\mathbb{F}_p}\underline{A}$. In this case $\widehat{S}$ is the affine linear group $\mathsf{AGL}(d,p)$. Hence, if S is regular and elementary abelian, then a group G satisfying condition (4.1) is a subgroup of some affine linear group $\mathsf{AGL}(d,p)$ that contains the group of all translations. Such a group G is called an *affine group*.

The first statement in the next corollary follows immediately from Burnside's Theorem. For the second statement, see [11] (Chapter XII, Theorem 6.5).

Corollary 4.3. *Let G be a permutation group acting on a finite set A.*

(1) *If G acts 2-transitively on A, then G is either an affine group or an almost simple group.*
(2) *If G acts 2-homogeneously, but not 2-transitively on A, then G is an affine group.*

To show that any weakly homogeneous group is one of the groups listed in Theorem 4.1 we have to argue that all other 2-homogeneous groups fail to be weakly k-homogeneous (i.e., fail to satisfy (WH_k)) for some k $(3 \leq k < |A|)$. Many of the 2-homogeneous groups are groups of automorphisms of discrete geometries: affine geometries, projective geometries, or, in general, Steiner systems. These groups will fail to be weakly k-homogeneous for some k for the same 'geometric' reason, as shown in Claim 4.4 below.

For other 2-homogeneous groups it will be useful to consider more general set systems than Steiner systems. A *set system* is a pair $(A; \mathcal{S})$ such that $\mathcal{S}$ is a family of subsets of A. An *automorphism of* $(A; \mathcal{S})$ is a permutation $\gamma \in \mathsf{S}_A$ such that $\gamma(X) \in \mathcal{S}$ for all $X \in \mathcal{S}$. A set system $(A; \mathcal{S})$ is called an $\mathrm{S}(k, m, n)$ *Steiner system* if A is an n-element set, $\mathcal{S}$ is a family of m-element subsets of A, and each k-element subset of A is contained in exactly one member of $\mathcal{S}$.

Claim 4.4. *Let $(A; \mathcal{S})$ be a set system such that, for some k,*

(i) *$\mathcal{S}$ contains a set X such that $k < |X| < |A|$ and*
(ii) *each k-element subset of A is contained in at most one member of $\mathcal{S}$.*

If G is a group of automorphisms of $(A; \mathcal{S})$, then (WH_{k+1}) fails for G.

Let C be a $(k+1)$-element subset of a fixed member X of $\mathcal{S}$ satisfying condition (i), and let $u \in A - X$. Let $B = C \cup \{u\}$, and let C' be a $(k+1)$-element subset of B containing u. We claim that C' is not contained in any member of $\mathcal{S}$. Indeed, the assumptions on C' imply that $C' = (C - \{c\}) \cup \{u\}$ for some $c \in C$. Since (ii) holds for $(A; \mathcal{S})$, the only member of $\mathcal{S}$ that contains the k-element set $C - \{c\}$ is X, which does not contain u. Thus, among the $(k+1)$-element subsets of B, C is the only one that is contained in a member of $\mathcal{S}$. Since G is a group of automorphisms of $(A; \mathcal{S})$, each set $\gamma(C)$ $(\gamma \in G)$ in the G-orbit of C will also have the property that it is contained in a member of $\mathcal{S}$. Thus the G-orbit of C contains none of the $(k+1)$-element subsets of B that are distinct from C. This proves that (WH_{k+1}) fails for this choice of B and C.

The special case of Claim 4.4 when $(A; \mathcal{S})$ is a Steiner system is the following.

Claim 4.5. *If G is a group of automorphisms of an $\mathrm{S}(k, m, n)$ Steiner system such that $k < m < n$, then (WH_{k+1}) fails for G.*

First we will apply Claim 4.5 to the affine groups.

Claim 4.6. *For an affine group $G \leq \mathsf{AGL}(d,p)$ ($d \geq 1$, p prime), condition* (WH_3) *or* (WH_4) *fails unless (d,p) is one of the pairs $(1,p)$, $p = 2,3,5$, or $(2,2)$.*

If $d \geq 2$ and $p > 2$ then the family of all lines of the d-dimensional affine geometry over $\mathbb{F}_p$ is an $\mathrm{S}(2,p,p^d)$ Steiner system satisfying $2 < p < p^d$. Moreover, $\mathsf{AGL}(d,p)$ (and hence G) is a group of automorphisms of this Steiner system. It follows from Claim 4.5 that (WH_3) fails for G. Similarly, if $d \geq 3$ and $p = 2$ then the family of all planes of the d-dimensional affine geometry over $\mathbb{F}_2$ is an $\mathrm{S}(3,4,2^d)$ Steiner system satisfying $3 < 4 < 8 \leq p^d$. We get as before that (WH_4) fails for G in this case.

Finally, let $d = 1$, $p \geq 7$. We may assume without loss of generality that $\mathsf{AGL}(1,p)$ acts on $A = \mathbb{F}_p = \{0,1,\ldots,p-1\}$. Let us call a three-element subset of A an isosceles triangle if it is of the form $\{a,(a+b)/2,b\}$ for some $a,b \in A$. Since every permutation in $\mathsf{AGL}(1,p)$ maps isosceles triangles into isosceles triangles, the G-orbit of an isosceles triangle consists of isosceles triangles only. Now, for $p \geq 11$, let $B = \{0,1,2,5\}$ and $C = \{0,1,2\}$. Then C is an isosceles triangle, but none of the other 3-element subsets of B are isosceles triangles. Therefore (WH_3) fails for this choice of B, C. For $p = 7$, let $B = \{0,1,2,4\}$ and $C = \{1,2,4\}$. Then C is not an isosceles triangle, while all other 3-element subsets of B are isosceles triangles. Hence (WH_3) fails for this choice of B, C.

Claim 4.7. *If $G \leq \mathsf{AGL}(d,p)$ is a 2-homogeneous affine group for one of the pairs $(d,p) = (1,2)$, $(1,3)$, $(1,5)$, or $(2,2)$, then G is one of the groups S_n, A_n ($2 \leq n \leq 4$) or $\mathsf{AGL}(1,5)$. All of these groups are weakly homogeneous.*

For $q = p^d = 2,3,4$ we have $\mathsf{AGL}(d,p) = \mathsf{S}_q$, and the group of translations in $\mathsf{AGL}(d,p)$ is A_q for $q = 2,3$, and the Klein group for $q = 4$. It follows that the only 2-homogeneous subgroups of $\mathsf{AGL}(d,p)$ that contain the translations are S_q and A_q. For $q = p^d = 5$, the only 2-homogeneous subgroup of $\mathsf{AGL}(1,5)$ that contains the translations is $\mathsf{AGL}(1,5)$ itself. This shows that G is one of the groups S_n, A_n ($2 \leq n \leq 4$) or $\mathsf{AGL}(1,5)$. All these groups are k-homogeneous, and hence weakly k-homogeneous, for all $k \geq 2$ (cf. Theorem 2.3).

Claims 4.6 and 4.7, combined with Lemma 2.1 prove that the weakly homogeneous affine groups are exactly the affine groups listed in Theorem 4.1. By Lemma 2.1 and Corollary 4.3 the remaining weakly homogeneous groups are all 2-transitive almost simple groups. 2-transitive almost simple groups have been classified ([2], or see Section 4.8 of [3], or Section 7.7 of [5]) by applying the classification of finite simple groups. Table 1 shows the classification of 2-transitive almost simple groups G by indicating the size $|A|$ of the set G acts on, the simple normal subgroup S of G, the index of S in $\widehat{S}$, and the transitivity degree of $\widehat{S}$. These data are taken from [3]. In addition to this we will also need an explicit description of the normalizer $\widehat{S}$, which

is usually easy to determine from S and the index $[\widehat{S} : S]$. We will discuss $\widehat{S}$ in each case separately, as we look at the 2-transitive groups G corresponding to each row of Table 1. The results are summarized in Table 2.

Alternating and symmetric groups (Row 1 of Table 1)

If $S = \mathsf{A}_n$ then

$$G = \mathsf{A}_n \quad \text{or} \quad G = \mathsf{S}_n \qquad (n \geq 5).$$

Claim 4.8. *G is weakly homogeneous.*

Projective groups (Rows 2–3 of Table 1)

The action of $\mathsf{PSL}(d, q)$ $(d \geq 2)$ is the natural action on the $(d-1)$-dimensional projective space A over the field $\mathbb{F}_q$. The group $\mathsf{P\Gamma L}(d, q)$, which is the extension of $\mathsf{PGL}(d, q)$ by the field automorphisms, acts on the same space, and has $\mathsf{PSL}(d, q)$ as a normal subgroup. Therefore

$$[\mathsf{P\Gamma L}(d, q) : \mathsf{PSL}(d, q)] = [\mathsf{P\Gamma L}(d, q) : \mathsf{PGL}(d, q)] \cdot [\mathsf{PGL}(d, q) : \mathsf{PSL}(d, q)] = e \cdot (d, q-1).$$

Since $[\widehat{S} : S] = e \cdot (d, q-1)$ holds by Table 1, we get that $\widehat{S} = \mathsf{P\Gamma L}(d, q)$. Thus

$$\mathsf{PSL}(d, q) \leq G \leq \mathsf{P\Gamma L}(d, q).$$

Claim 4.9. *If $d > 2$ then* (WH_3) *fails for G.*

To prove the claim notice that the family of all lines of a $(d-1)$-dimensional projective geometry over $\mathbb{F}_q$ form an $\mathrm{S}\big(2, q+1, (q^d-1)/(q-1)\big)$ Steiner system satisfying $2 < q+1 < (q^d-1)/(q-1)$. Moreover, $\mathsf{P\Gamma L}(d, q)$ (and hence G) is a group of automorphisms of this Steiner system. Therefore it follows from Claim 4.5 that (WH_3) fails for G.

Now let $d = 2$, so

$$\mathsf{PSL}(2, q) \leq G \leq \mathsf{P\Gamma L}(2, q) \qquad (q = p^e \neq 2, 3).$$

In this case A is the projective line over a finite field $\mathbb{F}_q$, and the elements of A (i.e., the points of the projective line) are

$$\left\langle \begin{bmatrix} a \\ 1 \end{bmatrix} \right\rangle \quad (a \in \mathbb{F}_q) \qquad \text{and} \qquad \left\langle \begin{bmatrix} 1 \\ 0 \end{bmatrix} \right\rangle. \tag{4.2}$$

The *cross ratio* of four distinct points $\langle \mathbf{x} \rangle, \langle \mathbf{y} \rangle, \langle \mathbf{v} \rangle, \langle \mathbf{w} \rangle \in A$ is defined as follows:

$$\mathrm{crr}(\langle \mathbf{x} \rangle, \langle \mathbf{y} \rangle, \langle \mathbf{v} \rangle, \langle \mathbf{w} \rangle) = \frac{|\mathbf{w}\ \mathbf{y}| \cdot |\mathbf{x}\ \mathbf{v}|}{|\mathbf{w}\ \mathbf{v}| \cdot |\mathbf{x}\ \mathbf{y}|} \tag{4.3}$$

where $|\mathbf{s}\ \mathbf{t}|$ denotes the determinant of the 2×2 matrix with columns $\mathbf{s}, \mathbf{t}$. Clearly, the right hand side does not depend on the choice of the generators of $\langle \mathbf{x} \rangle$, $\langle \mathbf{y} \rangle$, $\langle \mathbf{v} \rangle$, $\langle \mathbf{w} \rangle$; therefore the cross ratio is well defined.

	$\lvert A\rvert$	Condition	S	$[\widehat{S} : S]$	Tr. Deg.
1	n	$n \geq 5$	A_n	2	n
2	$\frac{q^d-1}{q-1}$	$q = p^e$ (p prime) $d \geq 3$	$\mathsf{PSL}(d, q)$	$(d, q-1)e$	2
3	$q+1$	$q = p^e$ (p prime) $q \neq 2, 3$	$\mathsf{PSL}(2, q)$	$(2, q-1)e$	3
4	$2^{2d-1} + 2^{d-1}$	$d \geq 3$	$\mathsf{Sp}(2d, 2)$	1	2
5	$2^{2d-1} - 2^{d-1}$	$d \geq 3$	$\mathsf{Sp}(2d, 2)$	1	2
6	q^3+1	$q = p^e$ (p prime) $q \geq 3$	$\mathsf{PSU}(3, q)$	$(3, q+1)e$	2
7	q^2+1	$q = 2^{2d+1} > 2$	$\mathsf{Sz}(q)$	$2d+1$	2
8	q^3+1	$q = 3^{2d+1} > 3$	$\mathsf{R}_1(q)$	$2d+1$	2
9	11		$\mathsf{PSL}(2, 11)$	1	2
10	11		M_{11}	1	4
11	12		M_{11}	1	3
12	12		M_{12}	1	5
13	15		A_7	1	2
14	22		M_{22}	2	3
15	23		M_{23}	1	4
16	24		M_{24}	1	5
17	28		$\mathsf{PSL}(2, 8)$	3	2
18	176		HS	1	2
19	276		Co_3	1	2

TABLE 1. 2-transitive almost simple groups ([3])

	$\lvert A\rvert$	Condition	$S \leq G \leq \widehat{S}$	Tr. Deg.
1	n	$n \geq 5$	$\mathsf{A}_n \leq G \leq \mathsf{S}_n$	n
2	$\frac{q^d-1}{q-1}$	$q = p^e$ (p prime) $d \geq 3$	$\mathsf{PSL}(d,q) \leq G \leq \mathsf{P\Gamma L}(d,q)$	2
3	$q+1$	$q = p^e$ (p prime) $q \neq 2,3$	$\mathsf{PSL}(2,q) \leq G \leq \mathsf{P\Gamma L}(d,q)$	3
4	$2^{2d-1}+2^{d-1}$	$d \geq 3$	$\mathsf{Sp}(2d,2) \leq G \leq \mathsf{Sp}(2d,2)$	2
5	$2^{2d-1}-2^{d-1}$	$d \geq 3$	$\mathsf{Sp}(2d,2) \leq G \leq \mathsf{Sp}(2d,2)$	2
6	q^3+1	$q = p^e$ (p prime) $q \geq 3$	$\mathsf{PSU}(3,q) \leq G \leq \mathsf{P\Gamma U}(3,q)$	2
7	q^2+1	$q = 2^{2d+1} > 2$	$\mathsf{Sz}(q) \leq G \leq \overline{\mathsf{Sz}}(q)$	2
8	q^3+1	$q = 3^{2d+1} > 3$	$\mathsf{R}_1(q) \leq G \leq \overline{\mathsf{R}}_1(q)$	2
9	11		$\mathsf{PSL}(2,11) \leq G \leq \mathsf{PSL}(2,11)$	2
10	11		$\mathsf{M}_{11} \leq G \leq \mathsf{M}_{11}$	4
11	12		$\mathsf{M}_{11} \leq G \leq \mathsf{M}_{11}$	3
12	12		$\mathsf{M}_{12} \leq G \leq \mathsf{M}_{12}$	5
13	15		$\mathsf{A}_7 \leq G \leq \mathsf{A}_7$	2
14	22		$\mathsf{M}_{22} \leq G \leq \overline{\mathsf{M}}_{22}$	3
15	23		$\mathsf{M}_{23} \leq G \leq \mathsf{M}_{23}$	4
16	24		$\mathsf{M}_{24} \leq G \leq \mathsf{M}_{24}$	5
17	28		$\mathsf{PSL}(2,8) \leq G \leq \mathsf{P\Gamma L}(2,8)$	2
18	176		$\mathsf{HS} \leq G \leq \mathsf{HS}$	2
19	276		$\mathsf{Co}_3 \leq G \leq \mathsf{Co}_3$	2

TABLE 2. The intervals $S \leq G \leq \widehat{S}$

To simplify notation we will identify the points of the projective line listed in (4.2) with the elements a of the field $\mathbb{F}_q$, and with ∞, respectively. Thus $A = \mathbb{F}_q \cup \{\infty\}$, and $\mathsf{P\Gamma L}(2,q)$ acts on A by fractional semilinear transformations

$$x \mapsto \frac{e \cdot \sigma(x) + f}{g \cdot \sigma(x) + h} \qquad (e, f, g, h \in \mathbb{F}_q,\ eh - fg \neq 0)$$

where σ is an automorphisms of $\mathbb{F}_q$, extended to A by $\sigma(\infty) = \infty$. The cross ratio of four distinct points $a, b, c, d \in A$ becomes

$$\operatorname{crr}(a,b,c,d) = \frac{(d-b)(a-c)}{(d-c)(a-b)} \tag{4.4}$$

if $a, b, c, d \in \mathbb{F}_q$ and

$$\begin{aligned} \operatorname{crr}(\infty,b,c,d) &= \frac{d-b}{d-c}, \qquad \operatorname{crr}(a,\infty,c,d) = \frac{a-c}{d-c}, \\ \operatorname{crr}(a,b,\infty,d) &= \frac{d-b}{a-b}, \qquad \operatorname{crr}(a,b,c,\infty) = \frac{a-c}{a-b} \end{aligned} \tag{4.5}$$

otherwise.

Claim 4.10. *The cross ratio has the following properties. For any four distinct points a, b, c, d of the projective line $A = \mathbb{F}_q \cup \{\infty\}$ over $\mathbb{F}_q$,*

(1) $\operatorname{crr}(a,b,c,d) \in \mathbb{F}_q - \{0,1\}$;
(2) *the assignment $u \mapsto \operatorname{crr}(a,b,c,u)$ yields a bijection between $A - \{a,b,c\}$ and $\mathbb{F}_q - \{0,1\}$; moreover, if $a, b, c \in K \cup \{\infty\}$ for a subfield K of $\mathbb{F}_q$, then*

$$u \in K \cup \{\infty\} \quad \Longleftrightarrow \quad \operatorname{crr}(a,b,c,u) \in K;$$

(3) *permutations of the points a, b, c, d have the following effect:*

$$\begin{aligned} \operatorname{crr}(a,c,b,d) &= 1/\operatorname{crr}(a,b,c,d), \\ \operatorname{crr}(b,a,c,d) &= 1 - \operatorname{crr}(a,b,c,d), \\ \operatorname{crr}(d,c,b,a) &= \operatorname{crr}(a,b,c,d), \\ \operatorname{crr}(b,a,d,c) &= \operatorname{crr}(a,b,c,d); \end{aligned}$$

(4) *if $\pi \in \mathsf{PGL}(2,q)$ then*

$$\operatorname{crr}\big(\pi(a),\pi(b),\pi(c),\pi(d)\big) = \operatorname{crr}(a,b,c,d),$$

that is, permutations from $\mathsf{PGL}(2,q)$ preserve the cross ratio;
(5) *if $\sigma \in \operatorname{Aut}(\mathbb{F}_q)$, then the extension of σ to the projective line has the following effect:*

$$\operatorname{crr}\big(\sigma(a),\sigma(b),\sigma(c),\sigma(d)\big) = \sigma\big(\operatorname{crr}(a,b,c,d)\big).$$

The easiest way to check (4) is to use (4.3) and observe that, because of the multiplicative property of the determinant, the right hand side is invariant under the action of $\mathsf{GL}(2,q)$. (5) follows immediately from (4.4) and (4.5). Since $\mathsf{PGL}(2,q)$ acts 3-transitively on A and preserves the cross ratio, it is enough to prove (1), the first part of (2), and (3) for $a=1$, $b=0$, $c=\infty$. In this case $\mathrm{crr}(a,b,c,u)=u$ for any $u\in A-\{a,b,c\}=\mathbb{F}_q-\{0,1\}$, so (1) and the first part of (2) follow immediately. To check (3) one can use (4.5). The second statement in (2) follows from the first and the expressions for the cross ratio in (4.4) and (4.5).

Now define an action of S_4 on $\mathbb{F}_q-\{0,1\}$ as follows: all permutations from the Klein group are in the kernel of the action, and the transpositions (1 2) and (2 3) act by the permutations $\alpha\mapsto 1-\alpha$ and $\alpha\mapsto 1/\alpha$, respectively. Claim 4.10 (3) implies that performing a permutation from S_4 on four distinct points $a,b,c,d\in A$ changes their cross ratio by the corresponding permutation of $\mathbb{F}_q-\{0,1\}$. Therefore we will call this action of S_4 on $\mathbb{F}_q-\{0,1\}$ the *cross ratio action*, and its orbits *cross ratio orbits*. Thus the cross ratio orbits are the sets of the form

$$[\alpha]=\{\alpha,\ 1-\alpha,\ 1/\alpha,\ 1/(1-\alpha),\ 1-1/\alpha,\ 1-1/(1-\alpha)\}\quad(\alpha\in\mathbb{F}_q-\{0,1\}),$$

and to each 4-element set $\{a,b,c,d\}\subseteq A$ we can unambiguously associate its cross ratio orbit $[\mathrm{crr}(a,b,c,d)]$.

