# CLIQUES IN DERANGEMENT GRAPHS FOR INNATELY TRANSITIVE GROUPS

MARCO FUSARI, ANDREA PREVITALI, AND PABLO SPIGA

ABSTRACT. Given a permutation group $G$, the derangement graph of $G$ is the Cayley graph with connection set the derangements of $G$. The group $G$ is said to be innately transitive if $G$ has a transitive minimal normal subgroup. Clearly, every primitive group is innately transitive. We show that, besides an infinite family of explicit exceptions, there exists a function $f : \mathbb{N} \to \mathbb{N}$ such that, if $G$ is innately transitive of degree $n$ and the derangement graph of $G$ has no clique of size $k$, then $n \le f(k)$.

Motivation for this work arises from investigations on Erdős-Ko-Rado type theorems for permutation groups.

## 1. INTRODUCTION

One of the most beautiful results in extremal combinatorics is the Erdős-Ko-Rado theorem [8]: let $n$ and $k$ be positive integers with $1 \le 2k < n$ and let $\mathcal{F}$ be a family of $k$-subsets of $\{1, \ldots, n\}$. If any two elements from $\mathcal{F}$ intersect in at least one point, then $|\mathcal{F}| \le \binom{n-1}{k-1}$. Moreover, the inequality is attained if and only if there exists $x \in \{1, \ldots, n\}$ such that each element from $\mathcal{F}$ contains $x$.

There are various analogues of the Erdős-Ko-Rado theorem for a number of combinatorial structures. In this paper we are interested in the analogue for permutation groups. Let $G$ be a finite permutation group on $\Omega$. A subset $\mathcal{F}$ of $G$ is said to be **intersecting** if, for any two elements $g, h \in \mathcal{F}$, $gh^{-1}$ fixes some point of $\Omega$. This is a very natural definition; indeed, by writing $g$ as the $n$-tuple $(1^g, 2^g, \ldots, n^g)$, we see that $gh^{-1}$ fixes some point of $\Omega$ if and only if the $n$-tuples corresponding to $g$ and $h$ agree in at least one coordinate. Therefore, somehow, this mimics the definition of intersecting sets in the original Erdős-Ko-Rado theorem.

Observe that, for every $\omega \in \Omega$, the point stabilizer $G_\omega$ is intersecting. More generally, each coset of the stabilizer of a point is an intersecting set. Answering a question of Erdős, Cameron-Ku [5] and Larose-Malvenuto [22] have independently proved an analogue of the Erdős-Ko-Rado theorem when $G = \mathrm{Sym}(\Omega)$.[a] Unfortunately, in general only rarely $G_\omega$ is an intersecting set of maximal size in $G$[b] and hence no analogue of the Erdős-Ko-Rado theorem holds for arbitrary permutation groups. Even when $|G_\omega|$ is the maximal cardinality of an intersecting set for $G$, it is far from being true that all intersecting sets attaining the bound $|G_\omega|$ are

---

2010 *Mathematics Subject Classification.* Primary 05C35; Secondary 05C69, 20B05.

[a]An intersecting set of $\mathrm{Sym}(\Omega)$ has cardinality at most $(|\Omega| - 1)!$; moreover, the intersecting sets attaining the bound $(|\Omega| - 1)!$ are cosets of the stabilizer of a point.

[b]For instance, if we let the alternating group $\mathrm{Alt}(5)$ acting on the ten 2-subsets of $\{1, 2, 3, 4, 5\}$, we see that $\mathrm{Alt}(4)$ is an intersecting set of size 12, whereas the point stabilizer in this action has only cardinality 6.

cosets of the stabilizer of a point.[c] These two difficulties make investigations on intersecting sets of maximal size in arbitrary permutation groups more interesting and challenging.

Let $\omega \in \Omega$ with $G_\omega$ having maximum cardinality among point stabilizers.[d] The **_intersection density_** of the intersecting family $\mathcal{F}$ of $G$ is defined by

$$\rho(\mathcal{F}) = \frac{|\mathcal{F}|}{|G_\omega|}.$$

The **_intersection density_** of $G$ is

$$\rho(G) = \max\{\rho(\mathcal{F}) \mid \mathcal{F} \subseteq G, \mathcal{F} \text{ is intersecting}\}.$$

This invariant was introduced by Li, Song and Pantagi in [23] to measure how "close" $G$ is from satisfying the Erdős-Ko-Rado theorem.

Let $\mathcal{D}$ be the set of all **_derangements_** of $G$, where a derangement is a permutation without fixed points. The derangement graph of $G$ is the graph $\Gamma_G$ whose vertex set is the set $G$ and whose edge set consists of all pairs $(h, g) \in G \times G$ such that $gh^{-1} \in \mathcal{D}$. Thus, $\Gamma_G$ is the Cayley graph of $G$ with connection set $\mathcal{D}$. With this terminology, an intersecting family of $G$ is an **_independent set_** or **_coclique_** of $\Gamma_G$, and vice versa. As customary, we denote by $\omega(\Gamma_G)$ the maximal size of a clique and by $\alpha(\Gamma_G)$ the maximal size of a coclique (a.k.a. independent set).

Now, the clique-coclique bound [13, Theorem 2.1.1]

(1) $$\alpha(\Gamma_G)\omega(\Gamma_G) \leq |V\Gamma_G| = |G|$$

can be used to extract useful information on the intersection density of $G$. Indeed, from (1) and from the definition of intersection density, we obtain

(2) $$\rho(G) \leq \frac{|\Omega|}{\omega(\Gamma_G)}.$$

When $G$ is transitive and $|\Omega| \geq 2$, Jordan's theorem[e] ensures that $G$ has a derangement $g$ and hence $\{1, g\}$ is a clique of $\Gamma_G$ of cardinality 2. Therefore, (2) yields $\rho(G) \leq |\Omega|/2$.

Theorem 1.5 in [21] shows that, when $G$ is transitive and $|\Omega| \geq 3$, the derangement graph $\Gamma_G$ has a clique of cardinality 3, that is a triangle, and hence $\rho(G) \leq |\Omega|/3$. Despite the fact that Jordan's theorem is elementary, the proof of [21, Theorem 1.5] is quite involved and ultimately relies on the Classification of the Finite Simple Groups.