It is easy to see that the cross ratio action of S_4 on $\mathbb{F}_q-\{0,1\}$ commutes with the action of the automorphism group $\mathrm{Aut}(\mathbb{F}_q)$ of $\mathbb{F}_q$ on $\mathbb{F}_q-\{0,1\}$ (see Claim 4.10 (5)). The orbits of the combined action of S_4 and $\mathrm{Aut}(\mathbb{F}_q)$, that is, the sets

$$[[\alpha]]=\bigcup\big([\sigma(\alpha)]:\sigma\in\mathrm{Aut}(\mathbb{F}_q)\big)\quad(\alpha\in\mathbb{F}_q-\{0,1\}).$$

will be called *extended cross ratio orbits*.

Claim 4.11. *For any two 4-element subsets $\{a,b,c,d\}$, $\{a',b',c',d'\}$ of A,*

1. *$\{a,b,c,d\}$ and $\{a',b',c',d'\}$ are in the same orbit of $\mathsf{PGL}(2,q)$ if and only if $[\mathrm{crr}(a,b,c,d)]=[\mathrm{crr}(a',b',c',d')]$; and*
2. *$\{a,b,c,d\}$ and $\{a',b',c',d'\}$ are in the same orbit of $\mathsf{P\Gamma L}(2,q)$ if and only if $[[\mathrm{crr}(a,b,c,d)]]=[[\mathrm{crr}(a',b',c',d')]]$.*

First we prove (1). If $\{a,b,c,d\}$ and $\{a',b',c',d'\}$ are in the same orbit of $\mathsf{PGL}(2,q)$, then $\{a',b',c',d'\}=\{\pi(a),\pi(b),\pi(c),\pi(d)\}$ for some $\pi\in\mathsf{PGL}(2,q)$. Thus the equality $[\mathrm{crr}(a,b,c,d)]=[\mathrm{crr}(a',b',c',d')]$ follows from Claim 4.10 (3) and (4). Conversely, assume that $[\mathrm{crr}(a,b,c,d)]=[\mathrm{crr}(a',b',c',d')]$. Claim 4.10 (3) and the definition of the cross ratio orbits imply that for a reordering a'',b'',c'',d'' of the elements a',b',c',d' we have $\mathrm{crr}(a,b,c,d)=\mathrm{crr}(a'',b'',c'',d'')$. Since $\mathsf{PGL}(2,q)$ acts 3-transitively on A, there is a $\pi\in\mathsf{PGL}(2,q)$ such that $\pi(a)=a''$, $\pi(b)=b''$, and $\pi(c)=c''$. Hence we get

$$\mathrm{crr}(a'',b'',c'',d'')=\mathrm{crr}(a,b,c,d)=\mathrm{crr}\big(\pi(a),\pi(b),\pi(c),\pi(d)\big)=\mathrm{crr}\big(a'',b'',c'',\pi(d)\big)$$

where the second equality follows from Claim 4.10 (3). The equality of the leftmost and rightmost cross ratios implies by Claim 4.10 (2) that $d'' = \pi(d)$. Thus $\{a', b', c', d'\} = \{a'', b'', c'', d''\} = \{\pi(a), \pi(b), \pi(c), \pi(d)\}$, showing that $\{a, b, c, d\}$ and $\{a', b', c', d'\}$ are in the same orbit of $\mathsf{PGL}(2, q)$.

The proof of (2) is similar, and uses the fact that $\mathsf{P\Gamma L}(2, q)$ is a semidirect product of its normal subgroup $\mathsf{PGL}(2, q)$ and its subgroup that consists of the permutations induced by the automorphisms of $\mathbb{F}_q$. Thus, if $\{a, b, c, d\}$ and $\{a', b', c', d'\}$ are in the same orbit of $\mathsf{P\Gamma L}(2, q)$, then $\{a', b', c', d'\} = \{\sigma(\pi(a)), \sigma(\pi(b)), \sigma(\pi(c)), \sigma(\pi(d))\}$ for some $\pi \in \mathsf{PGL}(2, q)$ and $\sigma \in \mathrm{Aut}(\mathbb{F}_q)$. Hence the equality $[[\mathrm{crr}(a, b, c, d)]] = [[\mathrm{crr}(a', b', c', d')]]$ follows from Claim 4.10 (3), (4), and (5). Conversely, assume that $[[\mathrm{crr}(a, b, c, d)]] = [[\mathrm{crr}(a', b', c', d')]]$. The definition of the extended cross ratio orbits, combined with Claim 4.10 (5), implies that

$$[\mathrm{crr}(a, b, c, d)] = \big[\sigma\big(\mathrm{crr}(a', b', c', d')\big)\big] = \big[\mathrm{crr}\big(\sigma(a'), \sigma(b'), \sigma(c'), \sigma(d')\big)\big]$$

for some $\sigma \in \mathrm{Aut}(\mathbb{F}_q)$. Now it follows form part (1) that the sets $\{a, b, c, d\}$ and $\{\sigma(a'), \sigma(b'), \sigma(c'), \sigma(d')\}$ are in the same orbit of $\mathsf{PGL}(2, q)$, hence $\{a, b, c, d\}$ and $\{a', b', c', d'\}$ are in the same orbit of $\mathsf{P\Gamma L}(2, q)$.

Claim 4.12. *Let* $\mathsf{PSL}(2, q) \leq G \leq \mathsf{P\Gamma L}(2, q)$ *where* $q = p^e \neq 2, 3$ *(p prime).*

(1) *If* $q \neq 4, 5, 7, 8, 11, 32$, *then* ($\mathrm{WH}_4$) *fails for* G.
(2) *If* $q = 11$ *or* $q = 32$, *then* (WH_5) *fails for* G.

We will prove (1) as follows. We will select an extended cross ratio orbit $\mathcal{O}$ and four points a, b, c, d of the projective line so that $\mathrm{crr}(a, b, c, d) \in \mathcal{O}$. Then we will argue that there exists a fifth point u on the projective line such that u is different from the solutions of each equation

$$\mathrm{crr}(a, b, c, x) = \alpha,\ \mathrm{crr}(a, b, x, d) = \alpha,\ \mathrm{crr}(a, x, c, d) = \alpha,\ \mathrm{crr}(x, b, c, d) = \alpha \quad (\alpha \in \mathcal{O}). \tag{4.6}$$

Since these solutions include $x = d$ (first equation), $x = c$ (second equation), $x = b$ (third equation), and $x = a$ (fourth equation, each with $\alpha = \mathrm{crr}(a, b, c, d) \in \mathcal{O}$), such a u will be distinct from a, b, c, d. Moreover u will satisfy the conditions

$$\mathrm{crr}(a, b, c, u),\ \mathrm{crr}(a, b, d, u),\ \mathrm{crr}(a, c, d, u),\ \mathrm{crr}(b, c, d, u) \notin \mathcal{O}. \tag{4.7}$$

By Claim 4.11 (2) these conditions imply that the 4-element set $C = \{a, b, c, d\}$ is in a different G-orbit than any other 4-element subset of $B = C \cup \{u\}$, which proves that (WH_4) fails for G.

Suppose first that $\mathbb{F}_q$ has a proper subfield K such that $|K| \geq 3$. Since every automorphism of $\mathbb{F}_q$ maps K onto itself, each extended cross ratio orbit is either contained in K or is disjoint from K. Let $\mathcal{O}$ be an extended cross ratio orbit such that $\mathcal{O} \subseteq K$, and let $a = \infty$, $b = 0$, $c = 1$, $d \in \mathcal{O}$. Then $\mathrm{crr}(a, b, c, d) = d/(d-1) \in \mathcal{O}$.

Now choose $u \in A$ such that $u \notin K \cup \{\infty\}$. Then Claim 4.10 (2) implies that u is not a solution of any of the equations in (4.6).

Recall that $q = p^e \neq 2, 3$. If $\mathbb{F}_q$ does not have a proper subfield K such that $|K| \geq 3$, then either $q = p$ is prime ($p \geq 5$), or $p = 2$ and $q = 2^e$ for some prime e. In most of these cases we can prove the existence of u by a counting argument. The number of equations in (4.6) is $4|\mathcal{O}|$, and by Claim 4.10 (2) and (3) each of these equations has a unique solution. Therefore there exists a point u distinct from the solutions of the equations in (4.6) provided $|A| > 4|\mathcal{O}|$.

If $q = p$ is prime ($p \geq 5$), then $\mathsf{P\Gamma L}(2, p) = \mathsf{PGL}(2, p)$, and the extended cross ratio orbits are the same as the cross ratio orbits. Choosing $\mathcal{O} = \{2, -1, 1/2\}$ we see that the required point u exists if $p + 1 = |A| > 4|O| = 12$. If $q = 2^e$ where e is prime, then let $\mathcal{O}$ be an arbitrary extended cross ratio orbit. Since a cross ratio orbit has at most 6 elements and $|\mathrm{Aut}(\mathbb{F}_q)| = e$, we get that $|\mathcal{O}| \leq 6e$. Hence the required point u will exist if $2^e + 1 = |A| > 24e$. It is easy to check that this inequality is true for $e \geq 11$.

Since e is prime, the only case satisfying the assumptions of Claim 4.12 (1) and not covered by the preceding argument is $q = 2^7 = 128$. For this case an appropriate choice for a, b, c, d, u was found and checked by MAPLE. To describe this choice, select and fix a root $\gamma \in \mathbb{F}_{128}$ of $1 + x + x^7 \in \mathbb{F}_2[x]$. Each element of $\mathbb{F}_{128}$ can be written uniquely as a sum of the form $\sum_{i=0}^{6} \varepsilon_i \gamma^i$ with $\varepsilon_i \in \{0, 1\}$, and therefore can be 'coded' by the natural number $\mathbf{n} = \sum_{i=0}^{6} \varepsilon_i 2^i$. We will use these codes $\mathbf{0}, \mathbf{1}, \ldots, \mathbf{127}$ as a shorthand notation for the elements of $\mathbb{F}_{128}$. For example, $0 = \mathbf{0}$, $1 = \mathbf{1}$, $\gamma = \mathbf{2}$, and $1 + \gamma + \gamma^4 = \mathbf{19}$.

The three extended cross ratio orbits are

$$\begin{aligned}\mathcal{O}_1 = \{&\mathbf{2}, \mathbf{3}, \mathbf{4}, \mathbf{5}, \mathbf{6}, \mathbf{7}, \mathbf{8}, \mathbf{9}, \mathbf{10}, \mathbf{11}, \mathbf{16}, \mathbf{17}, \mathbf{18}, \mathbf{19},\\ &\mathbf{20}, \mathbf{21}, \mathbf{22}, \mathbf{23}, \mathbf{36}, \mathbf{37}, \mathbf{42}, \mathbf{43}, \mathbf{54}, \mathbf{55}, \mathbf{62}, \mathbf{63}, \mathbf{64}, \mathbf{65},\\ &\mathbf{68}, \mathbf{69}, \mathbf{74}, \mathbf{75}, \mathbf{92}, \mathbf{93}, \mathbf{96}, \mathbf{97}, \mathbf{112}, \mathbf{113}, \mathbf{120}, \mathbf{121}, \mathbf{126}, \mathbf{127}\},\end{aligned}$$

$$\begin{aligned}\mathcal{O}_2 = \{&\mathbf{12}, \mathbf{13}, \mathbf{14}, \mathbf{15}, \mathbf{26}, \mathbf{27}, \mathbf{38}, \mathbf{39}, \mathbf{40}, \mathbf{41}, \mathbf{50}, \mathbf{51}, \mathbf{52}, \mathbf{53},\\ &\mathbf{56}, \mathbf{57}, \mathbf{60}, \mathbf{61}, \mathbf{66}, \mathbf{67}, \mathbf{78}, \mathbf{79}, \mathbf{80}, \mathbf{81}, \mathbf{84}, \mathbf{85}, \mathbf{88}, \mathbf{89},\\ &\mathbf{94}, \mathbf{95}, \mathbf{100}, \mathbf{101}, \mathbf{102}, \mathbf{103}, \mathbf{104}, \mathbf{105}, \mathbf{106}, \mathbf{107}, \mathbf{108}, \mathbf{109}, \mathbf{118}, \mathbf{119}\},\end{aligned}$$

$$\begin{aligned}\mathcal{O}_3 = \{&\mathbf{24}, \mathbf{25}, \mathbf{28}, \mathbf{29}, \mathbf{30}, \mathbf{31}, \mathbf{32}, \mathbf{33}, \mathbf{34}, \mathbf{35}, \mathbf{44}, \mathbf{45}, \mathbf{46}, \mathbf{47}\\ &\mathbf{48}, \mathbf{49}, \mathbf{58}, \mathbf{59}, \mathbf{70}, \mathbf{71}, \mathbf{72}, \mathbf{73}, \mathbf{76}, \mathbf{77}, \mathbf{82}, \mathbf{83}, \mathbf{86}, \mathbf{87}\\ &\mathbf{90}, \mathbf{91}, \mathbf{98}, \mathbf{99}, \mathbf{110}, \mathbf{111}, \mathbf{114}, \mathbf{115}, \mathbf{116}, \mathbf{117}, \mathbf{122}, \mathbf{123}, \mathbf{124}, \mathbf{125}\}.\end{aligned}$$

Choosing $\mathcal{O} = \mathcal{O}_3$ and $a = \infty$, $b = 1 = \mathbf{1}$, $c = \gamma = \mathbf{2}$, $d = \gamma^2 + \gamma^3 = \mathbf{12}$, $u = 0 = \mathbf{0}$ we get that

$$\begin{aligned}
\mathrm{crr}(a, b, c, d) &= \mathbf{44} \in \mathcal{O}, \\
\mathrm{crr}(a, b, c, u) &= \mathbf{65} \notin \mathcal{O}, \\
\mathrm{crr}(a, b, u, d) &= \mathbf{95} \notin \mathcal{O}, \\
\mathrm{crr}(a, u, c, d) &= \mathbf{55} \notin \mathcal{O}, \\
\mathrm{crr}(u, b, c, d) &= \mathbf{88} \notin \mathcal{O}.
\end{aligned}$$

This completes the proof of statement (1).

To prove (2), let first $q = 11$. Since $\mathsf{P\Gamma L}(2, 11) = \mathsf{PGL}(2, 11)$, the extended cross ratio orbits are the same as the cross ratio orbits. In fact, there are two cross ratio orbits:

$$\mathcal{O}_1 = \{2, -1, 1/2\} = \{2, 10, 6\} \quad \text{and} \quad \mathcal{O}_2 = \{3, 4, 5, 7, 8, 9\}.$$

Our goal is to find sets B and C that witness the failure of (WH_5). Let $C = \{\infty, 0, 1, 3, 4\}$ and $B = C \cup \{7\}$. Since

$$\begin{aligned}
\mathrm{crr}(\infty, 0, 1, 3) &= 3/2 = 7 \in \mathcal{O}_2, \\
\mathrm{crr}(\infty, 0, 1, 4) &= 4/3 = 5 \in \mathcal{O}_2, \\
\mathrm{crr}(\infty, 0, 3, 4) &= 4/1 = 4 \in \mathcal{O}_2, \\
\mathrm{crr}(\infty, 1, 3, 4) &= 3/1 = 3 \in \mathcal{O}_2, \\
\mathrm{crr}(0, 1, 3, 4) &= 3(-3)/(-1) = 9 \in \mathcal{O}_2, \\
\mathrm{crr}(\infty, 0, 3, 7) &= 7/4 = 10 \in \mathcal{O}_1, \\
\mathrm{crr}(\infty, 1, 4, 7) &= 6/3 = 2 \in \mathcal{O}_1, \\
\mathrm{crr}(0, 1, 3, 7) &= 6(-3)/4(-1) = 10 \in \mathcal{O}_1,
\end{aligned}$$

therefore the cross ratio orbit associated to each 4-element subset of C is in $\mathcal{O}_2$, while every 5-element subset of B containing 7 has a 4-element subset whose associated cross ratio orbit is $\mathcal{O}_1$. It follows from Claim 4.11 (1) that the G-orbit of C is distinct from the G-orbits of all other 5-element subsets of B. This proves that (WH_5) fails for G.

Finally, let $q = 32$. For this case an appropriate choice for sets B, C witnessing the failure of (WH_5) were found and checked by MAPLE. To describe the sets B, C, select and fix a root $\gamma \in \mathbb{F}_{32}$ of $1 + x^2 + x^5 \in \mathbb{F}_2[x]$. The cross ratio orbits are the

$(u_1 \dots, u_5)$	$(n_1, \dots, n_5)$
(a, b, c, d, e)	$(4, 3, 1, 2, 0)$
(b, c, d, e, u)	$(4, 3, 2, 1, 4)$
(a, c, d, e, u)	$(4, 1, 1, 0, 3)$
(a, b, d, e, u)	$(3, 1, 4, 0, 1)$
(a, b, c, e, u)	$(2, 1, 4, 0, 2)$
(a, b, c, d, u)	$(1, 0, 0, 0, 0)$

TABLE 3

following:

$$\mathcal{O}_0 = \{1+\gamma^2+\gamma^3+\gamma^4,\ 1+\gamma+\gamma^4,\ 1+\gamma,\ \gamma,\ \gamma^2+\gamma^3+\gamma^4,\ \gamma+\gamma^4\},$$
$$\mathcal{O}_1 = \{1+\gamma^3,\ \gamma^2,\ 1+\gamma+\gamma^2+\gamma^4,\ 1+\gamma^2,\ \gamma+\gamma^2+\gamma^4,\ \gamma^3\},$$
$$\mathcal{O}_2 = \{1+\gamma^4,\ 1+\gamma^3+\gamma^4,\ \gamma+\gamma^3,\ \gamma^3+\gamma^4,\ \gamma^4,\ 1+\gamma+\gamma^3\}$$
$$\mathcal{O}_3 = \{1+\gamma+\gamma^2+\gamma^3,\ \gamma+\gamma^2+\gamma^3,\ \gamma+\gamma^2,\ 1+\gamma+\gamma^2,\ \gamma^2+\gamma^3,\ 1+\gamma^2+\gamma^3\}$$
$$\mathcal{O}_4 = \{\gamma+\gamma^3+\gamma^4,\ 1+\gamma+\gamma^3+\gamma^4,\ 1+\gamma^2+\gamma^4,$$
$$1+\gamma+\gamma^2+\gamma^3+\gamma^4, \gamma+\gamma^2+\gamma^3+\gamma^4,\ \gamma^2+\gamma^4\}$$

The Frobenius automorphism permutes these orbits cyclically: $\mathcal{O}_0 \mapsto \mathcal{O}_1 \mapsto \mathcal{O}_2 \mapsto \mathcal{O}_3 \mapsto \mathcal{O}_4 \mapsto \mathcal{O}_0$. Therefore $\mathbb{F}_{32} - \{0, 1\}$ is a single extended cross ratio orbit, which implies by Claim 4.11 (2) that $\mathsf{P\Gamma L}(2, 32)$ is 4-homogeneous.

As before, our goal is to find sets B and C that witness the failure of (WH_5). Let $C = \{a, b, c, d, e\}$ and $B = C \cup \{u\}$ where $a = \infty$, $b = 0$, $c = 1$, $d = \gamma$, $e = 1+\gamma+\gamma^3$, and $u = 1+\gamma$. To show that the G-orbit of C is different from the G-orbits of all other 5-element subsets of B, we look at the 5-element subsets of B, and determine the cross ratio orbit of each of its 4-element subsets. The results are recorded in Table 3 in the following form: we represent a 5-element subset of B by a 5-tuple $(u_1, \dots, u_5)$ that we get from (a, b, c, d, e, f) by deleting a coordinate. To each such 5-tuple we assign a 5-tuple $(n_1, \dots, n_5)$ of numbers where, for each i $(1 \leq i \leq 5)$, n_i is the subscript of the cross ratio orbit $[\mathrm{crr}(u_1, \dots, u_{i-1}, u_{i+1}, \dots, u_5)]$ of the 4-tuple that we get from $(u_1, \dots, u_5)$ by deleting its i-th coordinate. We will refer to $(n_1, \dots, n_5)$ as the tuple of cross ratio orbits associated to $(u_1, \dots, u_5)$.

For any 5-tuple $(u_1, \dots, u_5)$ of distinct points of the projective line,

- a permutation of the coordinates of $(u_1, \dots, u_5)$ yields the same permutation of the associated tuple of cross ratio orbits (since any permutation of the arguments of the cross ratio leaves the cross ratio orbit unchanged);
- an application of a permutation from $\mathsf{PGL}(2, 32)$ to each coordinate of $(u_1, \dots, u_5)$ leaves the associated tuple of cross ratio orbits unchanged (since permutations from $\mathsf{PGL}(2, 32)$ preserve the cross ratio); and
- an application of the Frobenius automorphism of $\mathbb{F}_{32}$ to each coordinate of $(u_1, \dots, u_5)$ adds $1 \mod 5$ to each coordinate of the tuple of cross ratio orbits.

This implies that the property of having a repetition in the tuple of cross ratio orbits associated to a 5-tuple $(u_1, \dots, u_5)$ of distinct points is a property of the 5-element set $\{u_1, \dots, u_5\}$ (i.e., does not depend on the ordering of the coordinates of $(u_1, \dots, u_5)$), and is preserved by every permutation in $\mathsf{P\Gamma L}(2, 32)$. By Table 3, the tuple of cross ratio orbits associated to C has no repetition, while the tuples of cross ratio orbits associated to all other 5-element subsets of B have repetitions. This implies that the G-orbit of C is different from the G-orbits of all other 5-element subsets of B. The proof of Claim 4.12 is complete.

Claim 4.13. *If* $\mathsf{PSL}(2, q) \leq G \leq \mathsf{P\Gamma L}(2, q)$ $(q = p^e \neq 2, 3,\ p$ *prime*$)$ *and* $q = 4, 5, 7$ *or* 8*, then* G *is one of the following groups:*

$$\begin{array}{llll} \mathsf{PGL}(2,4) = \mathsf{A}_4, & \mathsf{P\Gamma L}(2,4) = \mathsf{S}_4, & \mathsf{PSL}(2,5), & \mathsf{PGL}(2,5), \\ \mathsf{PSL}(2,7), & \mathsf{PGL}(2,7), & \mathsf{PGL}(2,8), & \mathsf{P\Gamma L}(2,8). \end{array} \tag{4.8}$$

$\mathsf{PSL}(2, 7)$ *fails to satisfy* (WH_4)*, but the remaining groups are weakly homogeneous.*

Indeed, if $q = 5$ or 7, then $\mathsf{PGL}(2, q) = \mathsf{P\Gamma L}(2, q)$ and $[\mathsf{PGL}(2, q) : \mathsf{PSL}(2, q)] = 2$, while if $q = 2^e$ $(e = 2, 3)$, then $\mathsf{PSL}(2, 2^e) = \mathsf{PGL}(2, 2^e)$ and $[\mathsf{P\Gamma L}(2, 2^e) : \mathsf{PGL}(2, 2^e)] = e$. Therefore the only possibilities for G are the groups listed in (4.8).

The permutation group $\mathsf{PSL}(2, 7)$ acting on an 8-element set is a subgroup of the affine group $\mathsf{AGL}(3, 2)$ acting on an 8-element set ([2], p. 9). Since (WH_4) fails for $\mathsf{AGL}(3, 2)$ by Claim 4.6, it fails for $\mathsf{PSL}(2, 7)$ as well. The weak homogeneity of $\mathsf{PSL}(2, 5)$ and $\mathsf{PGL}(2, 7)$ is proved in the next two claims. The remaining groups in (4.8) are k-homogeneous for all k $(1 \leq k < |A|)$ by Theorem 2.3, so they are also weakly homogeneous.

Claim 4.14. *The permutation group* $G = \mathsf{PSL}(2, 5)$*, acting on the projective line* $A = \mathbb{F}_5 \cup \{\infty\}$ *over* $\mathbb{F}_5$*,*

(1) *is* k*-homogeneous for every* $k \neq 3$ $(1 \leq k \leq 5)$*, and*
(2) *has two orbits of* 3*-element sets; the two orbits consist of the following sets:*
   - $\{a-1, a, a+1\}, \quad \{a+1, \infty, a-1\} \qquad \big(a \in \mathbb{F}_5\big)$,
   - $\{a-2, a, a+2\}, \quad \{a+2, \infty, a-2\} \qquad \big(a \in \mathbb{F}_5\big)$.

Hence G *is weakly homogeneous.*

Geometrically, we can think of A as a pentagon with vertices $a \in \mathbb{F}_5$, together with a point ∞ at infinity. In this interpretation, the two G-orbits of 3-element sets are the following:

- one of the orbits consists of all isosceles triangles whose base is a diagonal of the pentagon, and
- the other orbit consists of all isosceles triangles whose base is a side of the pentagon.

To verify (1) we use that G acts 2-transitively on A. This implies that G is k-homogeneous, and hence also $(6-k)$-homogeneous, for $k = 1, 2$.

To prove (2) consider G as a subgroup of the group of all fractional linear transformations over $\mathbb{F}_5$. Since the transformation $\sigma\colon x \mapsto -1/x$ and the translations $\tau_a\colon x \mapsto x + a$ belong to G for all $a \in \mathbb{F}_5$, therefore the G-orbit of the 3-element set $S = \{-1, 0, 1\}$ contains $S' = \sigma(S) = \{1, \infty, -1\}$, and hence all sets

$$\tau_a(S) = \{a-1, a, a+1\} \quad \text{and} \quad \tau_a(S') = \{a+1, \infty, a-1\} \qquad \big(a \in \mathbb{F}_5\big). \tag{4.9}$$

These are ten of the twenty 3-element subsets of A. A similar calculation, starting with the set $T = \{-2, 0, 2\}$ which is not among those appearing in (4.9), shows that the G-orbit of T contains the remaining ten of the twenty 3-element subsets of A. Since G is not 3-homogeneous (by part (1) and Theorem 2.3), therefore the sets in (4.9) form one of the G-orbits of 3-element sets, and the remaining 3-element sets form the other orbit. This completes the proof of (2).

Finally we prove that G is weakly homogeneous. By part (1) G is k-homogeneous for every $k \neq 3$, therefore it remains to show that G is weakly 3-homogeneous. We have to verify that for every 4-element subset B of A exactly two of the four 3-element subsets of B belong to each orbit of 3-element sets. Since G is 4-homogeneous, it suffices to check this property for one 4-element set B. If $B = \{1, 2, 3, 4\}$, then $\{1, 2, 3\}$ and $\{2, 3, 4\}$ belong to the first orbit, while $\{2, 4, 1\}$ and $\{4, 1, 3\}$ belong to the second orbit. This completes the proof of Claim 4.14.

Claim 4.15. *The permutation group $G = \mathsf{PGL}(2, 7)$, acting on the projective line $A = \mathbb{F}_7 \cup \{\infty\}$ over $\mathbb{F}_7$,*

(1) *is k-homogeneous for every $k \neq 4$ $(1 \leq k \leq 7)$, and*
(2) *has two orbits of 4-element sets; the two orbits consist of the following sets:*
   - *$\{a, b, c, d\}$ $(\subseteq A)$ such that $\operatorname{crr}(a, b, c, d) \in \{3, 5\}$,*
   - *$\{a, b, c, d\}$ $(\subseteq A)$ such that $\operatorname{crr}(a, b, c, d) \in \{2, 4, 6\}$.*

Hence G is weakly homogeneous.

G acts 3-transitively on A. Therefore G is k-homogeneous, and hence also $(8-k)$-homogeneous, for $k = 1, 2, 3$. This proves (1).

To show (2) recall from Claim 4.11 that two 4-element sets $\{a, b, c, d\}$ and $\{a', b', c', d'\}$ belong to the same G-orbit if and only if the cross ratios $\operatorname{crr}(a, b, c, d)$ and $\operatorname{crr}(a', b', c', d')$

are in the same cross ratio orbit of $\mathbb{F}_7 - \{0,1\}$. The cross ratio orbits of $\mathbb{F}_7 - \{0,1\}$ are $\{3,5\} = \{3,3^5\}$ and $\{2,4,6\} = \{3^2,3^3,3^4\}$.

Finally we prove that G is weakly homogeneous. By part (1) G is k-homogeneous for every $k \neq 4$, therefore it remains to show that G is weakly 4-homogeneous. We have to verify that for every 5-element subset B of A two of the five 4-element subsets of B belong to one orbit, and the remaining three to the other orbit. Since G is 5-homogeneous, it suffices to check this property for one 5-element set B. Let $B = \{\infty,0,1,2,3\}$. Then $\mathrm{crr}(0,1,2,3) = 4$, $\mathrm{crr}(\infty,1,2,3) = 2$, $\mathrm{crr}(\infty,0,2,3) = 5$, $\mathrm{crr}(\infty,0,1,3) = 3$, and $\mathrm{crr}(\infty,0,1,2) = 2$. Hence the sets $\{\infty,0,2,3\}$, $\{\infty,0,1,3\}$ belong to one of the orbits, and the sets $\{0,1,2,3\}$, $\{\infty,1,2,3\}$, $\{\infty,0,1,2\}$ to the other. This completes the proof of Claim 4.15.

Claims 4.9–4.15 prove that among the projective groups (with their usual actions on projective spaces) the weakly homogeneous groups are exactly those listed in Theorem 4.1.

Symplectic groups (Rows 4–5 of Table 1)

The symplectic groups $\mathsf{Sp}(2d,2)$ have two different 2-transitive actions, as shown in Rows 4 and 5 of Table 1. Now we will describe these actions, following [5], pp. 245–248.

Let $V = \mathbb{F}_2^{2d}$ be the $2d$-dimensional (column) vector space over the 2-element field, let

$$E = \begin{bmatrix} 0 & I \\ 0 & 0 \end{bmatrix} \qquad \text{and} \qquad F = E + E^{\mathrm{T}} = \begin{bmatrix} 0 & I \\ I & 0 \end{bmatrix}$$

be $2d \times 2d$ matrices over $\mathbb{F}_2$ where I denotes the $d \times d$ identity matrix, and let $\varphi\colon V \times V \to \mathbb{F}_2$ be the bilinear form defined by $\varphi(u,v) = u^{\mathrm{T}}Fv$ for all $u,v \in V$. Let Ω denote the set of all functions $\theta\colon V \to \mathbb{F}_2$ that satisfy

$$\varphi(u,v) = \theta(u+v) - \theta(u) - \theta(v) \qquad \text{for all } u,v \in V.$$

For each vector $s \in V$, the quadratic form $\theta_s\colon V \to \mathbb{F}_2$ defined by $\theta_s(u) = u^{\mathrm{T}}Eu + s^{\mathrm{T}}Fu$ for all $u \in V$ is a member of Ω. In particular, $\theta_0(u) = u^{\mathrm{T}}Eu$ for all $u \in V$, and hence

$$\theta_s(u) = \theta_0(u) + s^{\mathrm{T}}Fu \qquad \text{for all } u \in V. \tag{4.10}$$

It is easy to see that for each $\theta \in \Omega$, the function $\theta - \theta_0\colon V \to \mathbb{F}_2$ is linear. Therefore each element of Ω is of the form θ_s for a unique vector $s \in V$. Hence $V \to \Omega$, $s \mapsto \theta_s$ is a bijection.

The symplectic group $\mathsf{Sp}(2d,2)$ is defined as the subgroup of $\mathsf{GL}(2d,2)$ consisting of all invertible matrices $M \in \mathsf{GL}(2d,2)$ such that $M^{\mathrm{T}}FM = F$. Since $\varphi(Mu,Mv) = \varphi(u,v)$ for all $M \in \mathsf{Sp}(2d,2)$ and $u,v \in V$, it follows that for each $\theta \in \Omega$, the function ${}^M\theta\colon V \to \mathbb{F}_2$ defined by ${}^M\theta(u) = \theta(M^{-1}u)$ is a member of Ω. Thus the

permutations $\theta \mapsto {}^M\theta$ ($M \in \mathsf{Sp}(2d,2)$) define an action of $\mathsf{Sp}(2d,2)$ on Ω. It can be shown (Corollary 7.7A and Theorem 7.7A of [5]) that this action has two orbits:

$$\Omega^+ = \{\theta_s : s \in V,\ \theta_0(s) = 0\} \qquad \text{and} \qquad \Omega^- = \{\theta_s : s \in V,\ \theta_0(s) = 1\}; \tag{4.11}$$

moreover, $\mathsf{Sp}(2d,2)$ acts 2-transitively on both of them. These are the two 2-transitive actions of $\mathsf{Sp}(2d,2)$.

For each $M \in \mathsf{Sp}(2d,2)$, let r_M denote the vector assigned to $\theta = {}^M\theta_0$; that is, r_M is the unique vector in V such that ${}^M\theta_0 = \theta_{r_M}$. Then ${}^M\theta_s = \theta_{Ms+r_M}$ holds for each $\theta_s \in \Omega$ and $M \in \mathsf{Sp}(2d,2)$, as the following calculation shows. Indeed, for arbitrary $u \in V$,

$$\begin{aligned} {}^M\theta_s(u) &= \theta_s(M^{-1}u) = \theta_0(M^{-1}u) + s^{\mathrm{T}}FM^{-1}u \\ &= {}^M\theta_0(u) + s^{\mathrm{T}}M^{\mathrm{T}}Fu = \theta_0(u) + r_M^{\mathrm{T}}Fu + s^{\mathrm{T}}M^{\mathrm{T}}Fu \\ &= \theta_0(u) + (r_M + Ms)^{\mathrm{T}}Fu = \theta_{Ms+r_M}(u); \end{aligned}$$

here we used the definition of the action of $\mathsf{Sp}(2d,2)$ on Ω, equation (4.10), the fact that $FM^{-1} = M^{\mathrm{T}}F$ for all $M \in \mathsf{Sp}(2d,2)$, and the definition of r_M.

Thus the action of $\mathsf{Sp}(2d,2)$ on Ω described earlier is equivalent, via the bijection $V \to \Omega$, $s \mapsto \theta_s$ to the action of $\mathsf{Sp}(2d,2)$ on V where each $M \in \mathsf{Sp}(2d,2)$ acts by the affine permutation $s \mapsto Ms + r_M$. Since $\theta_0(s) = s^{\mathrm{T}}Es$, we get from (4.11) that the orbits of this action are the sets

$$V^+ = \{s \in V : s^{\mathrm{T}}Es = 0\} \qquad \text{and} \qquad V^- = \{s \in V : s^{\mathrm{T}}Es = 1\}.$$

So, the 2-transitive actions of $\mathsf{Sp}(2d,2)$ are these actions G^+ and G^- of $\mathsf{Sp}(2d,2)$ on the orbits V^+ and V^-, respectively.

Claim 4.16. (WH_4) *fails for both 2-transitive actions G^+ and G^- of $S = \mathsf{Sp}(2d,2)$ ($d \geq 3$).*

To prove that (WH_4) fails for G^+ and G^-, we will use Claim 4.4. Let $\mathcal{S}$ be the set of all planes (cosets of 2-dimensional subspaces) of the affine geometry V over $\mathbb{F}_2$, and let

$$\mathcal{S}^+ = \{V^+ \cap X : X \in \mathcal{S}\} \qquad \text{and} \qquad \mathcal{S}^- = \{V^- \cap X : X \in \mathcal{S}\}.$$

Then $(V;\mathcal{S})$ is an $\mathrm{S}(3,4,2^{2d})$ ($d \geq 3$) Steiner system, and $(V^+,\mathcal{S}^+)$, $(V^-,\mathcal{S}^-)$ are its subsystems induced on the sets V^+ and V^-, respectively. Thus each 3-element subset of V^+ is contained in at most one member of $\mathcal{S}^+$, and similarly, each 3-element subset of V^- is contained in at most one member of $\mathcal{S}^-$. Since G^+ and G^- act by affine permutations restricted to V^+ and V^-, respectively, G^+ is a group of automorphisms of $(V^+,\mathcal{S}^+)$ and G^- is a group of automorphisms of $(V^-,\mathcal{S}^-)$. It remains to show that the affine geometry V over $\mathbb{F}_2$ has planes X^+ and X^- such that $X^+ \subseteq V^+$ and $X^- \subseteq V^-$. Indeed, if such planes exist, then $\mathcal{S}^+$ contains the set X^+, $\mathcal{S}^-$ contains

the set X^-, and because of $d \geq 3$ we have that $3 < |X^+| = |X^-| = 4 \leq 2^{2d-2} < |V^-| < |V^+|$. Hence it follows from Claim 4.4 that (WH_4) fails for both G^+ and G^-.

To find a plane $X^+ \subseteq V^+$ we have to find four distinct vectors $a, b, c, d \in V^+$ such that $a + b + c + d = 0$. All vectors we select will have 4th, ..., dth and $(d+4)$th, ..., $(2d)$th coordinates equal to 0, therefore we won't write out these coordinates. A possible choice for a, b, c, d is

$$\begin{aligned} a &= [0\ 0\ 0\ \ldots\ 0\ 0\ 0\ \ldots]^{\mathrm{T}}, \\ b &= [1\ 1\ 0\ \ldots\ 1\ 1\ 0\ \ldots]^{\mathrm{T}}, \\ c &= [1\ 0\ 1\ \ldots\ 1\ 0\ 1\ \ldots]^{\mathrm{T}}, \\ d &= [0\ 1\ 1\ \ldots\ 0\ 1\ 1\ \ldots]^{\mathrm{T}}. \end{aligned}$$

By adding the vector $[1\ 0\ 0\ \ldots\ 1\ 0\ 0\ \ldots]^{\mathrm{T}}$ to a, b, c, d we get four vectors that form a plane contained in V^-. This completes the proof of Claim 4.16.

Unitary groups (Row 6 of Table 1)

The group $\mathsf{PSU}(3, q)$ is defined as follows. Let $K = \mathbb{F}_{q^2}$, and let $V = K^3$ be the 3-dimensional (column) vector space over K. The field K has a unique automorphism of order 2, namely $K \to K$, $\alpha \mapsto \bar{\alpha} = \alpha^q$. This automorphism, acting entry-by-entry, induces a skew linear transformation of V and an automorphism of $GL(3, q^2)$, which will also be denoted by $\bar{}$. Let $\varphi\colon V \times V \to K$ denote the Hermitian form defined by $\varphi(v, w) = v^{\mathrm{T}}\bar{w}$ for all $v, w \in V$. The unitary group $\mathsf{GU}(3, q)$ is defined as the subgroup of $\mathsf{GL}(3, q^2)$ consisting of all Hermitian matrices; that is, $M \in \mathsf{GL}(3, q^2)$ belongs to $\mathsf{GU}(3, q)$ if and only if $\varphi(Mv, Mw) = \varphi(v, w)$ for all $v, w \in V$, or equivalently, $M^{\mathrm{T}}\bar{M} = I$.

The group $\mathsf{GU}(3, q)$ acts on the 1-dimensional subspaces of K (that is, on the points of the projective plain P over K); the induced group is the projective unitary group $\mathsf{PGU}(3, q)$, which is a subgroup of $\mathsf{PGL}(3, q^2)$. The subgroup $\mathsf{PGU}(3, q) \cap \mathsf{PSL}(3, q^2)$ of $\mathsf{PGU}(3, q)$ is the projective special unitary group $\mathsf{PSU}(3, q)$. The group $\mathsf{PGU}(3, q)$ can be extended by the field automorphisms of K to yield a group $\mathsf{P\Gamma U}(3, q)$; the construction is analogous to the construction of $\mathsf{P\Gamma L}(3, q^2)$ from $\mathsf{PGL}(3, q^2)$.

To describe the 2-transitive action of $\mathsf{P\Gamma U}(3, q)$, recall that a vector $v \in V$ is called isotropic if $\varphi(v, v) = 0$. If $v \in V$ is isotropic, then so is Mv for each $M \in \mathsf{PGU}(3, q)$ and so is the image of v under (the coordinatewise action of) each automorphism of K. Therefore the action of $\mathsf{P\Gamma U}(3, q)$ on the points of the projective plane P over K can be restricted to the set A of all isotropic points (1-dimensional subspaces $\langle v \rangle$ of V such that $v \in V$ is isotropic). The action of $\mathsf{P\Gamma U}(3, q)$ on A is faithful and 2-transitive; in fact, the action of its subgroup $\mathsf{PSU}(3, q)$ is also 2-transitive (cf. [5], pp. 248–250). This is the 2-transitive action S of $\mathsf{PSU}(3, q)$ with $|A| = q^3 + 1$ indicated in Row 6 of Table 1. Since $\mathsf{PSU}(3, q) \triangleleft \mathsf{P\Gamma U}(3, q)$ and $[\mathsf{P\Gamma U}(3, q) : \mathsf{PSU}(3, q)] = (3, q+1)e$,

we get that $\widehat{S} = \mathsf{P\Gamma U}(3,q)$. Therefore

$$\mathsf{PSU}(3,q) \leq G \leq \mathsf{P\Gamma U}(3,q) \quad (q = p^e \geq 3).$$

Claim 4.17. (WH_3) *fails for all such groups G.*

Let $\overline{\mathcal{S}}$ be the family of all lines of the projective plane P over K, and let

$$\mathcal{S} = \{A \cap X : X \in \overline{\mathcal{S}}\}.$$

Then $(P; \overline{\mathcal{S}})$ is an $\mathrm{S}(2, q^2+1, q^4+q^2+1)$ Steiner system, and $(A; \mathcal{S})$ is its subsystem induced on A. It follows that each 2-element subset of A is contained in at most one member of $\mathcal{S}$. The facts established in the preceding paragraph show that $\mathsf{P\Gamma U}(3,q)$, and hence also G, is a group of automorphisms of $(A; \mathcal{S})$. Now select two distinct points $a, b \in A$, and let $X \in \overline{\mathcal{S}}$ be the line containing a, b. It can be shown that $|A \cap X| = q+1$ (see Exercise 7.7.12 in [5]), so $A \cap X$ is a member of $\mathcal{S}$ such that $2 < |A \cap X| = q+1 < q^3+1 = |A|$. Thus Claim 4.4 implies that (WH_3) fails for G, and completes the proof of Claim 4.17.