In the light of these two results, Question 6.1 in [21] asks for the existence of a function $f : \mathbb{N} \to \mathbb{N}$ such that, if $G$ is transitive of degree $n$ and $\Gamma_G$ has no $k$-clique, then $n \leq f(k)$. Indeed, when $k = 2$, we have $n \leq 1$ by Jordan's theorem and, when $k = 3$, we have $n \leq 2$ by [21, Theorem 1.5]. A similar question, formulated in terms of (weak) normal coverings of groups is in [4].

From [14] and [29, 30, 31], we see that there are remarkable applications of normal coverings and Kronecker classes in algebraic number theory. In fact, Question 6.1

---

[c]For instance, in the projective general linear group $G = \mathrm{PGL}_d(q)$ in its 2-transitive action on the $(q^d - 1)/(q - 1)$ points of the projective space $\mathrm{PG}_{d-1}(q)$, the intersecting sets of maximal cardinality are either cosets of the stabilizer of a point or cosets of the stabilizer of a hyperplane, see [34].

[d]Observe that all point stabilizers have the same cardinality when $G$ is transitive.

[e]See [32] for a beautiful account of Jordan's theorem and for a number of applications in various areas of mathematics.

in [21] is very much related to conjectures of Neumann and Praeger on coverings of finite groups for applications on Kronecker classes. We have summarized in Section 1.1 these applications and the connection with our work.

In this paper we make the first substantial progress towards this question. A permutation group $G$ on $\Omega$ is said to be ***innately transitive*** if $G$ has a minimal normal subgroup $N$ with $N$ transitive on $\Omega$. These permutation groups greatly generalize the class of primitive and quasiprimitive groups. Moreover, innately transitive groups admit a structural result similar to the O'Nan-Scott theorem for primitive and quasiprimitive groups [1]; furthermore, they play a substantial role in a number of questions in finite permutation groups, see for instance [11].

**Theorem 1.1.** *There exists a function $f_1 : \mathbb{N} \to \mathbb{N}$ such that, if $G$ is innately transitive of degree $n$ and the derangement graph of $G$ has no clique of size $k$, then $n \leq f_1(k)$.*

In particular, we answer [21, Question 6.1] when the permutation group $G$ is innately transitive. We make no particular effort in optimizing the function $f$ in Theorem 1.1, except when $k = 4$.[f]

**Theorem 1.2.** *If $G$ is innately transitive of degree $n$ and the derangement graph of $G$ has no clique of size 4, then $n \leq 3$.*

A permutation group $X$ on $\Omega$ is said to be ***semiregular*** if no non-identity element of $X$ fixes some point of $\Omega$, that is, $X_\omega = 1 \ \forall \omega \in \Omega$. Observe that a semiregular subgroup $X$ forms a clique in the derangement graph of $\mathrm{Sym}(\Omega)$.[g] In fact, Theorems 1.1 and 1.2 both follow from a more general result concerning semiregular subgroups in innately transitive permutation groups.

**Theorem 1.3.** *There exists a function $f_2 : \mathbb{N} \to \mathbb{N}$ such that, if $G$ is innately transitive of degree $n$ and $G$ has no semiregular subgroup of order at least $k$, then either $n \leq f_2(k)$, or $G$ is primitive of degree $12^\kappa$ and $G = M_{11}\mathrm{wr}A$, for some positive integer $\kappa$ and for some transitive subgroup $A$ of $\mathrm{Sym}(\kappa)$, where $M_{11}$ is the Mathieu group.*

*Moreover, if $G$ has no semiregular subgroup of order at least 4, then one of the following holds*

*(1) $n \leq 3$,*
*(2) $n = 6$, $G$ is primitive and $G \cong \mathrm{Alt}(5)$,*
*(3) $n = 6$, $G$ is primitive and $G \cong \mathrm{Alt}(6)$,*
*(4) $n = 36$, $G$ is primitive and $\mathrm{PSU}_3(3) \leq G \leq \mathrm{P\Gamma U}_3(3)$,*
*(5) $n = 12^\kappa$, $G$ is primitive and $G = M_{11}\mathrm{wr}A$, for some positive integer $\kappa$ and for some transitive subgroup $A$ of $\mathrm{Sym}(\kappa)$.*

It was discovered by Giudici [11] that the Mathieu group $M_{11}$ in its primitive action on 12 points has no non-identity semiregular elements. Permutation groups having this property are called ***elusive*** and they are of paramount importance for investigations on the Polycirculant conjecture, see [11] for details. More generally,

---

[f]We make a special effort in characterizing the innately transitive groups $G$ such that $\Gamma_G$ has no clique of size 4, because in the future we intend to use this result to classify arbitrary transitive groups $G$ with $\Gamma_G$ having no clique of size 4.

[g]Indeed, the matrix having rows indexed by the elements of $X$, columns indexed by the elements of $\Omega$ and having $i^g$ in row $g$ and column $i$ is a partial Latin square and hence a clique in the derangement graph.

Giudici has proved that, for every positive integer $\kappa$ and for every transitive subgroup $A$ of $\mathrm{Sym}(\kappa)$, the group $G = M_{11}\mathrm{wr}A$ endowed with the primitive product action on $12^{\kappa}$ points is elusive. Therefore, this is a genuine exception in Theorem 1.3.

1.1. **Normal coverings and Kronecker classes.** There are some remarkable connections between normal coverings and algebraic number fields, see for instance [18, 19, 20, 29].

Given an algebraic number field $k$ and a finite extension field $K$ of $k$ the **Kronecker set** of $K$ over $k$ is defined as the set of all prime ideals of the ring of integers of $k$ having a prime divisor of relative degree one in $K$. Then, two finite extensions of $k$ are said to be **Kronecker equivalent** if their Kronecker sets have finite symmetric difference, that is, the Kronecker sets differ only in at most a finite number of primes. This defines an equivalence relation and such extensions are said to belong to the same **Kronecker class**. Clearly, extensions in the same Kronecker class have strong arithmetical similarities.