<u>*Suzuki groups*</u> (Row 7 of Table 1)

The 2-transitive action of the Suzuki group $\mathsf{Sz}(q)$ ($q = 2^{2d+1} > 2$), which is referred to in Row 7 of Table 1, is a group of automorphisms of an $\mathrm{S}(3, q+1, q^2+1)$ Steiner system $(A; \mathcal{S})$ that can be defined as follows. Let $K = \mathbb{F}_q$, $q = 2^{2d+1} > 2$, and let P be the projective 3-space over K; that is, the points of P are the 1-dimensional subspaces of the vector space K^4. Let A be the subset of P that consists of the point $\langle [1\ 0\ 0\ 0]^{\mathrm{T}} \rangle$ together with all points

$$\langle [xy + x^{2^{d+1}+2} + y^{2^{d+1}} \quad y \quad x \quad 1]^{\mathrm{T}} \rangle, \qquad x, y \in K.$$

The set A has q^2+1 elements. By Theorem 3.3 of Chapter XI of [11], $\mathsf{Sz}(q)$ is the subgroup of $\mathsf{PGL}(4,q)$ that leaves A invariant, and $\mathsf{Sz}(q)$ acts 2-transitively on A. If $\mathcal{S}$ consists of the intersections of the projective planes in P with A, then $(A; \mathcal{S})$ is a set system invariant under $\mathsf{Sz}(q)$, which is an $\mathrm{S}(3, q+1, q^2+1)$ Steiner system (see [4], p. 104). $(A; \mathcal{S})$ is also invariant under the field automorphisms from $\mathsf{P\Gamma L}(4,q)$. Hence the field automorphisms together with $\mathsf{Sz}(q)$ $\big(\leq \mathsf{PGL}(4,q)\big)$ generate a subgroup $\overline{\mathsf{Sz}}(q)$ of $\mathsf{P\Gamma L}(4,q)$ such that $\overline{\mathsf{Sz}}(q)$ is also a 2-transitive group of automorphisms of $(A; \mathcal{S})$ and $\mathsf{Sz}(q) \lhd \overline{\mathsf{Sz}}(q)$. Since $S = \mathsf{Sz}(q) \lhd \overline{\mathsf{Sz}}(q) \leq \widehat{S}$ and $[\overline{\mathsf{Sz}}(q) : \mathsf{Sz}(q)] = 2d+1 = [\widehat{S} : S]$, it follows that $\overline{\mathsf{Sz}}(q) = \widehat{S}$ is the group of all automorphisms of $(A; \mathcal{S})$.

Claim 4.18. *Condition* (WH_4) *fails for all such groups G.*

The fact that $\overline{\mathsf{Sz}}(q)$ is a group of automorphisms of an $\mathrm{S}(3, q+1, q^2+1)$ Steiner system where $3 < q+1 \leq q^2+1$ (since $q > 2$), implies by Claim 4.5 that (WH_4) fails for each subgroup G of $\overline{\mathsf{Sz}}(q)$. This completes the proof of Claim 4.18.

Ree groups (Row 8 of Table 1)

The 2-transitive action of the Ree group $\mathsf{R}_1(q)$ ($q = 3^{2d+1} > 3$) is a group of automorphisms of an $\mathrm{S}(2, q+1, q^3+1)$ Steiner system $(A; \mathcal{S})$. One way to describe this Steiner system is analogous to the above discussion of the Steiner system associated to a Suzuki group (see [5], pp. 251–252). We will follow a different description which is outlined in [4] (pp. 104–105).

Let P be a Sylow 3-subgroup of $\mathsf{R}_1(q)$, and let M be the normalizer of P in $\mathsf{R}_1(q)$. We will use the following facts on $\mathsf{R}_1(q)$ from [19] (see p. 797) and from Chapter XI, Theorem 13.2 in [11].

(1) $\mathsf{R}_1(q)$ acts 2-transitively on the set $A = \{gM : g \in \mathsf{R}_1(q)\}$ of left cosets of M by left multiplication, and $|A| = q^3 + 1$. From now on $\mathsf{R}_1(q)$ will denote the 2-transitive subgroup of S_A obtained in this way.
(2) A two-point stabilizer $\mathsf{R}_1(q)_{x,y}$ in $\mathsf{R}_1(q)$ is a cyclic group of order $q-1$, so it contains a unique involution $\iota_{x,y}$.
(3) Every involution in $\mathsf{R}_1(q)$ has at least three fixed points.

For distinct elements $x, y \in A$ let $B_{x,y}$ denote the set of fixed points of $\iota_{x,y}$, and let $\mathcal{S} = \{B_{x,y} : x, y \in A,\ x \neq y\}$. Then $(A; \mathcal{S})$ is a set system that satisfies conditions (i)–(ii) in Claim 4.4 for $k = 2$. In fact, it can be shown (see [4], pp. 104–105) that $(A; \mathcal{S})$ is an $\mathrm{S}(2, q+1, q^3+1)$ Steiner system.

Now let $\overline{\mathsf{R}}_1(q)$ denote the normalizer of $\mathsf{R}_1(q) \leq \mathsf{S}_A$ in S_A. We claim that $\overline{\mathsf{R}}_1(q)$ is a group of automorphisms of $(A; \mathcal{S})$. To see this let $\pi \in \overline{\mathsf{R}}_1(q)$ and $x, y \in A$, $x \neq y$. Since π normalizes $\mathsf{R}_1(q)$, it conjugates $\mathsf{R}_1(q)_{x,y}$ into a subgroup of $\mathsf{R}_1(q)$ that fixes $\pi(x)$ and $\pi(y)$. Therefore $\pi \circ \mathsf{R}_1(q)_{x,y} \circ \pi^{-1} = \mathsf{R}_1(q)_{\pi(x),\pi(y)}$. This implies that $\pi \circ \iota_{x,y} \circ \pi^{-1} = \iota_{\pi(x),\pi(y)}$ and $\pi(B_{x,y}) = B_{\pi(x),\pi(y)}$. Hence π is an automorphism of $(A; \mathcal{S})$, as claimed.

Thus, for $S = \mathsf{R}_1(q)$ from Row 8 of Table 1 we have $\widehat{S} = \overline{\mathsf{R}}_1(q)$, so in this case

$$\mathsf{R}_1(q) \leq G \leq \overline{\mathsf{R}}_1(q) \quad (q = 3^{2d+1} > 3).$$

Claim 4.19. *Condition* (WH_3) *fails for all such groups* G.

We saw above that $\overline{\mathsf{R}}_1(q)$ is a group of automorphisms of the set system $(A; \mathcal{S})$ which satisfies conditions (i)–(ii) in Claim 4.4 for $k = 2$. Thus we get from Claim 4.4 that (WH_3) fails for each subgroup G of $\overline{\mathsf{R}}_1(q)$.

The Mathieu groups and their subgroups (Rows 9–12 and 14–16 of Table 1)

We will use the following well known facts on the Mathieu groups and their subgroups.

(1) $\mathsf{M}_{12} \leq \mathsf{S}_{12}$ is 5-transitive, and is the automorphism group of an $\mathrm{S}(5, 6, 12)$ Steiner system. (See Theorem 6.3B in [5].)

(2) $\mathsf{M}_{11} \leq \mathsf{S}_{11}$ is 4-transitive, and is the automorphism group of an $\mathrm{S}(4, 5, 11)$ Steiner system. (See Theorem 6.4A in [5].)
(3) M_{11} has a 3-transitive action on $\underline{12}$, which is a subgroup of M_{12}. (See Theorem 6.18 in [6].)
(4) $\mathsf{PSL}(2, 11)$ has a 2-transitive action on $\underline{11}$, which is a subgroup of M_{11}. (See Proposition 6.22 in [6].)
(5) $\mathsf{M}_{24} \leq \mathsf{S}_{24}$ is 5-transitive, and is the automorphism group of an $\mathrm{S}(5, 8, 24)$ Steiner system. (See Theorem 6.7C in [5].)
(6) $\mathsf{M}_{23} \leq \mathsf{S}_{23}$ is 4-transitive, and is the automorphism group of an $\mathrm{S}(4, 7, 23)$ Steiner system. (See Theorem 6.7B in [5].)
(7) $\overline{\mathsf{M}}_{22} \leq \mathsf{S}_{22}$ is 3-transitive, and is the automorphism group of an $\mathrm{S}(3, 6, 22)$ Steiner system. (See Theorem 6.6D in [5].)
(8) $\overline{\mathsf{M}}_{22} = (\mathsf{M}_{24})_{\{\alpha,\beta\}}$ is the stabilizer of a two-element set in M_{24}. An index 2 subgroup in $\overline{\mathsf{M}}_{22}$ is $\mathsf{M}_{22} = (\mathsf{M}_{24})_{\alpha,\beta}$, the two-point stabilizer of M_{24}. (See p. 204 in [5].)

By Table 1, if S is one of the groups in (1)–(6), then $\widehat{S} = S$, while if $S = \mathsf{M}_{22}$ then $[\widehat{S} : S] = 2$. Since $\overline{\mathsf{M}}_{22}$ normalizes M_{22} and $[\overline{\mathsf{M}}_{22} : \mathsf{M}_{22}] = 2$, we get that $\widehat{S} = \overline{\mathsf{M}}_{22}$ in this case. Hence for S as in Rows 9–12 and 14–16 of Table 1 the 2-transitive groups G satisfying $S \leq G \leq \widehat{S}$ are exactly the groups listed in (1)–(8) above. All these groups are groups of automorphisms of Steiner systems, therefore Claim 4.5 implies the following.

Claim 4.20.
- (WH_6) *fails for* M_{24}, M_{12}, *and the* 3*-transitive action of* M_{11} *on a* 12*-element set.*
- (WH_5) *fails for* M_{23}, M_{11}, *and the* 2*-transitive action of* $\mathsf{PSL}(2, 11)$ *on an* 11*-element set.*
- (WH_4) *fails for* M_{22} *and* $\overline{\mathsf{M}}_{22}$.

$\underline{\mathsf{A}_7 \text{ acting on a } 15\text{-element set}}$ (Row 13 of Table 1)

The alternating group A_7 acting on a 15-element set is a subgroup of $\mathsf{PSL}(4, 2)$ with its natural action on the 15 points of the projective 3-space over $\mathbb{F}_2$ (see [2], p. 9). By Claim 4.9 (WH_3) fails for this action of $\mathsf{PSL}(4, 2)$, hence (WH_3) fails for all of its subgroups. This proves the following claim.

Claim 4.21. (WH_3) *fails for the alternating group* A_7 *acting on a* 15*-element set.*

$\mathsf{PSL}(2,8)$ *acting on a* 28*-element set* (Row 17 of Table 1)

For the permutation groups S and $\widehat{S}$ in Row 17 of Table 1 we will use the description that appears on pp. 22–24 of [3]. Let P be a Sylow 3-subgroup of the group $\mathsf{P\Gamma L}(2,8)$, and let M be the normalizer of P in $\mathsf{P\Gamma L}(2,8)$. Then $[\mathsf{P\Gamma L}(2,8) : M] = 28$, and $\mathsf{P\Gamma L}(2,8)$ acts faithfully and 2-transitively on the 28-element set A of left cosets of M by left multiplication. The image of this action is the 2-transitive permutation group $\widehat{S}$. Its commutator subgroup S has index 3 in $\widehat{S}$, and is isomorphic to $\mathsf{PGL}(2,8) = \mathsf{PSL}(2,8)$. The group S acts primitively, but not 2-transitively on A.

Therefore, if G is a 2-transitive permutation group on A such that $S \leq G \leq \widehat{S}$, then $G = \widehat{S}$, that is, G is the 2-transitive action of $\mathsf{P\Gamma L}(2,8)$ on a 28-element set.

Claim 4.22. (WH_3) *fails for the* 2*-transitive action of* $\mathsf{P\Gamma L}(2,8)$ *on a* 28*-element set.*

This claim can be established with the aid of the computer algebra system GAP, as we now explain. Let G denote the 2-transitive action of $\mathsf{P\Gamma L}(2,8)$ on a 28-element set A. We want to look at the natural action of G on the 3-element subsets of A. GAP calculations show that there are six G-orbits of 3-element sets: two orbits of size 252, one orbit of size 504, and three orbits of size 756. Choose a 3-element set $C = \{a, b, c\}$ from the orbit of size 504, and let $B = C \cup \{u\}$ where $u \in A - C$. One can check with GAP that for 16 of the 25 possible choices of u, the 3-element subsets of B that contain u are not in the same G-orbit as C. Such a choice of B and C witnesses the failure of (WH_3), and hence proves Claim 4.22.

The Higman–Sims group (Row 18 of Table 1)

The Higman–Sims group HS acting on a 176-element set is the automorphism group of a combinatorial geometry $(A; \mathcal{S})$ consisting of a set A of 176 points and a set $\mathcal{S}$ of 176 quadrics such that each quadric consists of 50 points, each point is in 50 quadrics, each pair of distinct points is incident with exactly 14 quadrics, and each pair of distinct quadrics is incident with exactly 14 points (see [5], pp. 252–253). Thus any 15 points are contained in at most one quadric. Therefore $(A; \mathcal{S})$ is a set system that satisfies the assumptions of Claim 4.4 for $k = 15$. Hence we get the following.

Claim 4.23. (WH_{16}) *fails for* HS *acting on a* 176*-element set.*

The Conway group (Row 19 of Table 1)

First we will describe the 2-transitive action of the Conway group Co_3. We will follow the treatment in [6], Chapter 9–10.

Let $(\underline{24}, \mathcal{S}_{24})$ be the $\mathrm{S}(5, 8, 24)$ Steiner system whose automorphism group is the Mathieu group M_{24}. This Steiner system is unique, up to isomorphism, and is determined by *the binary Golay code*, which can be defined as follows. Let $P(\Omega)$ denote

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
O_1	0	1	1	1	1	0	0	0	1	0	0	0	1	0	0	0	1	0	0	0	1	0	0	0
O_2	1	0	0	0	0	1	1	1	1	0	0	0	1	0	0	0	1	0	0	0	1	0	0	0
O_3	1	0	0	0	1	0	0	0	0	1	1	1	1	0	0	0	1	0	0	0	1	0	0	0
O_4	1	0	0	0	1	0	0	0	1	0	0	0	0	1	1	1	1	0	0	0	1	0	0	0
O_5	1	0	0	0	1	0	0	0	1	0	0	0	1	0	0	0	0	1	1	1	1	0	0	0
O_6	1	0	0	0	1	0	0	0	1	0	0	0	1	0	0	0	1	0	0	0	0	1	1	1
O_7	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0	0	0	0	0	0	0	0	0
O_8	0	0	0	0	0	0	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0
O_9	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	0	0	0	0	0	0	0	0
O_{10}	0	0	0	0	0	0	0	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0
O_{11}	0	0	0	0	1	1	0	0	0	0	0	0	1	1	0	0	1	0	1	0	1	0	0	1
O_{12}	0	0	0	0	1	0	1	0	0	0	0	0	1	0	1	0	1	0	0	1	1	1	0	0

TABLE 4. Standard basis of the Golay code

the set of all subsets of $\Omega = \underline{24}$, and let $\oplus$ denote symmetric difference on $P(\Omega)$. The binary Golay code is the subgroup $\mathcal{G}$ of $(P(\Omega); \oplus)$ generated by the sets $O_1, \ldots, O_{12}$ listed by their characteristic functions in Table 4. Alternatively, the binary Golay code can be described as the subspace of $\mathbb{F}_2^{24}$ generated by the vectors in Table 4.

It can be shown that $\emptyset, \Omega \in \mathcal{G}$ and every set $S \in \mathcal{G}$ such that $S \neq \emptyset, \Omega$ has 8, 12, or 16 elements. The 8-element sets in $\mathcal{G}$ are called *octads*, and the 12-element sets in $\mathcal{G}$ are called *dodecads*.

Next we will describe *the standard Leech lattice*. Let $(\cdot, \cdot)$ denote the standard inner product in the 24-dimensional $\mathbb{R}$-space $\mathbb{R}^\Omega$, and let $\{\alpha_i : i \in \Omega\}$ be a basis of $\mathbb{R}^\Omega$ such that $(\alpha_i, \alpha_j) = 2\delta_{ij}$ for all i, j. For any set $S \subseteq \Omega$ and $i \in \Omega$ we will use the following notation:

$$\alpha_S := \sum_{k \in S} \alpha_k \qquad \text{and} \qquad \nu_i := \tfrac{1}{4}\alpha_\Omega - \alpha_i.$$

The standard Leech lattice Λ is the additive subgroup of $\mathbb{R}^\Omega$ generated by the following vectors:

$$\alpha_i \pm \alpha_j \ (i, j \in \Omega), \qquad \tfrac{1}{2}\alpha_S \ (S \in \mathcal{G}), \qquad \nu_i \ (i \in \Omega).$$

It is easy to check that (v, v) is an even integer for each one of these generating vectors. Hence (v, v) is an even integer for all $v \in \Lambda$. A vector $v \in \Lambda$ is said to have *type* n if $(v, v) = 2n$. A *triangle of type* 223 is a set $\{u, v, x\}$ of vectors in Λ such that $u + v + x = 0$ and u, v are of type 2 while x is of type 3.

The automorphism group of the Leech lattice, denoted $\mathrm{Aut}(\Lambda)$, consists of all automorphisms of Λ as an abelian group which also preserve the bilinear form $(\cdot, \cdot)$

on Λ. For any set $S \in \mathcal{G}$ the linear map $\varepsilon_S \colon \mathbb{R}^\Omega \to \mathbb{R}^\Omega$ defined by

$$\varepsilon_S(\alpha_i) = \begin{cases} -\alpha_i & \text{if } i \in S \\ \alpha_i & \text{if } i \notin S \end{cases}$$

restricts to an automorphism of Λ.

We will need the following facts on Λ and $\mathrm{Aut}(\Lambda)$:

(1) If $v \in 2\Lambda$ then (v, v) is divisible by 8.
(2) $\mathrm{Aut}(\Lambda)$ preserves the types of vectors, and maps 2Λ to itself.
(3) The set of vectors of type 2 in Λ is the disjoint union of the following three sets:

$$\{\tfrac{1}{2}\varepsilon_S(\alpha_O) : O, S \in \mathcal{G},\ O \text{ an octad}\},$$
$$\{\varepsilon_S(\nu_i) : i \in \Omega,\ S \in \mathcal{G}\},$$
$$\{\pm\alpha_i \pm \alpha_j : i, j \in \Omega,\ i \neq j\}.$$

(4) For $n = 2$ and 3, $\mathrm{Aut}(\Lambda)$ acts transitively on the set of vectors of type n.
(5) For any $i \in \Omega$, the vector

$$x_i = \frac{1}{4}\Big(5\alpha_i + \sum_{j \neq i} \alpha_j\Big)$$

is of type 3.
(6) There are exactly 276 triangles of type 223 in which the type 3 member is x_i; 23 of them are of the form

$$\triangle_j = \{-\nu_j,\ -(\alpha_i + \alpha_j),\ x_i\} \quad (j \in \Omega,\ j \neq i),$$

and 253 are of the form

$$\triangle_O = \{-\tfrac{1}{2}\alpha_O,\ \varepsilon_{\Omega - O}(\nu_i),\ x_i\} \quad (O \in \mathcal{G} \text{ an octad}, i \in O).$$

Statements (1), (2), and (5) follow from the definitions. Statements (3) and (6) are taken from Theorem 9.2 and Exercise 10.2 in [6], while (4) is taken from Proposition 9.9 and Theorem 9.20 in [6].

The *Conway group* Co_3 is the stabilizer in $\mathrm{Aut}(\Lambda)$ of a vector x of type 3. This group acts 2-transitively on the set of triangles of type 223 containing x (see Theorem 10.3 in [6]). By the transitivity in (4) neither this definition of Co_3 nor its 2-transitive action depends on the choice of x. We will select and fix x to be one of the vectors x_i in (5), and we will use the description, given in (6), of the triangles of type 223 containing x_i.

Claim 4.24. (WH_8) *fails for* Co_3 *acting on a* 276*-element set.*

To prove the claim let $i = 13$ and let

$$A = \{\triangle_j : j \in \Omega,\ j \neq i\} \cup \{\triangle_O : O \in \mathcal{G} \text{ an octad},\ i \in O\}$$

be the set of triangles of type 223 containing x_i (see (6) above). Furthermore, let T_7, T_8, T_9, T_{10} be the octads in $\mathcal{G}$ defined as follows:

$$T_7 = O_1 \oplus O_2 \oplus O_7, \qquad T_8 = O_5 \oplus O_6 \oplus O_8,$$
$$T_9 = O_1 \oplus O_2 \oplus O_9, \qquad T_{10} = O_5 \oplus O_6 \oplus O_{10},$$

and let

$$\mathfrak{I} = \{O_7, O_8, O_9, O_{10}, T_7, T_8, T_9, T_{10}\}.$$

Since $i = 13$ is a member of each octad in $\mathfrak{I} \cup \{O_5\}$, we see that

$$C = \{\triangle_O : O \in \mathfrak{I}\} \qquad \text{and} \qquad B = C \cup \{\triangle_{O_5}\}$$

are subset of A. The nine triangles in B are pairwise distinct, therefore $|B| = 9$ and $|C| = 8$. Our goal is to show that B and C witness the failure of (WH_8)

The set C has following property:

($*$) one can select one vertex of type 2 of each triangle in the set so that the sum of the eight selected vectors is in 2Λ.