The connection between problems about Kronecker classes in field extensions and group theoretic problems is explained in [18, 19, 29]. Let $K$ and $K'$ be finite extensions of a given fixed algebraic number field $k$ and let $M$ be a Galois extension of $k$ containing $K$ and $K'$. Let $G = \mathrm{Gal}(M/k)$, $U = \mathrm{Gal}(M/K)$ and $U' = \mathrm{Gal}(M/K')$, in particular, $U$ and $U'$ are the subgroups of $G$ corresponding to $K$ and $K'$ via the Galois correspondence. It is shown in [18, 19] that $K$ and $K'$ are Kronecker equivalent if and only if

$$\tag{3} \bigcup_{g \in G} U^g = \bigcup_{g \in G} U'^g.$$

This already gives a very strong connection between the problem of understanding Kronecker classes and natural questions in finite permutation groups. For instance, if we consider the permutation representations of $G$ on the right cosets of $U$ and on the right cosets of $U'$, then (3) is equivalent to the fact that in these two permutation representations of $G$ the set of derangements is the same.

There is one special case where (3) yields a natural connection with (weak) normal coverings. Indeed, the special case where $K'/k$ is a Galois extension and $K$ is an extension of $K'$ corresponds to $U \le U' \trianglelefteq G$. In particular, in this special case, $K/k$ and $K'/k$ are Kronecker equivalent if and only if

$$U' = \bigcup_{g \in G} U^g.$$

Using the terminology in [29], this yields that $U'$ is a $G$-covering of $U$. As $G$ acts by conjugation as a group of automorphisms on $U'$, when $U' \ne U$, we deduce that $\{U\}$ is a weak normal 1-covering of $U'$.

There is a number of problems arising in Kronecker classes in algebraic number fields that have been addressed using finite group theory. We report here some open conjectures.

**Conjecture 1.4** (Neumann, Praeger, see [31])**.** *There is an integer function $f$ such that, if $G$ is a finite group with subgroups $U$, $U'$ such that $|G : U'| = n$ and*

$$\bigcup_{g \in G} U^g = \bigcup_{g \in G} U'^g,$$

*then $|G : U| \leq f(n)$.*

This conjecture phrased in terms of Kronecker classes is as follows.

**Conjecture 1.5.** *There is an integer function $f$ such that, if $K/k$ is an extension of degree $n$ of algebraic number fields and $L/k$ is Kronecker equivalent to $K/k$, then $|L : k| \leq f(n)$.*

As we mentioned above, with respect to (weak) normal coverings, the case of particular interest is when $U \leq U' \trianglelefteq G$.

**Conjecture 1.6** (Neumann, Praeger, see [31])**.** *There is an integer function $g$ such that, if $U'$ is a finite group, $G$ is a group of automorphisms of $U'$ containing the inner automorphisms $\mathrm{Inn}(U')$ as a subgroup of index $n$, and $U$ is a subgroup of $U'$ with*

$$\bigcup_{g \in G} U^g = U',$$

*then $|G : U| \leq g(n)$.*

Conjectures 1.4 and 1.6 can be phrased in terms of permutations groups: we focus on Conjecture 1.4. Let $G, U, U'$ be as in the statement of Conjecture 1.4 and let $\Omega$ be the set of right cosets of $U$ in $G$. Now,

$$\bigcup_{g \in G} U^g$$

is the set of elements of $G$ fixing some element of $\Omega$. If this union equals $\bigcup_{g \in G} U'^g$ and $|G : U'| = n$, then a clique in the derangement graph of $G$ in its action on $\Omega$ has cardinality at most $n$. In fact, let $C$ be a clique of size greater than $n$. Then by the pigeonhole principle, $C$ intersects a coset of $U'$ in at least two elements. Then the ratio $xy^{-1}$ lies in $U'$ and hence $xy^{-1}$ is conjugate to an element of $U$. Therefore, $xy^{-1}$ fixes some point, contradicting the fact that $C$ is a clique. Therefore Conjecture 1.4 can be seen as a particular case of Question 1.6 in [21].

In particular, our Theorem 1.1 gives substantial new evidence[h] to the veracity of Conjecture 1.4 and hence, in turn, to Conjecture 1.5 on Kronecker classes.

## 2. Proofs of Theorems 1.1 and 1.2 from Theorem 1.3

In this section, we show that Theorem 1.3 implies Theorems 1.1 and 1.2.

*Proof of Theorem* 1.1. Let $f_2$ be the function from Theorem 1.3 and let

$$f_1(k) = \max(f_2(k), 12^{\log_2(k)}).$$

We show that Theorem 1.1 holds true with this choice of $f_1$.

As semiregular subgroups are cliques in the derangement graph, Theorem 1.1 follows immediately from Theorem 1.3 using $f_1$, except when $G$ is primitive of degree $12^\kappa$ and $G = M_{11} \mathrm{wr} A$, for some positive integer $\kappa$ and some transitive subgroup $A$ of $\mathrm{Sym}(\kappa)$. Therefore, it suffices to deal with this case.

Let $\Omega$ be the domain of $G$. Then $\Omega$ admits a Cartesian decomposition $\Delta^\kappa$, where $|\Delta| = 12$ and $G$ acts on $\Delta^\kappa$ via its natural primitive product action. In particular, we identify $\Omega$ with $\Delta^\kappa$ and we denote the elements of $G$ as

$$(h_1, \ldots, h_\kappa)a,$$

_____

[h]In fact, Theorem 1.1 implies the veracity of Conjecture 1.4 when the action of $G$ on the right cosets of $U$ is innately transitive.

with $h_1, \ldots, h_\kappa \in M_{11}$ and $a \in A$. Moreover, given $(\delta_1, \ldots, \delta_\kappa) \in \Omega$, we have

$$(\delta_1, \ldots, \delta_\kappa)^{(h_1, \ldots, h_\kappa)a} = (\delta_{1^{a-1}}^{h_{1^{a-1}}}, \ldots, \delta_{\kappa^{a-1}}^{h_{\kappa^{a-1}}}).$$

From Jordan's theorem, $M_{11}$ has a derangement $h$ in its action on $\Delta$. Now, the set

$$\{(h^{\varepsilon_1}, h^{\varepsilon_2}, \ldots, h^{\varepsilon_\kappa}) \in M_{11}^\kappa \mid \varepsilon_1, \ldots, \varepsilon_\kappa \in \{0, 1\}\}$$

has cardinality $2^\kappa$ and it is a clique in $\Gamma_G$. In particular, if $2^\kappa \geq k$, then $\Gamma_G$ has a clique of size at least $k$. Otherwise, $2^\kappa < k$ and hence $\kappa < \log_2(k)$. Therefore,

$$|\Omega| = 12^\kappa < 12^{\log_2(k)} \leq f_1(k).$$

Thus, Theorem 1.1 follows also in this case. $\qquad\square$

*Proof of Theorem* 1.2. Let $G$ be innately transitive and assume that $\Gamma_G$ has no clique of size 4. Arguing as in the previous proof, we may assume that $G$ is one of the groups appearing in parts (2)–(5) of Theorem 1.3. Moreover, in part (5) we may assume that $\kappa = 1$. We have checked with a computer, using the computer algebra system `magma` [2], that in the derangement graph of each these permutation groups there is a clique of size 4. $\qquad\square$

Now, in the rest of this paper, we may focus only on Theorem 1.3.

## 3. Reduction of Theorem 1.3 to primitive simple groups

We recall that a permutation group $G$ on $\Omega$ is ***primitive*** if $\Omega$ admits no non-trivial $G$-invariant partition.[i] Moreover, $G$ is said to be ***quasiprimitive*** if each non-identity normal subgroup of $G$ is transitive on $\Omega$. It is remarkable that these concepts are already present in the work of Galois, see [27] for historical details.

Since the orbits of a normal subgroup of a transitive group form a system of imprimitivity, we deduce that each primitive group is quasiprimitive. Moreover, directly from the definition, each quasiprimitive group is innately transitive. Thus, we have the hierarchy

$$\text{primitive} \Longrightarrow \text{quasiprimitive} \Longrightarrow \text{innately transitive.}$$

**Lemma 3.1.** *Let $G$ be an innately transitive group on $\Omega$, let $N$ be a minimal normal subgroup of $G$ transitive on $\Omega$, let $\Sigma$ be a system of imprimitivity, let $\pi : G \to \mathrm{Sym}(\Sigma)$ be the natural homomorphism given by the action of $G$ on $\Sigma$ and let $G^\Sigma$ be the image of $\pi$. If $|\Sigma| > 1$ and $\bar{X}$ is a semiregular subgroup of $G^\Sigma$, then $\pi^{-1}(\bar{X})$ is a semiregular subgroup of $G$.*

*Proof.* Let $K = \mathrm{Ker}(\pi)$. Since $N$ is a minimal normal subgroup of $G$, we have $N \leq K$ or $K \cap N = 1$. If $N \leq K$, then $K$ is transitive because so is $N$. Since $K$ acts trivially on $\Sigma$, $K$ fixes setwise each element of $\Sigma$ and, since $|\Sigma| > 1$, we deduce that $K$ is intransitive. This contradiction yields $K \cap N = 1$. Hence $N$ centralizes $K$. Since $N$ is transitive on $\Omega$, we deduce from [7, Theorem 4.2A] that $K$ is semiregular on $\Omega$.

Let $X = \pi^{-1}(\bar{X})$. We prove that $X$ is semiregular on $\Omega$. Indeed, let $\omega \in \Omega$ and let $\sigma \in \Sigma$ with $\omega \in \sigma$. Clearly, $X_\omega \leq X_\sigma$ because each permutation of $G$ fixing $\omega$ must fix the block of the system of imprimitivity $\Sigma$ containing $\omega$. As $\bar{X}$ is semiregular on $\Sigma$, we have $\bar{X}_\sigma = 1$, that is, $X_\sigma$ fixes setwise each element of $\Sigma$.

---

[i] A partition $\pi$ of $\Omega$ is trivial if either each part of $\pi$ has cardinality 1 and hence $\pi = \{\{\omega\} \mid \omega \in \Omega\}$, or $\pi$ consists of only one part and hence $\pi = \{\Omega\}$.

Therefore, $\pi(X_\sigma) = 1$ and $X_\omega \leq X_\sigma \leq \text{Ker}(\pi) = K$. As $K$ is semiregular on $\Omega$, we obtain $X_\omega \leq K_\omega = 1$. This shows that $X$ is semiregular on $\Omega$. $\qquad\square$

The scope of this section is to reduce the proof of Theorem 1.3 to the case of simple primitive groups. The modern key for analyzing a finite primitive permutation group $G$ is to study the **socle** $N$ of $G$, that is, the subgroup generated by the minimal normal subgroups of $G$. The socle of a non-trivial finite group is isomorphic to the non-trivial direct product of simple groups; moreover, for finite primitive groups, these simple groups are pairwise isomorphic. The O'Nan-Scott theorem describes in detail the embedding of $N$ in $G$ and collects some useful information about the action of $N$. In [25, Theorem], five types of primitive groups are defined (depending on the group- and action-structure of the socle), namely HA (Affine), AS (Almost Simple), SD (Simple Diagonal), PA (Product Action) and TW (Twisted Wreath), and it is shown that every primitive group belongs to exactly one of these types. We remark that in [28] this subdivision into types is refined, namely the PA type in [25] is partitioned in four parts, which are called HS (Holomorphic Simple), HC (Holomorphic Compound), CD (Compound Diagonal) and PA. For what follows, we find it convenient to use this subdivision into eight types of the finite primitive permutation groups.[j]

We start with a technical lemma dealing with the exceptional family involving the Mathieu group arising in Theorem 1.3.