Indeed, select the vertices $-\frac{1}{2}\alpha_O$ ($O \in \mathfrak{I}$). Then

$$-\big(\tfrac{1}{2}\alpha_{O_7} + \tfrac{1}{2}\alpha_{O_8} + \tfrac{1}{2}\alpha_{T_7} + \tfrac{1}{2}\alpha_{T_8}\big) + \big(\tfrac{1}{2}\alpha_{O_9} + \tfrac{1}{2}\alpha_{O_{10}} + \tfrac{1}{2}\alpha_{T_9} + \tfrac{1}{2}\alpha_{T_{10}}\big)$$
$$= -2(\alpha_{10} + \alpha_{14}) + 2(\alpha_{11} + \alpha_{15}) \in 2\Lambda.$$

Hence

(4.12)
$$\sum_{O \in \mathfrak{I}} -\tfrac{1}{2}\alpha_O \equiv -\big(\tfrac{1}{2}\alpha_{O_7} + \tfrac{1}{2}\alpha_{O_8} + \tfrac{1}{2}\alpha_{T_7} + \tfrac{1}{2}\alpha_{T_8}\big) + \big(\tfrac{1}{2}\alpha_{O_9} + \tfrac{1}{2}\alpha_{O_{10}} + \tfrac{1}{2}\alpha_{T_9} + \tfrac{1}{2}\alpha_{T_{10}}\big)$$
$$\equiv 0 \pmod{2\lambda},$$

proving ($*$).

It follows from statement (2) above that for every automorphism $\pi \in \mathsf{Co}_3 \leq \mathrm{Aut}(\Lambda)$, the set $\pi(C)$ of triangles shares property ($*$). Therefore the failure of (WH_8) will be established if we show that no 8-element subset D of B that contains $\triangle_{O_5}$ has property ($*$).

Let D be an 8-element subset of B such that $\triangle_{O_5} \in D$. Then $D = \{\triangle_O : O \in \mathfrak{J}_S\}$ where $\mathfrak{J}_S = (\mathfrak{I} - \{S\}) \cup \{O_5\}$ for some $S \in \mathfrak{I}$. Let v_O be a vertex of type 2 of $\triangle_O$ ($O \in \mathfrak{J}_S$). We want to show that

$$\sum_{O \in \mathfrak{J}_S} v_O \not\equiv 0 \pmod{2\Lambda}. \tag{4.13}$$

It follows from statement (6) that for each O, either $v_O = -\frac{1}{2}\alpha_O$ or $v_O = \varepsilon_{\Omega - O}(\nu_i)$. In the second case

$$v_O = \varepsilon_{\Omega - O}(\nu_i) = \tfrac{1}{2}\alpha_O - x_i \equiv -\tfrac{1}{2}\alpha_O - x_i \pmod{2\Lambda},$$

because the vertices of a triangle sum to 0. Let k be the number of octads $O \in \mathfrak{J}_S$ for which $v_O = \frac{1}{2}\alpha_O - x_i$. Then

$$\sum_{O\in\mathfrak{J}_S} v_O \equiv kx_i + \sum_{O\in\mathfrak{J}_S} -\tfrac{1}{2}\alpha_O \pmod{2\Lambda}.$$

Combining this with (4.12) we get that

$$\begin{aligned}\sum_{O\in\mathfrak{J}_S} v_O &\equiv \sum_{O\in\mathfrak{J}_S} v_O - \sum_{O\in\mathfrak{I}} -\tfrac{1}{2}\alpha_O \\ &\equiv kx_i + \sum_{O\in\mathfrak{J}_S} -\tfrac{1}{2}\alpha_O - \sum_{O\in\mathfrak{I}} -\tfrac{1}{2}\alpha_O \\ &\equiv (-1)^k x_i - \tfrac{1}{2}\alpha_{O_5} + \tfrac{1}{2}\alpha_S \pmod{2\Lambda}.\end{aligned}$$

Let $w_S = \frac{1}{2}\alpha_S - \frac{1}{2}\alpha_{O_5}$ and $w'_S = w_S - x_i$. To prove (4.13) we have to show that $w_S, w'_S \notin 2\Lambda$. Since

$$w_S = \sum_{j\in S-O_5} \tfrac{1}{2}\alpha_j - \sum_{j\in O_5-S} \tfrac{1}{2}\alpha_j$$

and either $|S - O_5| = |O_5 - S| = 4$ or $|S - O_5| = |O_5 - S| = 6$, we get that

$$(w_S, w_S) = \sum_{j\in S-O_5} (\tfrac{1}{2}\alpha_j, \tfrac{1}{2}\alpha_j) + \sum_{j\in O_5-S} (-\tfrac{1}{2}\alpha_j, -\tfrac{1}{2}\alpha_j) = 2\cdot\tfrac{1}{4}(|S-O_5|+|O_5-S|) = 4 \text{ or } 6.$$

Hence, by statement (1), $w_S \notin 2\Lambda$. Notice that $i \notin (S - O_5) \cup (O_5 - S) = S \oplus O_5$ because $i \in S \cap O_5$. Therefore

$$w'_S = -\tfrac{5}{4}\alpha_i + \sum_{j\in S-O_5} \tfrac{1}{4}\alpha_j + \sum_{j\in O_5-S} -\tfrac{3}{4}\alpha_j + \sum_{j\notin(S\oplus O_5)\cup\{i\}} -\tfrac{1}{4}\alpha_j,$$

whence

$$\begin{aligned}(w'_S, w'_S) &= 2\tfrac{25}{16} + 2\tfrac{1}{16}|S - O_5| + 2\tfrac{9}{16}|O_5 - S| + 2\tfrac{1}{16}(24 - |(S \oplus O_5) \cup \{i\}|) \\ &= 10 \text{ or } 12.\end{aligned}$$

Thus we get as before that $w'_S \notin 2\Lambda$. This completes the proof of Claim 4.24 and also of Theorem 4.1. □

5. The weakly homogeneous groups that are not homogeneous

By Theorems 2.3 and 4.1, $\mathsf{PSL}(2,5)$ and $\mathsf{PGL}(2,7)$ are the only weakly homogeneous groups that fail to be m-homogeneous for some m. In fact, by Claims 4.14 and 4.15, $\mathsf{PSL}(2,5)$ has two orbits of 3-element sets and is k-homogeneous for all $k \neq 3$, while $\mathsf{PGL}(2,7)$ has two orbits of 4-element sets and is k-homogeneous for all $k \neq 4$. In this section we establish some properties of these groups that are needed in the sequel.

Lemma 5.1. *Let $G = \mathsf{PSL}(2,5)$ with its action on the projective line A over $\mathbb{F}_5$.*

(1) *Every partition* $\{B_1, B_2, B_3\}$ *of* A *has transversals in each* G*-orbit of* 3*-element sets.*
(2) *For every* 5*-element subset* B *of* A *and for any distinct elements* b, b' *of* B*, each* G*-orbit of* 3*-element sets contains a set* S *such that* $\{b, b'\} \subset S \subset B$.

Proof. In the proof we will use the geometrical description of the two $\mathsf{PSL}(2,5)$-orbits of 3-element sets; see the remark following Claim 4.14.

(1) Let $\{B_1, B_2, B_3\}$ be a partition of A. We may assume without loss of generality that $|B_1| \leq |B_2| \leq |B_3|$. Suppose first that $|B_1| = 1$. Since G is 2-transitive on A, we may also assume that $B_1 = \{\infty\}$ and $0 \in B_2$. Thus $\{B_2, B_3\}$ is a partition of $\mathbb{F}_5$ with $|B_3| \geq 3$. One can check that there exist $b, b' \in B_3$ such that $0, b$ is a side, while $0, b'$ is a diagonal of the pentagon. Consequently the transversals $\{\infty, 0, b\}$ and $\{\infty, 0, b'\}$ belong to distinct G-orbits.

Now suppose that $|B_1| > 1$. Then $|B_1| = |B_2| = |B_3| = 2$, so by the 2-transitivity of G we may assume that $B_1 = \{\infty, 0\}$. It is easy to check that there exist elements $a, a' \in B_2$ and $b, b' \in B_3$ such that a, b is a side, while a', b' is a diagonal of the pentagon. As before, it follows that the transversals $\{\infty, a, b\}$ and $\{\infty, a', b'\}$ belong to distinct G-orbits. This completes the proof of (1)

(2) Let B be a 5-element subset of A. Since G acts transitively on the projective line $A = \mathbb{F}_5 \cup \{\infty\}$ over $\mathbb{F}_5$, we may assume that $B = \mathbb{F}_5$. For any two distinct vertices b, b' of the pentagon B, there exist vertices s, s' such that $\{b, b', s\}$ is an isosceles triangle whose base is a side, and $\{b, b', s'\}$ is an isosceles triangle whose base is a diagonal of the pentagon. This proves (2). □

Lemma 5.2. *Let* $G = \mathsf{PGL}(2,7)$ *with its action on the projective line* A *over* $\mathbb{F}_7$.

(1) *Every partition* $\{B_1, B_2, B_3, B_4\}$ *of* A *has transversals in each* G*-orbit of* 4*-element sets.*
(2) *For every* 6*-element subset* B *of* A *and for any distinct elements* b, b' *of* B*, each* G*-orbit of* 4*-element sets contains a set* S *such that* $\{b, b'\} \subset S \subset B$.

Proof. The proof of this lemma relies on the description of the two $\mathsf{PGL}(2,7)$-orbits of 4-element sets in Claim 4.15 (2).

(1) Let $\{B_1, B_2, B_3, B_4\}$ be a partition of $A = \mathbb{F}_7 \cup \{\infty\}$. Since G acts 3-transitively on A, we may assume without loss of generality that $|B_2| \leq |B_1|, |B_4| \leq |B_3|$ and $0 \in B_1$, $1 \in B_2$, $\infty \in B_4$. Thus, for every element $u \in B_3 \subseteq \mathbb{F}_7$, we have $\mathrm{crr}(0, 1, u, \infty) = u$. If B_3 intersects both cross ratio orbits $\{3, 5\}$ and $\{2, 4, 6\}$, then we get two transversals of the form $\{0, 1, u, \infty\}$ that belong to distinct G-orbits. Otherwise, if $|B_3| \geq 3$ then

(i) $B_2 = \{1\}$ and $B_3 = \{2, 4, 6\} = \{3^2, 3^3, 3^4\}$,

while if $|B_3| < 3$ then

(ii) $|B_1| = |B_2| = |B_3| = |B_4| = 2$ and B_3 is one of the sets $\{3, 5\} = \{3, 3^5\}$, $\{2, 4\} = \{3^2, 3^4\}$, $\{2, 6\} = \{3^2, 3^3\}$, or $\{4, 6\} = \{3^4, 3^3\}$.

In case (i) the cross ratio orbit $\{3,5\}$ has a nonempty intersection with B_1 or B_4. Since our assumptions and conclusions on the partition $\{B_1,B_2,B_3,B_4\}$ are invariant under performing the transformation $x \mapsto 1/x$ from G and simultaneously switching the role of B_1 and B_4, we may assume that $\{3,5\}$ has a nonempty intersection with B_1. Let $v \in \{3,5\} \cap B_1$. Then $v+1 \in \{2,4,6\} = B_3$. Thus the transversals $\{0,1,v+1,\infty\}$ and $\{v,1,v+1,\infty\}$ belong to distinct G-orbits, as $\mathrm{crr}(0,1,v+1,\infty) = v+1 \in \{2,4,6\}$ and $\mathrm{crr}(v,1,v+1,\infty) = 1/(1-v) \in \{3,5\}$.

Now we will consider case (ii). If $B_3 = \{3,3^5\}$ then $B_2 = \{1,u\}$ for some $u \in \{3^2,3^3,3^4\}$. For each such u there exists $v \in \{3,3^5\} = B_3$ with $v/u \in \{3^2,3^3,3^4\}$; namely, we can choose $v = 3 = 3^7$ for $u = 3^3, 3^4$, and $v = 3^5$ for $u = 3^2$. Thus the transversals $\{0,1,v,\infty\}$ and $\{0,u,v,\infty\}$ belong to distinct G-orbits, as $\mathrm{crr}(0,1,v,\infty) = v \in \{3,3^5\}$ and $\mathrm{crr}(0,u,v,\infty) = v/u \in \{3^2,3^3,3^4\}$. Similarly, if $B_3 = \{3^2,3^4\}$ then $B_2 = \{1,u\}$ for some $u \in \{3,3^3,3^5\}$. For each such u there exists $v \in \{3^2,3^4\} = B_3$ with $v/u \in \{3,3^5\}$; namely, we can choose $v = 3^2 = 3^8$ for $u = 3, 3^3$, and $v = 3^4 = 3^{10}$ for $u = 3^5$. Thus the transversals $\{0,1,v,\infty\}$ and $\{0,u,v,\infty\}$ belong to distinct G-orbits, as $\mathrm{crr}(0,1,v,\infty) = v \in \{3^2,3^3,3^4\}$ and $\mathrm{crr}(0,u,v,\infty) = v/u \in \{3,3^5\}$.

Finally, it suffices to consider the case $B_3 = \{3^2,3^3\}$, because the remaining case $B_3 = \{3^4,3^3\}$ can be reduced to it by performing the transformation $x \mapsto 1/x$ from G and simultaneously switching the role of B_1 and B_4. So, let $B_3 = \{3^2,3^3\}$. Then $B_2 = \{1,u\}$ for some $u \in \{3,3^4,3^5\}$. If $u = 3$ or $u = 3^4$ then there exists $v \in \{3^2,3^3\} = B_3$ with $v/u \in \{3,3^5\}$; namely, we can choose $v = 3^2$ for $u = 3$, and $v = 3^3 = 3^9$ for $u = 3^4$. Thus the transversals $\{0,1,v,\infty\}$ and $\{0,u,v,\infty\}$ belong to distinct G-orbits, as before. If $u = 3^5 = 5$, then $B_1 = \{0,w\}$ with $w = 3$ or $w = 4$. Thus the transversals $\{0,1,2,\infty\}$ and $\{w,5,2,\infty\}$ belong to distinct G-orbits, as $\mathrm{crr}(0,1,2,\infty) = 2 \in \{2,4,6\}$ and $\mathrm{crr}(w,5,2,\infty) = (w-2)/(w-5) = 3$ or 5 if $w = 3$ or 4, respectively. This completes the proof of (1).

(2) Let B be a 6-element subset of A. Since $G = \mathsf{PGL}(2,7)$ acts 3-transitively on the projective line $A = \mathbb{F}_7 \cup \{\infty\}$, we may assume without loss of generality that $b = \infty$, $b' = 0$, and $B = A - \{1,a\}$ for some element $a \neq 1$ of the group $\mathbb{F}_7^\times$ of units. The group $\mathbb{F}_7^\times$ is cyclic, and 3 is one of its generators. Therefore $a = 3^k$ for a unique k with $1 \leq k \leq 5$, and

$$B = \{\infty,0\} \cup \{3^i : 1 \leq i \leq 5,\ i \neq k\}.$$

By the description of the two G-orbits of 4-element sets, we need to verify that for any choice of k $(1 \leq k \leq 5)$ and for each one of the two cross ratio orbits $C = \{3,5\} = \{3,3^5\}$ and $C = \{2,4,6\} = \{3^2,3^3,3^4\}$ there exist distinct i,j with $1 \leq i,j \leq 5$ and $i,j \neq k$ such that $\mathrm{crr}(0,3^i,3^j,\infty) \in C$. Since $\mathrm{crr}(0,3^i,3^j,\infty) = 3^{j-i}$, what we need to check is that for any choice of k $(1 \leq k \leq 5)$ there exist i,j with $1 \leq i,j \leq 5$ and $i,j \neq k$ such that $j - i \mod 6 = \pm 1$, and there exist distinct i',j' with $1 \leq i',j' \leq 5$ and $i',j' \neq k$ such that $j' - i' \mod 6 \neq \pm 1$. It is easy to see that

these statements are indeed true, since for any choice of k, among the four numbers in $\{1,2,3,4,5\} - \{k\}$ there will be two that are consecutive and there will be two distinct numbers that are not consecutive. This completes the proof of (2). □

6. G-closed clones with constants for weakly homogeneous G

Finally, in this section we establish the implication (iii)⇒(i) in Theorem 2.2. We will describe explicitly all G-closed clones that contain all constants in the case when G is a weakly homogeneous permutation group, that is, when G is one of the groups listed in Theorem 2.2 (iii).

To state the result we need some terminology and notation. We define the *kernel type* of a transformation f on A to be the increasing sequence $\kappa = (k_1, k_2, \dots, k_r)$ of positive integers that lists the sizes of the kernel classes of f. (Thus $0 < k_1 \leq k_2 \leq \cdots \leq k_r$ and $k_1 + k_2 + \cdots + k_r = |A|$.) A transformation f on A is said to have *even kernel type* if in its kernel type $\kappa = (k_1, k_2, \dots, k_r)$ all numbers k_i are even. Transformations of even kernel type exist on A if and only if $|A|$ is even.

For $2 \leq m \leq |A|$ we will use the notation $\mathfrak{R}_m$ for the clone consisting of the projections and all operations whose range has size at most m. Recall from Claims 4.14 and 4.15 that if $G = \mathsf{PSL}(2,5)$, $m = 3$, or $G = \mathsf{PGL}(2,7)$, $m = 4$, then G is not m-homogeneous; in fact, G has exactly two orbits under its natural action on the set of m-element subsets of A. For each such orbit O, $\mathfrak{R}_m(O)$ will denote the clone that we get from $\mathfrak{R}_m$ by omitting all operations whose range is an m-element set not in O.

It is easy to see that the projections and those operations on A whose range has size at most 2 and have the form

$$\varphi\big(\varphi_1(x_1) + \cdots + \varphi_n(x_n)\big) \qquad (n \geq 1) \tag{6.1}$$

where $\varphi_1, \dots, \varphi_n$ are mappings $A \to \{0,1\}$, $+$ is addition modulo 2, and φ is any mapping $\{0,1\} \to A$ form a clone. This clone will be denoted by $\mathfrak{B}$. If $|A|$ is even, then the projections and all operations of the form (6.1) where each φ_i $(i = 1, \dots, n)$ has even kernel type form a proper subclone in $\mathfrak{B}$; this clone will be denoted by $\mathfrak{B}^*$.

Theorem 6.1. *Let G be a weakly homogeneous permutation group acting on a finite set A ($|A| \geq 3$). The G-closed clones on A that contain all constants are the following:*

- (U) *$\langle T \rangle$ where T is a G-closed transformation monoid that contains all constants;*
- (A_1) *$\mathrm{Clo}({}_{\mathbb{F}_q}\underline{A}^{\mathrm{c}}) = \mathrm{Pol}({}_{\mathbb{F}_q}\underline{A})$ where ${}_{\mathbb{F}_q}\underline{A}$ is a d-dimensional vector space over the q-element field, if $3 \leq q^d \leq 4$ and $\mathsf{A}_{q^d} \leq G \leq \mathsf{S}_{q^d}$, or $q^d = 5$ and $G = \mathsf{AGL}(1,5)$;*
- (A_2) *$\mathrm{Clo}({}_R\underline{A}^{\mathrm{c}}) = \mathrm{Pol}({}_R\underline{A})$ where ${}_R\underline{A}$ is a 4-element simple module over the ring R of 2×2 matrices over $\mathbb{F}_2$, if $\mathsf{A}_4 \leq G \leq \mathsf{S}_4$;*
- (B) *$\mathfrak{B} \cup \langle T \rangle$ where T is as in* (U)*;*
- (B*) *$\mathfrak{B}^* \cup \langle T \rangle$ if $|A|$ is even, where T is as in* (U) *such that each nonpermutation in T has even kernel type;*

(S) *the clone* $\mathfrak{R}_m \cup \langle T\rangle$ *where* $2 \le m \le |A|$, *and* T *is as in* (U);
(S_O) *the clone* $\mathfrak{R}_m(O) \cup \langle T\rangle$ *if* $G = \mathsf{PSL}(2,5)$, $m = 3$, *or* $G = \mathsf{PGL}(2,7)$, $m = 4$, *where* O *is an orbit of* G *under its natural action on the* m*-element subsets of* A, *and* T *is as in* (U) *such that for all* $M \in O$ *and* $f \in T$ *with* $|f(M)| = m$ *we have* $f(M) \in O$.

Proof. Let G be a weakly homogeneous permutation group on A.

All clones listed are G-closed and contain all constants. This is clear for the clones in (U), (B), (B*), (S), and (S_O). For the other two let ${}_R\underline{A}$ be an R-module such that for some subfield K of $\mathrm{End}(\underline{A})$, $R = K$ or $R = \mathrm{End}({}_K\underline{A})$. Let $K = \mathbb{F}_q$ and let d be the dimension of the vector space ${}_K\underline{A}$. (Hence, in case $R = \mathrm{End}({}_K\underline{A})$, $\mathrm{End}({}_K\underline{A})$ can be replaced by the ring of $d \times d$ matrices over K.) It is easy to check (see e.g. [23], Example 2.11) that whether $R = K$ or $R = \mathrm{End}({}_K\underline{A})$, the weak automorphism group of the algebra ${}_R\underline{A}^{\mathrm{c}}$ is the affine semilinear group $\mathsf{A\Gamma L}({}_K\underline{A}) = \mathsf{A\Gamma L}(d,q)$. Since $\mathsf{AGL}(1,3) = \mathsf{S}_3$ and $\mathsf{A\Gamma L}(1,4) = \mathsf{AGL}(2,2) = \mathsf{S}_4$, the clones listed in ($A_1$) and ($A_2$) are G-closed for the groups G indicated. They obviously contain all constants.