**Lemma 3.2.** *Let $G$ be an innately transitive group on $\Omega$, let $\Sigma$ be a system of imprimitivity such that the permutation group $G^\Sigma$ induced by $G$ on $\Sigma$ is isomorphic to $M_{11}\text{wr}A$ with its natural primitive product action on $12^\kappa$ points, for some positive integer $\kappa$ and some transitive subgroup $A$ of $\text{Sym}(\kappa)$, and let $\pi : G \to \text{Sym}(\Sigma)$ be the natural homomorphism given by the action of $G$ on $\Sigma$. Then either $G$ in its action on $\Omega$ has semiregular subgroups of order at least $\min(|\text{Ker}(\pi)| \cdot 11^\kappa, 660^\kappa)$, or $\Sigma = \Omega$ and the action of $G = M_{11}\text{wr}A$ on $\Omega$ is the natural primitive product action on $12^\kappa$ points.*

*Proof.* Let $K$ be the kernel of $\pi$. By definition, $G^\Sigma$ is the image of $\pi$. Let $N$ be a minimal normal subgroup of $G$ with $N$ transitive on $\Omega$: the existence of $N$ is guaranteed by the fact that $G$ is innately transitive on $\Omega$.

We first assume $K = 1$. As $G \cong G^\Sigma = M_{11}\text{wr}A$, we deduce $N$ is the unique minimal normal subgroup of $G$, $G$ is quasiprimitive on $\Omega$ and $N = M_{11}^\kappa$. Let $\sigma \in \Sigma$ and let $\omega \in \sigma$. Since $G^\Sigma$ is endowed with its natural primitive product action of degree $12^\kappa$, we get

$$G_\sigma = \text{PSL}_2(11)\text{wr}A \quad \text{and} \quad N_\sigma = \text{PSL}_2(11)^\kappa.$$

If $\Sigma$ is the trivial system of imprimitivity $\{\{\omega\} \mid \omega \in \Omega\}$, then the action of $G = M_{11}\text{wr}A$ on $\Omega$ is the natural primitive product action on $12^\kappa$ points and the lemma is satisfied. Therefore, for the rest of the proof we assume that $\Sigma$ is not the trivial system of imprimitivity. Therefore, $G$ is imprimitive on $\Omega$ and $G_\omega < G_\sigma$. In particular, there exists a maximal subgroup $R$ of $G_\sigma$ with $G_\omega \leq R$. Since there is a one to one order-reversing correspondence between the lattice of subgroups of $G$ containing $G_\omega$ and the systems of imprimitivity for $G$ acting on $\Omega$, $R$ corresponds

---

[j]This division has the advantage that there are no overlaps between the eight O'Nan-Scott types of primitive permutation groups.
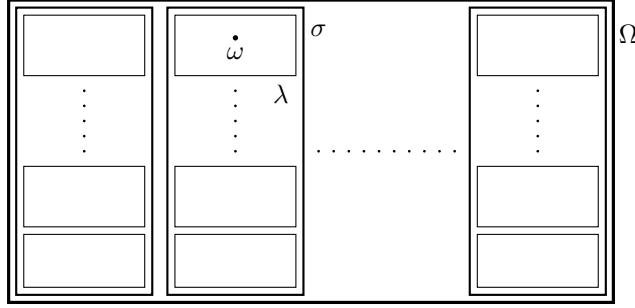
FIGURE 1. Systems of imprimitivity $\Sigma$ and $\Lambda$: $\Sigma$ is shown with thick lines

to the stabilizer of a block $\lambda$ in a system of imprimitivity, $\Lambda$ say. As $G_\lambda = R \leq G_\sigma$, $\Lambda$ is a refinement of the system of imprimitivity $\Sigma$. See Figure 1.

Set $H = G_\sigma$ and $\Lambda_\sigma = \{\mu \in \Lambda \mid \mu \subseteq \sigma\}$. We claim that $H$ acts primitively and faithfully on $\Lambda_\sigma$. The fact that $H$ acts primitively on $\Lambda_\sigma$ follows from the fact that, by definition, $R$ is a maximal subgroup of $G_\sigma = H$ and from the fact that $R = G_\lambda$ is the stabilizer of the part $\lambda \in \Lambda_\sigma$ in the system of imprimitivity $\Lambda$. Let

$$L = \bigcap_{h \in H} R^h.$$

Observe that $\mathrm{PSL}_2(11)^\kappa$ is the unique minimal normal subgroup of $H$. Therefore, if $H$ were not faithful on $\Lambda_\sigma$, that is $L \neq 1$, then $L$ contains the socle $\mathrm{PSL}_2(11)^\kappa = N_\sigma$ of $H$. Now, since $N$ is transitive on $\Omega$, we have $G = G_\omega N$. Intersecting both sides of this equality with $G_\sigma$ and using the modular law, we deduce $G_\sigma = G_\omega N_\sigma$. Therefore, $N_\sigma$ seen as a permutation group on $\Omega$ is transitive on the points contained in the block $\sigma$. As $L \geq N_\sigma$, we deduce that $L$ is transitive on the points contained in the block $\sigma$, which is a contradiction because $L \leq R = G_\lambda$ fixes setwise the subset $\lambda$ of $\Omega$ and $\lambda \subsetneq \sigma$.

We apply the O'Nan-Scott theorem to the primitive permutation group $H$ in its action on $\Lambda_\sigma$. Since H, as an abstract group, is isomorphic to $\mathrm{PSL}_2(11)\mathrm{wr}A$, $H$ in its primitive action on $\Lambda_\sigma$ is of type

- AS (when $\kappa = 1$), or PA (when $\kappa > 1$), or
- SD, or CD, or
- TW.

We deal with each of these cases in turn.

Assume that $H$ in its action on $\Lambda_\sigma$ has type AS or PA. Thus, we have

$$G_\lambda = R = B\mathrm{wr}A,$$

for some maximal subgroup $B$ of $\mathrm{PSL}_2(11)$. This shows that $G$ in its action on $\Lambda$ has stabilizer the wreath product $B\mathrm{wr}A$. Therefore, $\Lambda$ admits a $G$-invariant Cartesian decomposition $\Lambda'^\kappa$, where $\Lambda'$ is the set of right cosets of $B$ in $M_{11}$ and has cardinality $|M_{11} : B|$. Now, $\mathrm{PSL}_2(11)$ has four conjugacy classes of maximal subgroups: isomorphic to $11 : 5$, $6 : 2$, and two conjugacy classes isomorphic to $\mathrm{Alt}(5)$. Therefore, $B$ is $M_{11}$-conjugate to one of these five subgroups. We have computed with the auxiliary help of a computer these five permutation representations and we have computed their semiregular subgroups: in the action of $M_{11}$ on the cosets

of $11 : 5$ there are semiregular subgroups of order 144, in the action of $M_{11}$ on the cosets of $6 : 2$ there are semiregular subgroups of order 55, in the action of $M_{11}$ on the cosets of $\mathrm{Alt}(5)$ (for each of the two choices of $M_{11}$-conjugacy classes) there are semiregular subgroups of order 11. In particular, $M_{11}$ in its action on $\Delta'$ has semiregular subgroups of order at least 11. Therefore, $G = M_{11}\mathrm{wr}A$ in its action on $\Lambda = \Delta'^{\kappa}$ has semiregular subgroups of order at least $11^{\kappa}$. Applying Lemma 3.1 (with $\Sigma = \Lambda$), we deduce that $G$ in its action on $\Omega$ has semiregular subgroups of order at least $11^{\kappa}$.

Assume that $H$ in its action on $\Lambda_{\sigma}$ has type SD or CD. Recall that $N_{\sigma} = \mathrm{PSL}_2(11)^{\kappa}$ is the socle of $H$. Let $T_1, \ldots, T_{\kappa}$ be the $\kappa$ simple direct factors of $N_{\sigma}$. Then $(N_{\sigma})_{\lambda} = N_{\lambda}$ is isomorphic to the direct product of $a$ diagonal subgroups, indeed, up to relabeling the indexed set, there exists a divisor[k] $a > 1$ of $\kappa$ such that

$$N_{\lambda} = \mathrm{Diag}(T_1 \times \cdots \times T_a) \times \mathrm{Diag}(T_{a+1} \times \cdots \times T_{2a}) \times \cdots \times \mathrm{Diag}(T_{\kappa-a+1} \times \cdots \times T_{\kappa}).$$

Now, if we let

$$X = \{(x_1, \ldots, x_{\kappa}) \in N_{\sigma} = \mathrm{PSL}_2(11)^{\kappa} \mid x_{ia} = 1 \,\forall i \in \{1, \ldots, \kappa/a\}\},$$

then we see that $X \cap N_{\lambda} = 1$. Therefore, $X$ acts semiregularly on $\Lambda_{\sigma}$. What is more, from the definition of $X$ we deduce $N_{\lambda^n} \cap X = N_{\lambda}^n \cap X = 1$, $\forall n \in N$. As $N$ is transitive on $\Lambda$, we get that $X$ is semiregular on $\Lambda$. Applying Lemma 3.1 (with $\Sigma = \Lambda$), we deduce that $G$ in its action on $\Omega$ has semiregular subgroups of order at least $|X| = |\mathrm{PSL}_2(11)|^{\kappa-\kappa/a} = 660^{\kappa-\kappa/a} \geq 660^{\kappa/2} \geq 11^{\kappa}$.

Assume that $H$ in its action on $\Lambda_{\sigma}$ has type TW. Then the socle $N_{\sigma}$ of $H = G_{\sigma}$ acts regularly on $\Lambda_{\sigma}$, that is, $N_{\lambda} = 1$. As $N_{\omega} \leq N_{\lambda} = 1$, we deduce $N_{\omega} = 1$ and hence $N$ is regular on $\Omega$. So $G$ in its action on $\Omega$ has semiregular subgroups of order at least $|N| = |M_{11}|^{\kappa} \geq 11^{\kappa}$.

It remains to consider the case that $G$ does not act faithfully on $\Sigma$, that is $K \neq 1$; we pivot on the previous part of the proof. Let $\Lambda$ be the system of imprimitivity consisting of the $K$-orbits, that is, $\Lambda = \{\omega^K \mid \omega \in \Omega\}$. Let $\omega \in \Omega$, let $\sigma \in \Sigma$ with $\omega \in \sigma$ and let $\lambda = \omega^K \in \Lambda$. Observe that the stabilizer of the block $\lambda$ in $G$ is $G_{\lambda} = KG_{\omega}$. As $K$ and $G_{\omega}$ are both subgroups of $G_{\sigma}$, we get $G_{\lambda} \leq G_{\sigma}$. Therefore, $\Lambda$ is a refinement of the the system of imprimitivity $\Sigma$. See again Figure 1: here the system of imprimitivity $\Lambda$ is formed by the $K$-orbits.

We have

$$K \leq \bigcap_{g \in G} (KG_{\omega})^g \leq \bigcap_{g \in G} G_{\sigma}^g = \mathrm{Ker}(\pi) = K.$$

Therefore, $K$ is also the kernel of the action of $G$ on $\Lambda$. In particular, applying the first part of the proof with the group $G$ replaced by $G/K$ and with the set $\Omega$ replaced by $\Lambda$, we deduce that either

- $G/K$ in its action on $\Lambda$ has a semiregular subgroup of order at least $11^{\kappa}$, or
- $\Lambda = \Sigma$ and the action of $G/K$ on $\Lambda$ is the natural primitive product action on $12^{\kappa}$ points.

In the first case, Lemma 3.1 implies that $G$ in its action on $\Omega$ has a semiregular subgroup of order at least

$$|K| \cdot 11^{\kappa} \geq \min(|\mathrm{Ker}(\pi)| \cdot 11^{\kappa}, 660^{\kappa}).$$

---

[k]When $a = \kappa$, $H$ has type SD, whereas when $1 < a < \kappa$, $H$ has type CD.