To prove that the list of clones in Theorem 6.1 is complete, let $\mathfrak{C}$ be an arbitrary G-closed clone on A that contains all constants, and let $\mathbf{A} = (A; \mathfrak{C})$ be the associated algebra. Thus $\mathfrak{C} = \mathrm{Pol}(\mathbf{A})$ is the clone of all polynomial operations of $\mathbf{A}$. Our goal is to prove that $\mathfrak{C}$ is one of the clones listed in the theorem.

Claim 6.2. *Either* $\mathfrak{C}$ *is one of the clones described in (U) or* $(A)_1$, *or the algebra* $\mathbf{A}$ *is simple but not essentially unary, and* $\mathfrak{C}$ *contains a unary operation that is neither constant nor a permutation.*

The assumption that G is weakly homogeneous implies that G is 2-homogeneous (see Lemma 2.1). Since $\mathfrak{C}$ is G-closed, Theorem 2.5 applies to $\mathfrak{C}$. The assumption that $\mathfrak{C}$ contains all constants restricts the possibilities to (a), the clones $\mathrm{Pol}({}_K\underline{A})$ in (e), and the clones $\langle M \cup \mathsf{C}_A\rangle$ in (f). The clones in (f) and some of the clones in (a) are essentially unary: each such clone $\mathfrak{C}$ is generated by the monoid $T = \mathfrak{C}^{(1)}$ of unary operations in $\mathfrak{C}$. Since $\mathfrak{C}$ is G-closed, so is T. Thus $\mathfrak{C}$ has the form described in (U).

If $\mathfrak{C} = \mathrm{Pol}({}_K\underline{A})$ for some vector space ${}_K\underline{A}$ on A, then $\mathrm{WAut}(\mathbf{A}) = \mathsf{A\Gamma L}({}_K\underline{A}) = \mathsf{A\Gamma L}(d,q)$ where $K = \mathbb{F}_q$ ($q = p^e$, p prime), and the dimension of ${}_K\underline{A}$ is d. Thus G is a weakly homogeneous subgroup of $\mathsf{A\Gamma L}(d,q) \le \mathsf{AGL}(de,p)$. By Claims 4.6, 4.7, and the assumption $|A| \ge 3$ we must have $3 \le q^d = p^{de} \le 5$. Thus $\mathfrak{C}$ is one of the clones in (A_1) with G as described there.

In the remaining cases $\mathfrak{C}$ is a G-closed clone that is not essentially unary, but satisfies condition (a) in Theorem 2.5. This completes the proof of Claim 6.2.

The rest of the proof will be concerned with the algebras $\mathbf{A}$ specified by the last option in Claim 6.2. More explicitly we will adopt the following assumption.

Assumption 6.3. $\mathbf{A}$ is a simple algebra that is not essentially unary, but has a unary polynomial operation that is neither constant nor a permutation.

Since $\mathbf{A}$ is simple and $\mathfrak{C}$ is the clone $\mathrm{Pol}(\mathbf{A})$ of polynomial operations of $\mathbf{A}$, this is the perfect setting to apply tame congruence theory (see [10]).

Claim 6.4. *For every unary polynomial operation $f \in \mathrm{Pol}^{(1)}(\mathbf{A})$ of $\mathbf{A}$ and for every subset R of A with $|R| = |f(A)|$ there exists $\gamma \in G$ such that $|{}^{\gamma}f(R)| = |R|$.*

Let $r = |R| = |f(A)|$. The kernel of f determines a partition of A into r blocks. We claim that this partition has a transversal T such that T is in the same G-orbit as R. This statement is obviously true if G is r-homogeneous. If G is not r-homogeneous then either $G = \mathsf{PSL}(2,5)$ and $r = 3$, or $G = \mathsf{PGL}(2,7)$ and $r = 4$. In these cases our statement follows from parts (1) of Lemmas 5.1 and 5.2. Let $\gamma \in G$ be such that $\gamma(T) = R$. Then ${}^{\gamma}f(R) = (\gamma \circ f \circ \gamma^{-1})(R) = \gamma\big(f(T)\big)$. Since T is a transversal for the kernel of f, we get that $|{}^{\gamma}f(R)| = \big|\gamma\big(f(T)\big)\big| = |f(T)| = r = |R|$, as required.

Claim 6.5. *If $f \in \mathrm{Pol}^{(1)}(\mathbf{A})$ then $\mathbf{A}$ has an idempotent polynomial $e^2 = e \in \mathrm{Pol}^{(1)}(\mathbf{A})$ such that* $\ker(e) = \ker(f)$.

Let $|f(A)| = r$. We can construct an infinite sequence $g_1, g_2, \ldots \in \mathrm{Pol}^{(1)}(\mathbf{A})$ of operations, each one with an r-element range, as follows: we let $g_1 = f$, and whenever g_k has been constructed with $|g_k(A)| = r$, then we select ${}^{\gamma}f$, using Claim 6.4, such that $\big|{}^{\gamma}f\big(g_k(A)\big)\big| = r$, and let $g_{k+1} = {}^{\gamma}f \circ g_k$.

Since A is finite, there will be a repetition among the ranges of $g_1, g_2, \ldots$. Let $1 \leq s < t$ be such $g_t(A) = g_s(A)$. Let B denote this common range. By construction, $|B| = r$ and $g_t = h \circ g_s$ for some operation $h \in \mathrm{Pol}^{(1)}(\mathbf{A})$ where h is a composition of conjugates ${}^{\gamma}f$ ($\gamma \in G$) of f. It follows that h restricts to B as a permutation and $|h(A)| \leq |f(A)| = r$. Thus $h(A) = B$. Since B is finite, some power $\bar{e} = h^m$ of h will act as the identity on B. Hence $\bar{e}^2 = \bar{e}$ is an idempotent unary polynomial of $\mathbf{A}$ such that $\bar{e}(A) = B$ and $\bar{e}$ is a composition of conjugates ${}^{\gamma}f$ ($\gamma \in G$) of f. The fact $|\bar{e}(A)| = |B| = r$ ensures that the kernel of $\bar{e}$ coincides with the kernel of its first factor, a conjugate ${}^{\delta}f$ ($\delta \in G$) of f. Thus $e = {}^{\delta^{-1}}\bar{e}$ is an idempotent unary polynomial of $\mathbf{A}$ with $\ker(e) = \ker(f)$.

Claim 6.6. *Let $e^2 = e$ be an idempotent unary polynomial of $\mathbf{A}$. If there exists a set C in the G-orbit of $e(A)$ such that C intersects exactly s kernel classes of e then $\mathbf{A}$ has an idempotent unary polynomial whose range has size s.*

Let C be a set in the G-orbit of $e(A)$ such that C intersects exactly s kernel classes of e. Since C belongs to the G-orbit of $e(A)$, we have $C = \gamma\big(e(A)\big)$ for some $\gamma \in G$. The polynomial $f = e \circ {}^{\gamma}e$ of $\mathbf{A}$ has range $f(A) = e\big({}^{\gamma}e(A)\big) = e\big(\gamma(e(A))\big)$. Since $\gamma\big(e(A)\big)$ intersects exactly s kernel classes of e, therefore the range of f has size s. Hence, by Claim 6.5, $\mathbf{A}$ has an idempotent unary polynomial whose range has size s.

Claim 6.7. $\mathbf{A}$ *has an idempotent unary polynomial $e^2 = e$ with $|e(A)| = 2$.*

By Assumption 6.3, $\mathbf{A}$ has a unary polynomial that is neither constant nor a permutation. Thus Claim 6.5 implies that $\mathbf{A}$ has such an idempotent unary polynomial as well. Our claim will follow if we show that whenever e is a nonsurjective idempotent unary polynomial of $\mathbf{A}$ whose range has size $r > 2$ then $\mathbf{A}$ has a nonconstant idempotent unary polynomial whose range has size less than r. To get this conclusion, it suffices to verify by Claim 6.6 that there exists a set C in the G-orbit of $e(A)$ such that C intersects at least two, but less than r kernel classes of e.

To prove the existence of such a C suppose first that G is k-homogeneous for some k, $3 \leq k \leq r$. Using the fact that e has at least two kernel classes, not all singletons, we can select a k-element subset S of A such that S intersects at least two kernel classes of e, and one of the intersections has at least two elements. Since G is k-homogeneous, there exists $\gamma \in G$ such that $\gamma^{-1}(S) \subseteq e(A)$. Hence $C = \gamma\big(e(A)\big)$ belongs to the G-orbit of $e(A)$, and because of $S \subseteq C$, C intersects at least two, but less than r kernel classes of e, as required.

Now suppose that G is not k-homogeneous for any k, $3 \leq k \leq r$. Then $G = \mathsf{PSL}(2,5)$, $A = 6$, and $r = 3$. Let B_1, B_2, B_3 denote the kernel classes of e such that $|B_1| \geq |B_2| \geq |B_3|$. If $|B_1| \geq 3$, let S be a 4-element subset of A such that $|B_1 \cap S| = 3$. Let $\{c\} = S - B_1$. Recall that G has two orbits of 3-element sets (see Claim 4.14), and since G is weakly 3-homogeneous, among the four 3-element subsets of S exactly two belong to each G-orbit. Therefore it follows that the G-orbit of $e(A)$ contains a 3-element subset C of S such that $c \in C$. By construction, C intersects exactly two kernel classes of e. Finally, if $|B_1| < 3$, then the assumption that $\{B_1, B_2, B_3\}$ is a partition of A with $|B_1| \geq |B_2| \geq |B_3|$ implies that $|B_1| = |B_2| = |B_3| = 2$. Let $S = B_1 \cup B_2$. It follows as before that the G-orbit of $e(A)$ contains a 3-element subset C of S. Clearly, C intersects exactly two kernel classes of e. This completes the proof of Claim 6.7.

Claim 6.8. *Let $|A| > 4$. If $\mathbf{A}$ has an idempotent unary polynomial whose range has size 4, then $\mathbf{A}$ also has an idempotent unary polynomial whose range has size 3.*

Let $e^2 = e$ be an idempotent unary polynomial of $\mathbf{A}$ such that $|e(A)| = 4$. Since $|A| > 4$, e has a kernel class that is not a singleton. To prove that $\mathbf{A}$ has an idempotent unary polynomial whose range has size 3 it suffices to show, by Claim 6.6, that there exists a set C in the G-orbit of $e(A)$ such that C intersects exactly 3 kernel classes of e. Therefore we will be done if we establish that every G-orbit of 4-element sets contains a set C which intersects exactly 3 kernel classes of e. This is clearly true if G is 4-homogeneous.

It remains to consider the case when $G = \mathsf{PGL}(2,7)$, $|A| = 8$. Let B_1, B_2, B_3, B_4 be the kernel classes of e such that $|B_1| > 1$. Let $S = \{a, b, u, v, w\}$ be a 5-element subset of A such that $a, b \in B_1$ and $u \in B_2$, $v \in B_3$, $w \in B_4$. If for some choice of S there exist 4-element subsets C_1, C_2 of S, each containing a, b, which belong to distinct G-orbits, then we are done. Otherwise, for each choice of S, the three sets

$\{a,b,u,v\}$, $\{a,b,u,w\}$, $\{a,b,v,w\}$ belong to the same G-orbit. Thus Claim 4.15 (2) implies that for each such S, $\mathrm{crr}(a,u,v,w) \in \{3,5\}$ and $\mathrm{crr}(b,u,v,w) \in \{3,5\}$. Hence every transversal $\{a,u,v,w\}$ of the partition $\{B_1,B_2,B_3,B_4\}$ belongs to the same G-orbit of 4-element sets. By part (1) of Lemma 5.2 this is impossible. Therefore the proof of Claim 6.8 is complete.

Claim 6.9. *Let $|A|$ be even. If $\mathbf{A}$ has a nonsurjective idempotent unary polynomial e with kernel type $(k_1,\dots,k_r)$ such that $r \geq 3$ and some k_i is odd, then $\mathbf{A}$ has an idempotent unary polynomial $\bar{e}$ with kernel type (l_1,l_2) such that l_1,l_2 are odd.*

Suppose $e^2 = e \in \mathrm{Pol}^{(1)}(\mathbf{A})$ has kernel type $(k_1,\dots,k_r)$ such that $r \geq 3$ and some k_i is odd. It suffices to prove the existence of a polynomial $f \in \mathrm{Pol}^{(1)}(\mathbf{A})$ such that f has kernel type $(l_1,\dots,l_s)$ where $s < r$ and some l_j is odd. Once this has been established, then it follows from Claim 6.5 that f can be chosen to be idempotent. Hence, if $\bar{e}$ is an idempotent unary polynomial of $\mathbf{A}$ whose kernel type contains an odd number and has minimum size range, then the preceding statement shows that $\bar{e}$ has a 2-element range. This proves the statement in the claim.

To show the existence of f we will use the same construction as in Claim 6.6: $f = e \circ {}^{\gamma}e$ where $\gamma \in G$. Let $B_1,\dots,B_r$ denote the kernel classes of e, and let $e(B_i) = a_i \in B_i$, $|B_i| = k_i$ $(1 \leq i \leq r)$. Since $|A|$ is even, the number of odd k_i-s is even. Suppose that k_1,k_2 are odd and k_1 is the minimal odd kernel class size. We have $\ker(f) \supseteq \ker({}^{\gamma}e)$ where the kernel classes of ${}^{\gamma}e$ are $\gamma(B_1),\dots,\gamma(B_r)$. Thus each kernel class of f is a union of some kernel classes of ${}^{\gamma}e$. It suffices to find $\gamma \in G$ such that one of the kernel classes of f is equal to $\gamma(B_1)$, and another kernel class of f contains a union of two distinct kernel classes of ${}^{\gamma}e$.

First we will consider the case when there exists a singleton kernel class. Then $k_1 = 1$, that is, $B_1 = \{a_1\}$. Note that since $|A|$ is even, we have

$$\mathsf{A}_n \leq G \ (|A| = n) \quad \text{or} \quad \mathsf{PSL}(2,5) \leq G \ (|A| = 6) \quad \text{or} \quad \mathsf{PGL}(2,7) = G \ (|A| = 8).$$

As

$$(\mathsf{A}_n)_{a_1} \cong \mathsf{A}_{n-1}, \qquad \mathsf{PSL}(2,5)_{a_1} \cong D_5, \qquad \mathsf{PGL}(2,7)_{a_1} \cong \mathsf{AGL}(1,7),$$

the stabilizer G_{a_1} of G acts 2-homogeneously on $A - \{a_1\}$ unless $G = \mathsf{PSL}(2,5)$ and $G_{a_1} \cong D_5$; in the latter case G_{a_1} has two orbits on the 2-element subsets of the set $A - \{a_1\}$ of vertices of the pentagon: one orbit consists of the sides and the other orbit consists of the diagonals of the pentagon. We claim that in all cases there exists $\gamma \in G$ such that γ fixes a_1 and maps two distinct elements a_s, a_t of $e(A) - \{a_1\} = \{a_2,\dots,a_r\}$ into the same kernel class B_j $(j > 1)$ of e. If G_{a_1} acts 2-homogeneously on $A - \{a_1\}$, then such a γ exists for any choice of a_s, a_t $(s \neq t)$ and B_j with $|B_j| \geq 2$. If $G = \mathsf{PSL}(2,5)$ and $r = 3$, then there exists B_j $(2 \leq j \leq 3)$ such that $|B_j| \geq 3$. There are sides as well as diagonals among the 2-element subsets of B_j, therefore there exists $\gamma \in G$ such that γ fixes a_1 and maps a_2, a_3 into B_j. Similarly, if $G = \mathsf{PSL}(2,5)$ and $r \geq 4$, then there exists B_j $(2 \leq j \leq r)$ such that

$|B_j| \geq 2$, and there are sides as well as diagonals among the 2-element subsets of $\{a_2, a_3, a_4\}$. Therefore there exists $\gamma \in G$ such that γ fixes a_1 and maps some a_s, a_t $(2 \leq s < t \leq 4)$ into B_j. This proves the existence of γ in all cases. Since $\gamma(a_1) = a_1$ and $\gamma(a_i) \notin \{a_1\} = B_1$ for $i = 2, \ldots, r$, one of the kernel classes of $f = e \circ {}^{\gamma}e$ is $\gamma(B_1)$. Since $\gamma(a_s), \gamma(a_t) \in B_j$, therefore another kernel class of f contains $\gamma(B_s) \cup \gamma(B_t)$. Thus f satisfies our requirements.

Now assume that e has no singleton kernel class. Then every kernel class of odd size has at least three elements. In particular, $k_1, k_2 \geq 3$. Since $r \geq 3$, we must have $|A| \geq k_1 + k_2 + k_3 \geq 3 + 3 + 2 = 8$. Thus either $\mathsf{A}_n \leq G$ $(|A| = n)$, or else $\mathsf{PGL}(2, 7) = G$, $r = 3$, and $|B_1| = |B_2| = 3$, $|B_3| = 2$. If $\mathsf{A}_n \leq G$, then there exists $\gamma \in G$ such that $\gamma(B_1) = B_1$ and $\gamma(a_2), \gamma(a_3) \in B_2$. The same argument as in the preceding paragraph shows that f satisfies our requirements. In the remaining case when $\mathsf{PGL}(2, 7) = G$, $r = 3$, and $|B_1| = |B_2| = 3$, $|B_3| = 2$, let γ be a cycle of length 7 that fixes a_3 and maps a_2 into the unique element of $B_3 - \{a_3\}$. Then $\{\gamma(a_2), \gamma(a_3)\} = B_3$, whence $\gamma(a_1) \in B_i$ for $i = 1$ or 2. Thus $f = e \circ {}^{\gamma}e$ has two kernel classes: $\gamma(B_1)$ and $\gamma(B_2) \cup \gamma(B_3)$, hence it satisfies our requirements. The proof of Claim 6.9 is complete.

Claim 6.10. *Every 2-element subset of A is a trace (= minimal set) of $\mathbf{A}$.*

By Claim 6.7 $\mathbf{A}$ has an idempotent unary polynomial e with 2-element range. Since $\mathfrak{C} = \mathrm{Pol}(\mathbf{A})$ is G-closed, therefore for each $\gamma \in G$, ${}^{\gamma}e$ is an idempotent unary polynomial of $\mathbf{A}$ with 2-element range ${}^{\gamma}e(A) = \gamma\big(e(\gamma^{-1}(A))\big) = \gamma\big(e(A)\big)$. Since G is 2-homogeneous, this implies that every 2-element subset of A is the range of an idempotent polynomial of A. By Theorem 2.8(6) of [10] it follows that every 2-element subset of A is a minimal set. Since minimal sets and traces coincide for simple algebras, the claim is proved.

If N is a trace of a finite simple algebra $\mathbf{A}$, then the authors of [12] call a set of the form $M = p(N, N, \ldots, N)$, $p \in \mathrm{Pol}(\mathbf{A})$, a *multitrace* of $\mathbf{A}$. The special case when p is a projection shows that every trace is a multitrace.

Claim 6.11. *If M is a multitrace of $\mathbf{A}$ and $\gamma \in G$, then $\gamma(M)$ is also a multitrace of $\mathbf{A}$.*

If M is a multitrace then $M = p(N, \ldots, N)$ for some trace N and some polynomial p of $\mathbf{A}$. Then $\gamma(M) = {}^{\gamma}p\big(\gamma(N), \ldots, \gamma(N)\big)$. By Claim 6.10 $\gamma(N)$ is a minimal set of $\mathbf{A}$, hence Theorem 2.8 (1) of [10] yields that $\gamma(N)$ is polynomially isomorphic to N. Thus $\gamma(N) = g(N)$ for some $g \in \mathrm{Pol}^{(1)}(\mathbf{A})$. Now the polynomial $h(x_1, \ldots, x_n) = {}^{\gamma}p\big(g(x_1), \ldots, g(x_n)\big)$ of $\mathbf{A}$ witnesses the fact that $\gamma(M) = h(N, \ldots, N)$ is a multitrace.

For the proof of the next claim on multitraces we will use Yablonskiĭ's Lemma:

Lemma 6.12. [24] *Let A be a finite set and $f(x_1, \dots, x_n)$ be an operation on A that depends on more than one variable. If $|f(A, A, \dots, A)| > r$ for some $r > 1$, then there exist r-element subsets $M_1, \dots, M_n \subseteq A$ for which $|f(M_1, M_2, \dots, M_n)| > r$.*

Claim 6.13. *Suppose that for some r $(2 \leq r < |A|)$ all r-element subsets of A are multitraces of $\mathbf{A}$. If $\mathbf{A}$ has a polynomial f such that f depends on more than one variable and has range of size $> r$, then $\mathbf{A}$ has a multitrace of size $> r$ that is contained in the range of f.*

Let f be a polynomial of $\mathbf{A}$ such that f depends on more than one variable and f has range $f(A, \dots, A)$ of size $> r$. Yablonskiĭ's Lemma implies that there exist r-element sets $M_1, \dots, M_n \subseteq A$ such that $|f(M_1, M_2, \dots, M_n)| > r$. By our assumption $M_1, \dots, M_n$ are multitraces of $\mathbf{A}$, so each M_i equals $f_i(N, \dots, N)$ for some polynomial f_i of $\mathbf{A}$ and some fixed trace N of $\mathbf{A}$. Hence

$$f(M_1, M_2, \dots, M_n) = f\big(f_1(N, \dots, N), \dots, f_n(N, \dots, N)\big)$$

is a multitrace of size larger than r, and is contained in the range of f, as claimed.