This concludes the analysis of the first case.[1]

We deal with the second case. Observe that in this case Figure 1 is somehow misleading, because in this case we have $\Lambda = \Sigma$. Let $M = NK = N \times K$. We have

$$(4) \qquad\qquad M = NM_\omega,$$

$$(5) \qquad\qquad M_\lambda = N_\lambda \times K,$$

where the first equality follows from the fact that $N$ is transitive on $\Omega$ and the second equality follows from the fact that $K$ fixes setwise the $K$-orbit $\lambda = \omega^K$. Since $M_\omega \le M_\lambda = N_\lambda \times K$, we may write each element of $m \in M_\omega$ as an ordered pair $ab$, for a unique $a \in N_\lambda$ and a unique $b \in K$. Let $\pi_{N_\lambda} : M_\omega \to N_\lambda$ and $\pi_K : M_\omega \to K$ be the natural projections. From (4), $\pi_K$ is surjective. Let $m \in \mathrm{Ker}(\pi_{N_\lambda})$. Then $m \in K \cap M_\omega = K_\omega = 1$, because $K$ is semiregular on $\Omega$. Thus $\pi_{N_\lambda}$ is injective. Moreover, since $M_\lambda$ is transitive on the points contained in the block $\lambda$ and since $\lambda = \omega^K$, from (5), we deduce

$$|N_\lambda||K| = |M_\lambda| = |M_\omega||\omega^K| = |M_\omega||K : K_\omega| = |M_\omega||K|.$$

This yields $|N_\lambda| = |M_\omega|$. As $\pi_{N_\lambda} : M_\omega \to N_\lambda$ is injective, we obtain that $\pi_{N_\lambda}$ is surjective and hence it is a bijection. This shows that

$$\psi = \pi_{N_\lambda}^{-1} \circ \pi_K : N_\lambda \to K$$

is a surjective group homomorphism. Furthermore, from the definitions of $\pi_{N_\lambda}$ and $\pi_K$, we have

$$M_\omega = \{aa^\psi \mid a \in N_\lambda\}.$$

Recall that, in the case under consideration, $\Lambda = \Sigma$. As $N_\lambda = N_\sigma = \mathrm{PSL}_2(11)^\kappa$ and as $\psi : N_\lambda \to K$ is a surjective group homomorphism, we get $K \cong \mathrm{PSL}_2(11)^\ell$ for some $1 \le \ell \le \kappa$, and $\mathrm{Ker}(\psi) = \mathrm{PSL}_2(11)^{\kappa-\ell}$.

Now, if $a \in N_\omega$, then $a \in M_\omega$ and hence $a \in \mathrm{Ker}(\psi)$. Conversely, if $a \in \mathrm{Ker}(\psi)$, then $a = aa^\psi \in M_\omega \cap N = N_\omega$. This yields $\mathrm{PSL}_2(11)^{\kappa-\ell} = \mathrm{Ker}(\psi) = N_\omega$.

Since $N$ is transitive on $\Omega$, we have $G = NG_\omega$. This implies that $G_\omega$ acts transitively by conjugation on the $\kappa$ simple direct factors of $N = M_{11}^\kappa$. Thus $G_\omega$ acts transitively by conjugation on $\kappa$ the simple direct factors of $N_\lambda = \mathrm{PSL}_2(11)^\kappa$. As $N \trianglelefteq G$, we have $N_\omega \trianglelefteq G_\omega$. Putting together the fact that $G_\omega$ acts transitively on the simple direct factors of $N_\lambda = \mathrm{PSL}_2(11)^\kappa$ and the fact that $N_\omega = \mathrm{PSL}_2(11)^{\kappa-\ell} \trianglelefteq G_\omega$, we deduce $\ell = \kappa$. Therefore, $|K| = |\mathrm{PSL}_2(11)^\kappa|$ and hence $G$ in its action on $\Omega$ has a semiregular subgroup of order at least $|K| = 660^\kappa \ge \min(|\mathrm{Ker}(\pi)| \cdot 11^\kappa, 660^\kappa)$. $\square$

Using Lemma 3.2, we can reduce Theorem 1.3 to the realm of primitive groups.

**Proposition 3.3.** *Suppose that Theorem* 1.3 *holds true for primitive permutation groups. Then Theorem* 1.3 *holds true.*

*Proof.* Let $g : \mathbb{N} \to \mathbb{N}$ be a function witnessing that Theorem 1.3 holds true for primitive permutation groups. This means that, if $G$ is primitive of degree $n$ and $G$ has no semiregular subgroup of order at least $k$, then either $n \le g(k)$, or $G$ has degree $12^\kappa$ and $G = M_{11}\mathrm{wr}A$, for some positive integer $\kappa$ and for some transitive subgroup $A$ of $\mathrm{Sym}(\kappa)$. Moreover, if $G$ has no semiregular subgroup of order at least 4, then one of parts (1)–(5) holds.

Let $f : \mathbb{N} \to \mathbb{N}$ be the function defined by

$$f(k) = \max(g(k)!k, k!(k-1)).$$

---

[1]The relevance of $600^\kappa$ in the inequality above arises when dealing with the second case.

We show that the first part of Theorem 1.3 holds true using this function $f$. Let $G$ be an innately transitive group of degree $n$ and suppose that $G$ has no semiregular subgroup of order at least $k$. If $G$ is primitive, then we have nothing to prove because we are assuming the veracity of Theorem 1.3 for primitive groups. Therefore, we may suppose that $G$ is imprimitive.

Let $\Omega$ be the domain of $G$ and let $N$ be a minimal normal subgroup witnessing that $G$ is innately transitive, that is, $N$ is transitive on $\Omega$. Let $\Sigma$ be a system of imprimitivity for the action of $G$ on $\Omega$ with the property that $G$ acts primitively on $\Sigma$.[m] Let $K$ be the kernel of the action of $G$ on $\Sigma$ and let $G^{\Sigma} \cong G/K$ be the permutation group induced by $G$ on $\Sigma$. We denote by $\pi : G \to \mathrm{Sym}(\Sigma)$ the natural homomorphism; by definition, $G^{\Sigma}$ is the image of $\pi$.