Multitraces are well behaved only in types $\mathbf{1}$, $\mathbf{2}$ and $\mathbf{3}$, so we now reduce to these cases.

Claim 6.14. $\mathbf{A}$ *is a simple algebra of type* $\mathbf{1}$, $\mathbf{2}$, *or* $\mathbf{3}$.

The algebra $\mathbf{A}$ is simple by Assumption 6.3. Suppose that $\mathrm{typ}(\mathbf{A}) \in \{\mathbf{4}, \mathbf{5}\}$. By Theorem 5.26 (2) of [10], $\mathbf{A}$ has precisely two minimal connected compatible partial orders; they are inverses of each other, therefore we will denote them by ζ and ζ^{-1}. Since $\mathfrak{C} = \mathrm{Pol}(\mathbf{A})$ is G-closed, the permutations in G map compatible relations of $\mathbf{A}$ into compatible relations of $\mathbf{A}$. Thus $\gamma(\zeta)$ is a minimal connected compatible partial order of $\mathbf{A}$ for each $\gamma \in G$. Hence $\gamma(\zeta) = \zeta$ or ζ^{-1} for each $\gamma \in G$. This implies that for arbitrary elements $a, b \in A$ that are comparable with respect to ζ (or, equivalently, with respect to ζ^{-1}), the elements $\gamma(a)$, $\gamma(b)$ $(\gamma \in G)$ are also comparable. Since the partial order ζ is connected, there exist distinct comparable elements a, b in A. Hence the 2-homogeneity of G implies that any two distinct elements of A are comparable; that is, ζ is a total order on A. Let 1_ζ and 0_ζ denote the largest and the smallest elements with respect to ζ. Since $\gamma(\zeta) = \zeta$ or ζ^{-1} for each $\gamma \in G$, we get that $\gamma(1_\zeta)$ is equal to 1_ζ or 0_ζ for each $\gamma \in G$. But this is impossible, since G is transitive and $|A| \geq 3$. This contradiction proves that $\mathbf{A}$ is of type $\mathbf{1}$, $\mathbf{2}$, or $\mathbf{3}$.

Now we are in a position to use the structure theorem for multitraces of types $\mathbf{1}$, $\mathbf{2}$ and $\mathbf{3}$. Recall that for any subset $M = e(A)$ of A where e is an idempotent unary polynomial of $\mathbf{A}$ the induced algebra $\mathbf{A}|_M$ is defined as follows:

$$\mathbf{A}|_M = (M; \{ef|_M : f \text{ is a polynomial operation of } \mathbf{A}\}).$$

Theorem 6.15. (From Theorems 3.10 & 3.12 of [12]) *If N is a trace of the simple algebra $\mathbf{A}$, $\mathrm{typ}(\mathbf{A}) \in \{\mathbf{1}, \mathbf{2}, \mathbf{3}\}$, and $M = p(N, \dots, N)$ is a multitrace, then*

(1) $M = e(A)$ *for some idempotent unary polynomial* $e \in \mathrm{Pol}^{(1)}(\mathbf{A})$, *and*
(2) *the induced algebra* $\mathbf{A}|_M$ *is term equivalent to*
  (i) *a matrix power* $(\mathbf{A}|_N)^{[k]}$ *if* $\mathrm{typ}(\mathbf{A}) \in \{\mathbf{1}, \mathbf{2}\}$*; or*
  (ii) *a primal algebra if* $\mathrm{typ}(\mathbf{A}) = \mathbf{3}$.

Claim 6.16. *If* $\mathrm{typ}(\mathbf{A}) \in \{\mathbf{1}, \mathbf{2}\}$ *then either every multitrace has size* 2*, or else* $|A| = 4$ *and* $\mathbf{A}$ *is term equivalent to* $(\mathbf{A}|_N)^{[2]}$ *for some trace* N.

Suppose that $\mathbf{A}$ is of type $\mathbf{1}$ or $\mathbf{2}$ and $\mathbf{A}$ has a multitrace of size > 2. Let M be a multitrace of minimum size with $|M| > 2$. Theorem 6.15 (2) implies that $\mathbf{A}|_M$ is term equivalent to $(\mathbf{A}|_N)^{[k]}$ for some k and some trace N of $\mathbf{A}$. It follows from Claim 6.10 that $|N| = 2$, and hence from Corollary 4.11 in [10] that $\mathbf{A}|_N$ is polynomially equivalent to a 2-element unary algebra or vector space. Thus $|M| = 2^k$. In fact, every multitrace of $(\mathbf{A}|_N)^{[k]}$ is of size 2^l for some l $(2 \leq l \leq k)$, and every such power of 2 is the size of a multitrace of $(\mathbf{A}|_N)^{[k]}$. Since $\mathbf{A}|_M$ is term equivalent to $(\mathbf{A}|_N)^{[k]}$, the same conclusion holds for the sizes of multitraces of $\mathbf{A}|_M$. The definition of $\mathbf{A}|_M$ shows that every multitrace of $\mathbf{A}|_M$ is a multitrace of $\mathbf{A}$ as well, so the minimality of M yields that $k = 2$ and $|M| = 4$.

Next we show that $|A| = 4$. Suppose $|A| > 4$. By Theorem 6.15 (1), $\mathbf{A}$ has an idempotent unary polynomial e whose range is M, a set of size 4. Therefore by Claim 6.8 $\mathbf{A}$ also has an idempotent unary polynomial $\bar{e}$ whose range has size 3. We claim that M has a 3-element subset of the form $\gamma\big(\bar{e}(A)\big)$ for some $\gamma \in G$. This is clear if G is 3-homogeneous. It holds also if G is not 3-homogeneous, because then $G = \mathsf{PSL}(2, 5)$ and the 3-element subsets of the 4-element set M represent both G-orbits. So, let us fix $\gamma \in G$ such that $\gamma\big(\bar{e}(A)\big) \subseteq M$. The left hand side is the range of the conjugate ${}^{\gamma}\bar{e}$ of $\bar{e}$. Thus ${}^{\gamma}\bar{e}|_M = (e{}^{\gamma}\bar{e})|_M$ is an idempotent unary polynomial operation of $\mathbf{A}|_M$. Hence $\gamma\big(\bar{e}(A)\big)$ is a multitrace of $\mathbf{A}|_M$, since

$$\gamma\big(\bar{e}(A)\big) = {}^{\gamma}\bar{e}|_M(M) = {}^{\gamma}\bar{e}|_M\big(e(M)\big) = {}^{\gamma}\bar{e}|_M\big(ep|_M(N, \ldots, N)\big).$$

This shows that $\mathbf{A}|_M$ has a multitrace of size 3. However, we established in the preceding paragraph that every multitrace of $\mathbf{A}|_M$ is of size 2 or 4. This contradiction proves that $|A| = 4$. It follows that $\mathbf{A}$ is term equivalent to $\mathbf{A}|_M$, and hence to $(\mathbf{A}|_N)^{[2]}$.

Claim 6.17. $\mathrm{typ}(\mathbf{A}) \neq \mathbf{1}$.

If $\mathrm{typ}(\mathbf{A}) = \mathbf{1}$, then Claim 6.16 proves that either every multitrace has size 2 or else $\mathbf{A}$ is term equivalent to $(\mathbf{A}|_N)^{[2]}$. In the case where every multitrace has size 2, we get from Claims 6.10 and from the case $r = 2$ of Claim 6.13 that every polynomial operation of $\mathbf{A}$ that depends on more than one variable has range in a trace. But if $\mathbf{A}$ is of type $\mathbf{1}$ and $f(x_1, \ldots, x_n)$ is a polynomial operation of $\mathbf{A}$ for which $f(A, \ldots, A) \subseteq N$ for some trace N, then f depends on at most one variable. (See

[10], Theorem 5.6, Claim 3.) We assumed in Assumption 6.3 that $\mathbf{A}$ has a polynomial operation depending on more than one variable, so this case is impossible.

Now assume that $\mathbf{A}$ is term equivalent to $(\mathbf{A}|_N)^{[2]}$. It follows from Claim 6.10 that $\mathbf{A}|_N$ is a 2-element unary algebra, hence $|A| = 4$. This information allows one to calculate the group of unary polynomial permutations of $(\mathbf{A}|_N)^{[2]}$ (equivalently of $\mathbf{A}$): it is a 2-element group or an octic group according to whether the group of unary permutations of $\mathbf{A}|_N$ is A_2 or S_2. None of these groups are normal in $G = \mathsf{A}_4$ or S_4, so in this case the clone of $(\mathbf{A}|_N)^{[2]}$ is not G-closed. This finishes the proof of the claim.

Claim 6.18. *If* $\operatorname{typ}(\mathbf{A}) = \mathbf{2}$ *and* $\mathfrak{C}$ *contains an operation that depends on at least two variables and has range of size at least* 3*, then* $\mathfrak{C}$ *is the clone described in Theorem 6.1 (*A_2*).*

From Claims 6.10, 6.13, and 6.16 we get that $\mathbf{A}$ is term equivalent to $(\mathbf{A}|_N)^{[2]}$. From Claim 6.10 and the fact that $\operatorname{typ}(\mathbf{A}) = \mathbf{2}$ we get that $\mathbf{A}|_N$ is the constant expansion of a 2-element vector space. It follows that the clone of $(\mathbf{A}|_N)^{[2]}$ (equivalently of $\mathbf{A}$) is the clone of polynomial operations of the 4-element module over the 2×2 matrix ring over the 2-element field.

Claim 6.19. *If* $\operatorname{typ}(\mathbf{A}) = \mathbf{2}$ *and every operation in* $\mathfrak{C}$ *that depends on at least two variables has range of size at most* 2*, then* $\mathfrak{C}$ *is one of the clones described in Theorem 6.1 (B) or (*B^**).*

According to Claim 6.10, every polynomial operation of $\mathbf{A}$ that depends on more than one variable has range in a trace. Moreover, since traces are polynomially isomorphic, the polynomial operations with range in a trace N' can be derived from the polynomial operations with range in a trace N by composing with a polynomial isomorphism $p\colon N \to N'$. It follows from this that $\mathfrak{C}$ is the clone on $\mathbf{A}$ generated by $\mathfrak{C}^{(1)}$ and the collection $\mathfrak{N}$ of polynomials with range in a specific trace $N = \{0, 1\} \subseteq A$.

Let $x + y$ denote a polynomial of $\mathbf{A}$ whose restriction to N is the vector space addition on N (which exists since $\operatorname{typ}(\mathbf{A}) = \mathbf{2}$). In the fourth paragraph of the proof of Theorem 13.5 of [10] it is shown that any polynomial operation of a type $\mathbf{2}$ simple algebra $\mathbf{A}$ that has range in a trace N is constructible from unary polynomials of $\mathbf{A}$ and from $x + y$. In fact, any polynomial in $\mathfrak{N}$ is a sum of unary polynomials in $\mathfrak{N}^{(1)}$. Thus, $\mathfrak{C}$ is generated by $\mathfrak{C}^{(1)}$ and $\mathfrak{N}$, and $\mathfrak{N}$ is generated by $x + y$ and $\mathfrak{N}^{(1)}$. Therefore we need to determine the possibilities for $\mathfrak{N}^{(1)}$.

An element of $\mathfrak{N}^{(1)}$ is a function $f\colon A \to N = \{0, 1\}$, so it can be thought of as a characteristic function on A which may be identified with its support $U_f = \{a \in A : f(a) = 1\}$. The family $\mathcal{F}$ of subsets of $\mathbf{A}$ that are supports of unary polynomials in $\mathfrak{N}^{(1)}$ has the following properties.

(i) $\mathcal{F}$ contains $\emptyset$, A, and at least one nonempty proper subset of A.
(ii) $\mathcal{F}$ is closed under symmetric difference, $\oplus$.

(iii) $\mathcal{F}$ is closed under G; that is, if $U \in \mathcal{F}$ and $V = \gamma(U)$ for some $\gamma \in G$ then $V \in \mathcal{F}$.

Item (i) follows from the fact that the constant polynomials into N have support $\emptyset$ and A respectively, and the fact proved in Claim 6.10 that N is the image of some function from $\mathfrak{C}^{(1)}$. Item (ii) follows from the fact that the support of $f + g$ ($f, g \in \mathfrak{N}^{(1)}$) is $U_f \oplus U_g$. To prove (iii) let $f \in \mathfrak{N}^{(1)}$ be such that $U = U_f$, and let $\gamma \in G$. Since $\gamma(N)$ is a trace by Claim 6.10, and traces are polynomially isomorphic, there exists $p \in \mathfrak{C}^{(1)}$ such that $p\big(\gamma(N)\big) = N$. The transposition on N is a polynomial isomorphism $x \mapsto x + 1$, therefore p can be chosen so that $p\big(\gamma(i)\big) = i$ for $i \in N$. Now for $g = p \circ {}^{\gamma}f$ we have $g \in \mathfrak{N}^{(1)}$ and $U_g = \gamma(U)$. Thus $\gamma(U) \in \mathcal{F}$, as claimed.

Now we prove that $\mathcal{F}$ contains a nonempty set of size ≤ 2. Let U be a proper nonempty subset of A that belongs to $\mathcal{F}$. (Such a set exists by (i).) We are done if $|U| \leq 2$. Suppose therefore that $|U| \geq 3$, and let $c \in A - U$. By the property (WH) of G, the G-orbit of U contains a subset V of $U \cup \{c\}$ distinct from U. By (iii), $V \in \mathcal{F}$. Thus, by (ii), the 2-element set $U \oplus V$ also belongs to $\mathcal{F}$. This proves that if $W \in \mathcal{F}$ is a nonempty set of least cardinality, then either $|W| = 1$ or $|W| = 2$.

If $|W| = 1$, then by (iii) and by the transitivity of G, all 1-element subsets of A belong to $\mathcal{F}$, and so by (ii) (using symmetric difference) every subset of A belongs to $\mathcal{F}$. This means that every function from A into N belongs to $\mathfrak{N}^{(1)}$. Composing with polynomial isomorphisms between traces, this implies that $\mathfrak{C}^{(1)}$ contains all transformations whose range has size at most 2. The transformations whose range have size at most 2 and the polynomial $x + y$ belong to Burle's clone $\mathfrak{B}$, and are sufficient to generate all operations in Burle's clone. Thus, from the remarks we have made, $\mathfrak{C}$ is generated by $\mathfrak{B} \cup \langle \mathfrak{C}^{(1)} \rangle$. Since this union is a clone, we get that $\mathfrak{C} = \mathfrak{B} \cup \langle \mathfrak{C}^{(1)} \rangle = \mathfrak{B} \cup \langle T \rangle$ for some G-closed transformation monoid T that contains all transformations whose range has size at most 2. This is a clone from Theorem 6.1 (B).

Now suppose that $|W| = 2$. Then all 2-element subsets of A are in $\mathcal{F}$, and taking symmetric differences we get that all even-element subsets of A are in $\mathcal{F}$. We cannot have any odd-element sets in $\mathcal{F}$, for if $a \in U \in \mathcal{F}$ and $|U|$ is odd, then by our previous remark $(U - \{a\}) \in \mathcal{F}$; hence $\{a\} = U \oplus (U - \{a\}) \in \mathcal{F}$. This contradicts the minimality of W. (In particular, $|A|$ is even when $|W| = 2$.) Thus, the nonconstant unary polynomials $f \in \mathfrak{N}^{(1)}$ are precisely those of even kernel type. As in the preceding paragraph, the higher arity polynomials in $\mathfrak{N}$ are sums of unary polynomials in $\mathfrak{N}^{(1)}$, and the higher arity polynomials with range $N' \neq N$ are obtained from these by composing with a polynomial isomorphism $p\colon N \to N'$. It follows readily that $\mathfrak{C} = \mathfrak{B}^* \cup \langle \mathfrak{C}^{(1)} \rangle = \mathfrak{B}^* \cup \langle T \rangle$ where T is a G-closed transformation monoid such that a transformation with 2-element range belongs to T if and only if it has even kernel type. Claims 6.5 and 6.9 imply that each nonsurjective member of T has even kernel type. Thus $\mathfrak{C}$ is a clone from Theorem 6.1 (B*).

It remains to consider the case when $\mathrm{typ}(\mathbf{A}) = \mathbf{3}$.

Claim 6.20. *If* $\operatorname{typ}(\mathbf{A}) = \mathbf{3}$ *and* M *is a multitrace of* $\mathbf{A}$ *then every operation* $A^n \to A$ *with range in* M *is a polynomial operation of* $\mathbf{A}$*.*

Let $N \subseteq M$ be a trace of $\mathbf{A}$, and choose polynomials $p_1, \dots, p_k \in \operatorname{Pol}^{(1)}(\mathbf{A})$ with range in N which separate the points of $\mathbf{A}$. (The existence of these polynomials is guaranteed by Theorem 2.8(4) of [10].) View $\pi = (p_1, \dots, p_k) \colon A \to M^k$ as a polynomial injection of A into M^k. Now, if $f \colon A^n \to M$ is an arbitrary function, then we can try to find $h \in \operatorname{Pol}(\mathbf{A}|_M)$ that allows us to factor f as

$$A^n \xrightarrow{\pi^n} (M^k)^n \xrightarrow{h} M.$$

The existence of such a factorization depends on the ability to interpolate the partial operation $f \circ (\pi^n)^{-1} \colon (M^k)^n \to M$ by a total operation $h \colon (M^k)^n \to M$ that is a polynomial of $\mathbf{A}|_M$. We can do this since $\mathbf{A}|_M$ is primal (see Theorem 6.15). Thus, an arbitrary operation $f \colon A^n \to A$ with range in M agrees with some polynomial operation of the form $h \circ \pi^n$.

Notation 6.21. From now on m will denote the size of the largest multitrace of $\mathbf{A}$, and $\widehat{m}$ will denote the size of the largest possible range of a polynomial of $\mathbf{A}$ that depends on at least two variables.

Claim 6.22. *If* $\operatorname{typ}(\mathbf{A}) = \mathbf{3}$ *then either*

(1) *all subsets of* A *of size* $\leq m$ *are multitraces of* $\mathbf{A}$*,*

or

(2) *the following conditions hold:*
   - (†) $G = \mathsf{PSL}(2,5)$*,* $m = 3$ *or* $G = \mathsf{PGL}(2,7)$*,* $m = 4$*,*
   - $(\ddagger)_1$ *all subsets of* A *of size* $< m$ *are multitraces of* $\mathbf{A}$*, and*
   - $(\ddagger)_2$ *there exists a* G*-orbit* O *of* m*-element subsets of* A *such that the* m*-element multitraces of* $\mathbf{A}$ *are exactly the members of* O*.*

Let M be an m-element multitrace of $\mathbf{A}$, and let O denote the G-orbit of M. By Claim 6.11

(i) all sets $M' \in O$ are multitraces of $\mathbf{A}$.

Thus, by Claim 6.20, every operation $A^n \to A$ with range contained in an $M' \in O$ is a polynomial of $\mathbf{A}$. Hence

(ii) every subset of any set $M' \in O$ is a multitrace of $\mathbf{A}$.

If G is m-homogeneous, (i) and (ii) imply (1).

So, suppose that G is not m-homogeneous. Then (†) holds, and G has exactly two orbits of m-element sets. If $\mathbf{A}$ has an m-element multitrace in each G-orbit, then the facts established in the preceding paragraph show that (1) holds. If $\mathbf{A}$ has an m-element multitrace in one G-orbit O only, then (i) shows that $(\ddagger)_2$ holds.

Furthermore, by (ii), $\mathbf{A}$ has a k-element multitrace for each $k < m$. Since G is k-homogeneous for all $k < m$, Claim 6.11 implies that $(\ddagger)_1$ holds as well. This proves (2), and completes the proof of Claim 6.22.

Claim 6.23. *If* $\operatorname{typ}(\mathbf{A}) = \mathbf{3}$ *and* $m = \widehat{m}$ *then* $\mathfrak{C}$ *is one of the clones in Theorem 6.1 (S) or (S$_O$).*

The assumption $m = \widehat{m}$ implies that

$$\mathfrak{C} \subseteq \mathfrak{R}_m \cup \langle \mathfrak{C}^{(1)} \rangle.$$

If all m-element subsets of A are multitraces of $\mathbf{A}$ then we get from Claim 6.20 that $\mathfrak{R}_m \subseteq \mathfrak{C}$. Thus $\mathfrak{C} = \mathfrak{R}_m \cup \langle \mathfrak{C}^{(1)} \rangle$, and $\mathfrak{C}$ satisfies Theorem 6.1 (S) with $T = \mathfrak{C}^{(1)}$.

If not all m-element subsets of A are multitraces of $\mathbf{A}$, then conditions $(\dagger)$, $(\ddagger)_1$, and $(\ddagger)_2$ in Claim 6.22 (2) hold for G and $\mathbf{A}$. In view of $(\ddagger)_1$ and $(\ddagger)_2$, Claim 6.20 yields that $\mathfrak{R}_m(O) \subseteq \mathfrak{C}$. Denoting the other G-orbit of m-element sets by O' we get that

$$\mathfrak{R}_m(O) \cup \langle \mathfrak{C}^{(1)} \rangle \subseteq \mathfrak{C} \subseteq \mathfrak{R}_m \cup \langle \mathfrak{C}^{(1)} \rangle = \mathfrak{R}_m(O) \cup \mathfrak{R}_m(O') \cup \langle \mathfrak{C}^{(1)} \rangle.$$

The difference between the rightmost and leftmost clones is the set of all operations f on A such that $f(A, \dots, A) \in O'$ and f depends on at least two variables. Such an operation cannot belong to $\mathfrak{C}$, since otherwise $(\ddagger)_1$, combined with Claim 6.13 (for $r = m - 1$), would imply that $f(A, \dots, A) \in O'$ is a multitrace of $\mathbf{A}$, contradicting $(\ddagger)_2$. This proves that $\mathfrak{C} = \mathfrak{R}_m(O) \cup \langle \mathfrak{C}^{(1)} \rangle = \mathfrak{R}_m(O) \cup \langle T \rangle$ with $T = \mathfrak{C}^{(1)}$. To see that $\mathfrak{C}$ satisfies Theorem 6.1 (S$_O$) it remains to verify the requirements on T. Clearly, T satisfies the conditions in (U). Now let $M \in O$ and let $f \in T$ be such that $|f(M)| = m$. Since M is a multitrace of $\mathbf{A}$, we have $M = p(N, \dots, N)$ for some trace N and some $p \in \operatorname{Pol}(\mathbf{A}) = \mathfrak{C}$. Hence $f(M) = f\big(p(N, \dots, N)\big)$ is also a multitrace of $\mathbf{A}$. Therefore, if $|f(M)| = m$, then $(\ddagger)_2$ forces $f(M) \in O$. This completes the proof of Claim 6.23.

Claim 6.24. *If* $\operatorname{typ}(\mathbf{A}) = \mathbf{3}$ *and* $m \neq \widehat{m}$ *then* $\widehat{m} > m$*, and conditions* $(\dagger)$*,* $(\ddagger)_1$*, and* $(\ddagger)_2$ *in Claim 6.22 (2) hold for* G *and* $\mathbf{A}$*.*

Let M be an m-element multitrace of $\mathbf{A}$. Then $M = p(N, \dots, N)$ for some trace N and some polynomial $p \in \operatorname{Pol}(\mathbf{A}) = \mathfrak{C}$. Hence $m = |M| \leq |p(A, \dots, A)| \leq \widehat{m}$. Since we assumed $m \neq \widehat{m}$ we get that $m < \widehat{m}$. The definition of $\widehat{m}$ yields the existence of an operation $f \in \operatorname{Pol}(\mathbf{A}) = \mathfrak{C}$ such that f depends on at least two variables and has range of size $\widehat{m} > m$. Claim 6.13 (for $r = m$) implies that not all m-element subsets of A are multitraces of $\mathbf{A}$. Thus, by Claim 6.22, conditions $(\dagger)$, $(\ddagger)_1$, and $(\ddagger)_2$ hold for G and $\mathbf{A}$.

The proof of Theorem 6.1 will be complete if we show that $\widehat{m} > m$ and conditions $(\dagger)$, $(\ddagger)_1$, and $(\ddagger)_2$ from Claim 6.22 (2) cannot hold simultaneously for G and $\mathbf{A}$. We will assume that this is not the case, and work towards a contradiction.

Assumption 6.25. Let G be as in (†), and assume that $\mathbf{A}$ has a G-closed clone $\mathfrak{C} = \mathrm{Pol}(\mathbf{A})$ such that conditions $(\ddagger)_1$ and $(\ddagger)_2$ hold for the multitraces of $\mathbf{A}$. Furthermore we assume that $\widehat{m} > m$, and we fix an operation $f \in \mathrm{Pol}(\mathbf{A}) = \mathfrak{C}$ such that f depends on at least two variables and has range R of size $|R| = \widehat{m}$. Without loss of generality, we will assume that f is n-ary ($n \geq 2$) and depends on all of its variables.

For each i ($1 \leq i \leq n$) and $\bar{z} = (z_1, \ldots, z_{n-1}) \in A^{n-1}$ let $f_{i,\bar{z}}$ denote the unary term operation of $\mathbf{A}$ defined by

$$f_{i,\bar{z}}(x) = f(z_1, \ldots, z_{i-1}, x, z_i, \ldots, z_{n-1}).$$

The range of each $f_{i,\bar{z}}$ is a subset of R.

Claim 6.26. *Let $f_{i,\bar{z}}$ have range V.*

1. *If $V = R$ then V has distinct elements v, v' such that all m-element subsets of V that contain $\{v, v'\}$ are multitraces of $\mathbf{A}$.*
2. *If $V \subsetneq R$ then for every element $r \in R - V$ there exists an element v in V such that all m-element subsets of $V \cup \{r\}$ that contain $\{r, v\}$ are multitraces of $\mathbf{A}$.*
3. *If $V \subsetneq R$ and $m = 4$, then for every element $r \in R - V$ there exists an element v in V such that the 4-element subsets of $V \cup \{r, r'\}$ that contain $\{r, v\}$ are multitraces of $\mathbf{A}$ for all $r' \in R - V$, $r' \neq r$.*

Without loss of generality, we may assume throughout the proof of the claim that $i = 1$. Let $Y_1, \ldots, Y_s$ denote the kernel classes of $f_{1,\bar{z}}$, and $v_1, \ldots, v_s$ the values of $f_{1,\bar{z}}$ on these classes.

(1) Suppose first that $V = R$. Since f depends on more than one variable, there exists $\bar{y} \in A^{n-1}$ such that the function $f_{1,\bar{y}}$ differs from $f_{1,\bar{z}}$. Let us choose and fix such a $\bar{y}$. We may assume without loss of generality that there exists $x_1 \in Y_1$ such that $f_{1,\bar{y}}(x_1) \neq v_1$; say $f_{1,\bar{y}}(x_1) = v_2$. Thus, choosing elements $x_j \in Y_j$ for $j = 2, \ldots, s$, we get that

$$f(x_1, \bar{z}) = v_1, \quad f(x_1, \bar{y}) = v_2, \quad \text{and} \quad f(x_j, \bar{z}) = v_j \text{ for } j = 3, \ldots, s.$$

If $G = \mathsf{PSL}(2, 5)$, then by condition $(\ddagger)_1$ all 2-element sets $\{x_1, x_j\}$, $\{y_l, z_l\}$ are multitraces of $\mathbf{A}$, whence we get that all 3-element subsets $\{v_1, v_2, v_j\}$ ($j = 3, \ldots, s$) of V that contains $\{v_1, v_2\}$ are multitraces of $\mathbf{A}$. If $G = \mathsf{PGL}(2, 7)$, then by condition $(\ddagger)_1$ all sets $\{x_1, x_j, x_k\}$, $\{y_l, z_l\}$ are multitraces of $\mathbf{A}$, therefore we get that all 4-element subsets of V that contain $\{v_1, v_2\}$ are multitraces of $\mathbf{A}$.

(2) Now let $V \subsetneq R$, $r \in R - V$, and let $r = f(x_1, \bar{y})$. We have $x_1 \in Y_k$ for a unique k ($1 \leq k \leq s$). We may assume without loss of generality that $k = 1$. Choosing again elements $x_j \in Y_j$ for $j = 2, \ldots, s$, we get that

$$f(x_1, \bar{z}) = v_1, \quad f(x_1, \bar{y}) = r, \quad \text{and} \quad f(x_j, \bar{z}) = v_j \text{ for } j = 2, \ldots, s.$$

This is the same situation as in the preceding paragraph. Thus we get the same way as before that all m-element subsets of $V \cup \{r\}$ that contain $\{v_1, r\}$ are multitraces of $\mathbf{A}$.

(3) Suppose that, in addition to the assumptions in part (2), we have $m = 4$. With the notation from part (2) we have that all 4-element subsets of $V \cup \{r\}$ that contain $\{v_1, r\}$ are multitraces of $\mathbf{A}$. Now let $r' \in R - V$ be an arbitrary element distinct from r, and let $r' = f(p, \bar{q})$. By condition $(\ddagger)_1$, all 3-element sets $\{x_1, x_j, p\}$, $\{y_l, z_l, q_l\}$ are multitraces of $\mathbf{A}$, therefore we get that all 4-element subsets of $V \cup \{r, r'\}$ of the form $\{v_1, r, v_j, r'\}$ $(j = 2, \dots, s)$ are multitraces of $\mathbf{A}$ as well. Hence every 4-element subset of $V \cup \{r, r'\}$ that contains $\{v_1, r\}$ is a multitrace of $\mathbf{A}$, as claimed.

Now let t denote the largest number that is the size of the range of $f_{i,\bar{z}}$ for some $\bar{z}$ and i. Clearly, $t \geq 2$ since f is not constant. We may assume without loss of generality that the range of $f_{1,\bar{a}}$ has size t for some $\bar{a}$. We select such an $\bar{a}$ and will keep it fixed. Let $X_1, \dots, X_t$ denote the kernel classes of $f_{1,\bar{a}}$, and $u_1, \dots, u_t$ the values of $f_{1,\bar{a}}$ on these classes. Further, let $U = \{u_1, \dots, u_t\}$.

Claim 6.27. *$U \subsetneq R$.*

Suppose not. Then $U = R$, whence $t = \widehat{m}$. Claim 6.26 (1) applied to the operation $f_{1,\bar{a}}$ yields that U has two distinct elements, say u_1 and u_2, such that all m-element subsets of U that contain $\{u_1, u_2\}$ are multitraces of $\mathbf{A}$. By condition $(\ddagger)_2$ all these multitraces belong to the orbit O. By parts (2) of Lemmas 5.1 and 5.2 this is impossible if $|U| = t > m + 1$. Thus $t = m + 1$. By parts (1) of Lemmas 5.1 and 5.2 the partition of A with m blocks $X_1 \cup X_2, X_3, \dots, X_t$ has a transversal T that belongs to the orbit O. Thus, by condition $(\ddagger)_2$, T is a multitrace of $\mathbf{A}$. Furthermore, the multitrace $f_{1,\bar{a}}(T)$, which is equal to $U - \{u_1\}$ or $U - \{u_2\}$, also belongs to O. But then m of the $m + 1$ m-element subsets of U belong to the G-orbit O, which is impossible. This completes the proof of Claim 6.27.

Claim 6.28. *If $U \subsetneq R$ then $t < m$.*

Suppose $U \subsetneq R$ and $t \geq m$. Let $r \in R - U$ be arbitrary. Claim 6.26 (2) applied to the operation $f_{1,\bar{a}}$ yields that U has an element, say u_1, such that all m-element subsets of $U \cup \{r\}$ that contain $\{u_1, r\}$ are multitraces of $\mathbf{A}$. By condition $(\ddagger)_2$ all these multitraces belong to the orbit O. By parts (2) of Lemmas 5.1 and 5.2 this is impossible if $|U \cup \{r\}| > m + 1$. Thus $|U \cup \{r\}| \leq m + 1$. By assumption we have $|U| = t \geq m$, therefore $t = m$. By parts (1) of Lemmas 5.1 and 5.2 the partition of A with m blocks $X_1, X_2, \dots, X_t$ has a transversal T that belongs to the orbit O. Thus, by condition $(\ddagger)_2$, T is a multitrace of $\mathbf{A}$. Furthermore, the multitrace $U = f_{1,\bar{a}}(T)$ also belongs to O. But then m of the $m + 1$ m-element subsets of $U \cup \{r\}$ belong to the G-orbit O, which is impossible. This completes the proof of Claim 6.28.

Since $t \geq 2$ and $m = 3$ or $m = 4$, the only possibilities that are not ruled out by Claims 6.27 and 6.28 are the following: either $t = 3$ for $G = \mathsf{PGL}(2, 7)$, $m = 4$, or $t = 2$.

Claim 6.29. *$t = 3$ is impossible for $G = \mathsf{PSL}(2, 7)$, $m = 4$.*

Suppose that $G = \mathsf{PSL}(2, 7)$, $m = 4$, and $t = 3$. Since $|R| = \widehat{m} > 4$, there exist distinct elements $r, r' \in R - U$. Applying Claim 6.26 (3) to the operation $f_{1,\bar{a}}$ and to both of the elements $r \in R - U$ and $r' \in R - U$ we get that there exist elements $u, u' \in U$ such that all 4-element subsets of $U \cup \{r, r'\}$ that contain $\{u, r\}$ or $\{u', r'\}$ are multitraces of $\mathbf{A}$. This implies that if $u \neq u'$ then all 4-element subsets of the 5-element set $U \cup \{r, r'\}$ are multitraces of $\mathbf{A}$, while if $u = u'$ then four of the five 4-element subsets of $U \cup \{r, r'\}$ are multitraces of $\mathbf{A}$. This is impossible, because by condition $(\ddagger)_2$ all multitraces have to belong to the same G-orbit O of 4-element sets.

Claim 6.30. *$t = 2$ is impossible for both $G = \mathsf{PSL}(2, 5)$, $m = 3$ and $G = \mathsf{PGL}(2, 7)$, $m = 4$.*

Suppose that $t = 2$. If $G = \mathsf{PSL}(2, 5)$, $m = 3$, then an application of Claim 6.26 (2) to the operation $f_{1,\bar{a}}$ yields that $\{r, u_1, u_2\}$ is a multitrace of $\mathbf{A}$ for every element $r \in R - U$. If $G = \mathsf{PSL}(2, 7)$, $m = 4$, then an application of Claim 6.26 (3) shows that $\{r, r', u_1, u_2\}$ is a multitrace of $\mathbf{A}$ for any distinct elements $r, r' \in R - U$. Thus, in both cases,

(∗) all m-element subsets of R that contain the range U of $f_{1,\bar{a}}$ are multitraces of $\mathbf{A}$.

It follows from parts (2) of Lemmas 5.1 and 5.2 that $|R| \leq m+1$. But $|R| = \widehat{m} > m$, so $|R| = m + 1$.

Now choose n-tuples $\bar{d} = (d_1, \ldots, d_n)$ and $\bar{e} = (e_1, \ldots, e_n) \in A^n$ so that $f(\bar{d}) \in U$ and $f(\bar{e}) \in R - U$. The sequence $\bar{d}^{(i)} = (e_1, \ldots, e_i, d_{i+1}, \ldots, d_n)$ $(i = 0, \ldots, n)$ of n-tuples has two consecutive members $\bar{d}^{(k-1)}$ and $\bar{d}^{(k)}$ such that $f(\bar{d}^{(k-1)}) \in U$ and $f(\bar{d}^{(k)}) \in R-U$. Thus, for $\hat{d} = (e_1, \ldots, e_{k-1}, d_{k+1}, \ldots, d_n)$ the unary operation $f_{k,\hat{d}}$ has range containing a member of U and a member of $R-U$. However, by the maximality of t, the range of $f_{k,\hat{d}}$ has at most two elements. Thus $f_{k,\hat{d}}$ has a 2-element range, which we may assume to be equal to $\{u_1, r_1\}$ where $r_1 \in R-U$. The argument in the preceding paragraph that led to conclusion (∗) works for the operation $f_{k,\hat{d}}$ as well, in place of $f_{1,\hat{a}}$. Thus we get that

(∗∗) all m-element subsets of R that contain the range $\{u_1, r_1\}$ of $f_{k,\bar{d}}$ are multitraces of $\mathbf{A}$.

(∗) and (∗∗) imply that m of the $m + 1$ m-element subsets of R are multitraces of $\mathbf{A}$. By condition $(\ddagger)_2$ all there sets have to belong to the same G-orbit O, which is impossible. This contradiction completes the proof of Claim 6.30, and hence the proof of Theorem 6.1. □

References

[1] R. A. Beaumont, R. P. Peterson, *Set transitive permutation groups,* Canad. J. Math. **7** (1955), 35–42.

[2] P. J. Cameron, *Finite permutation groups and finite simple groups.* Bull. London Math. Soc. 13 (1981), no. 1, 1–22.

[3] P. J. Cameron, *Permutation groups,* London Mathematical Society Student Texts, vol. 45. Cambridge University Press, Cambridge, 1999.

[4] P. Dembowski, *Finite geometries,* Ergebnisse der Mathematik und ihrer Grenzgebiete, Band 44, Springer-Verlag, Berlin–New York, 1968

[5] J. D. Dixon, B. Mortimer, *Permutation groups,* Graduate Texts in Mathematics, vol. 163, Springer-Verlag, New York, 1996.

[6] R. L. Griess, *Twelve Sporadic Groups,* Springer Monographs in Mathematics, Springer-Verlag, Berlin–Heidelberg, 1998.

[7] Nguen Van Hoa [Khoa], *On the structure of self-dual closed classes of three-valued logic P_3,* Diskretn. Matematika **4** (1992), 82–95.

[8] Nguen Van Hoa [Khoa], *Families of closed classes of k-valued logic that are preserved by all automorphisms* (Russian), Diskret. Mat. **5** (1993), no. 4, 87–108.

[9] Nguen Van Hoa [Khoa], *Description of closed classes that are preserved by all inner automorphisms of k-valued logic* (Russian), Dokl. Akad. Nauk Belarusi **38** (1994), no. 3, 16–19, 122.

[10] D. Hobby, R. McKenzie , *The Structure of Finite Algebras,* Contemporary Mathematics **76**, American Mathematical Society, Providence, RI, 1988.

[11] B. Huppert, N. Blackburn, *Finite groups. III,* Grundlehren der Mathematischen Wissenschaften, vol. 243. Springer-Verlag, Berlin–New York, 1982.

[12] K. A. Kearnes, E. W. Kiss, M. Valeriote, *Minimal sets and varieties,* Trans. Amer. Math. Soc. **350** (1998), no. 1, 1–41.

[13] S. S. Marchenkov, *Homogeneous algebras,* Problemy Kibernet. **39** (1982), 85–106. (Russian)

[14] S. S. Marchenkov, *S-classification of functions of many-valued logic* (Russian), Diskret. Mat. **9** (1997), no. 3, 125–152; translation in: Discrete Math. Appl. **7** (1997), no. 4, 353–381; announcement of results in: *S-classification of idempotent algebras with finite support* (Russian), Dokl. Akad. Nauk **348** (1996), no. 5, 587–589.

[15] S. S. Marchenkov, *A-closed classes of many-valued logic that contain constants* (Russian), Diskret. Mat. **10** (1998), no. 3, 10–26; translation in: Discrete Math. Appl. **8** (1998), no. 4, 357–374.

[16] S. S. Marchenkov, *A-classification of idempotent functions of many-valued logic* (Russian), Diskretn. Anal. Issled. Oper. Ser. 1 **6** (1999), no. 1, 19–43, 97; announcement of results of [15], [16] in: Dokl. Akad. Nauk **366** (1999), no. 4, 455–457.

[17] P. P. Pálfy, *Unary polynomials in algebras I,* Algebra Universalis **18** (1984), 262–273.

[18] E. L. Post, *The Two-Valued Iterative Systems of Mathematical Logic,* Ann. Math. Studies **5**, Princeton University Press, Princeton, N.J. 1941.

[19] R. Ree, *Sur une famille de groupes de permutations doublement transitifs,* Canad. J. Math. **16** (1964), 797–820.

[20] L. Szabó, *Algebras that are simple with weak automorphisms,* Algebra Universalis **42** (1999), 205–233.

[21] Á. Szendrei, *Clones in Universal Algebra,* Séminaire de Mathématiques Supérieures, vol. 99, Les Presses de l'Université de Montréal, Montréal, 1986.

[22] Á. Szendrei, *Simple surjective algebras having no proper subalgebras,* J. Austral. Math. Soc. Ser. A **48** (1990), 434–454.

[23] Á. Szendrei, *A survey of clones closed under conjugation,* in: *Galois connections and applications* (Edited by K. Denecke, M. Erné and S. L. Wismath), pp. 297–343, Math. Appl., 565, Kluwer Acad. Publ., Dordrecht, 2004.

[24] S. V. Yablonskiĭ, *Functional constructions in a k-valued logic*, (Russian) Trudy Mat. Inst. Steklov. **51** (1958), 5–142.

(Keith A. Kearnes) Department of Mathematics, University of Colorado, Boulder, CO 80309-0395, U.S.A.

E-mail address: Keith.Kearnes@Colorado.EDU

(Ágnes Szendrei) Bolyai Institute, Aradi vértanúk tere 1, H–6720 Szeged, Hungary, and, Department of Mathematics, University of Colorado, Boulder, CO 80309-0395, U.S.A.

E-mail address: A.Szendrei@math.u-szeged.hu