Let $\bar{X}$ be a semiregular subgroup of $G^{\Sigma}$ and let $X = \pi^{-1}(\bar{X})$ be the preimage of $\bar{X}$ via $\pi$. By Lemma 3.1, $X$ is semiregular on $\Omega$. As $G$ has no semiregular subgroups of order at least $k$, we get

(6) $$|\bar{X}||K| = |X| \le k - 1.$$

As $|K| \ge 1$, (6) shows that the primitive group $G^{\Sigma}$ has no semiregular subgroups of order at least $1 + (k - 1)/|K| \le k$. Since we are assuming the veracity of Theorem 1.3 for primitive permutation groups, we deduce that either

- $|\Sigma| \le g(k)$, or
- $G^{\Sigma}$ is primitive of degree $12^{\kappa}$ and $G^{\Sigma} = M_{11}\mathrm{wr}A$, for some positive integer $\kappa$ and for some transitive subgroup $A$ of $\mathrm{Sym}(\kappa)$.

Assume first that $|\Sigma| \le g(k)$. In particular,

$$|G^{\Sigma}| \le |\mathrm{Sym}(g(k))| \le g(k)!.$$

Since $n \le |G|$, we deduce

$$n \le |G| = |G : K||K| = |G^{\Sigma}||K| \le g(k)!k \le f(k),$$

where we are using (6) in the second inequality.

Assume that the second possibility above holds. Our auxiliary Lemma 3.2 implies that either $G$ in its action on $\Omega$ has a semiregular subgroup of order at least $\min(|K| \cdot 11^{\kappa}, 660^{\kappa}) \ge 11^{\kappa}$, or $\Sigma = \Omega$ and the action of $G = M_{11}\mathrm{wr}A$ on $\Omega$ is the natural primitive product action on $12^{\kappa}$ points. The second case is impossible in our situation because we are assuming that $G$ is imprimitive on $\Omega$. Moreover, if $k \le 11^{\kappa}$, then $G$ does have a semiregular subgroup of order at least $k$. Assume then $11^{\kappa} < k$. Observe that $G^{\Sigma} = M_{11}\mathrm{wr}A$ has a faithful permutation representation of degree $11^{\kappa}$ and hence $|G^{\Sigma}| \le (11^{\kappa})! \le k!$. Therefore,

$$n = |\Omega| \le |G| = |G^{\Sigma}||K| \le k!(k - 1) \le f(k),$$

where as above we are using (6) in the second inequality.

It remains to prove the second part of the statement of Theorem 1.3 for innately transitive groups. Therefore, let $G$ be innately transitive with no semiregular subgroups having order at least 4. We use the notation above (with $k = 4$). In particular, we may assume that $G$ is not primitive, because we are assuming the veracity of Theorem 1.3 for primitive groups. Recall that $G^{\Sigma}$ is primitive and either

- each semiregular subgroup of $G^{\Sigma}$ has order at most $(k - 1)/|K| = 3/|K|$, see (6) with $k = 4$, or

---

[m]The existence of $\Sigma$ is clear: choose a system of imprimitivity whose blocks have cardinality as large as possible.

- $G^\Sigma$ has degree $12^\kappa$ and $G^\Sigma = M_{11}\mathrm{wr}A$, for some positive integer $\kappa$ and for some transitive subgroup $A$ of $\mathrm{Sym}(\kappa)$.

Assume that the second possibility above holds. Our auxiliary Lemma 3.2 implies that either $G$ in its action on $\Omega$ has a semiregular subgroup of order at least $11^\kappa$, or $\Sigma = \Omega$ and the action of $G = M_{11}\mathrm{wr}A$ on $\Omega$ is the natural primitive product action on $12^\kappa$ points. In the first case we have a semiregular subgroup of order at least $11 \geq 4$ and in the second case we obtain that part (5) holds. This concludes the proof for this case.

Assume now that the first possibility above holds. In particular, as $3/|K| < 4$ and as $G^\Sigma$ is primitive, by hypothesis, one of parts (1)–(5) holds for $G^\Sigma$. Observe that part (5) is exactly the second possibility, which we have already dealt with; therefore, we may disregard this part from further consideration. Before dealing with each of the remaining four possibilities we make some preliminary observations.

Recall that $|K| \leq 3$, because $K$ is semiregular on $\Omega$ and $G$ has no semiregular subgroups of order at least 4. Assume $|K| \in \{2,3\}$. Then $3/|K| < 2$ and hence $G^\Sigma$ has no non-trivial semiregular subgroups. A direct inspection on parts (1)–(4) shows that $|\Sigma| = 1$ and $G^\Sigma = 1$. This is impossible because $\Sigma$ is a non-trivial system of imprimitivity of $\Omega$ and hence $|\Sigma| > 1$.

Assume $|K| = 1$. In particular, $G \cong G^\Sigma$ as abstract groups. We have constructed with a computer the abstract group $G$ (for each of the cases arising in parts (1)–(4)), we have determined all the imprimitive innately transitive faithful actions of these groups and we have verified that in each action $G$ admits a semiregular subgroup of order at least 4. $\square$

In the light of Proposition 3.3, for the rest of the paper we may focus only on the class of primitive groups. In the rest of the section, we reduce the proof of Theorem 1.3 further, indeed to the case of primitive simple groups.

For six of the eight O'Nan-Scott types, the proof of Theorem 1.3 is immediate: the socle of $G$ contains a subgroup acting regularly on the domain and hence forming a clique in the derangement graph.

**Lemma 3.4.** *Let $G$ be a primitive group of degree $n$ of type HA, HS, HC, TW, SD or CD. Then $G$ has a semiregular subgroup of order $n$. In particular, Theorem* 1.3 *holds true in these cases.*

*Proof.* Let $N$ be the socle of $G$ and let $\Omega$ be the domain of $G$.

When $G$ is of type HA or TW, $N$ acts regularly on $\Omega$. In particular, $N$ is a clique in $\Gamma_G$ of cardinality $|N| = |\Omega| = n$.

When $G$ is of type HS or HC, $N$ is the direct product of two minimal normal subgroups of $G$, say $M_1$ and $M_2$. From the description of the primitive groups of type HS or HC, we see that $M_1$ and $M_2$ act regularly on $\Omega$ and they form a clique in $\Gamma_G$ of cardinality $|M_i| = |\Omega| = n$.

Suppose $G$ is of type SD. Then $N = T_1 \times \cdots \times T_{\ell+1}$, where $T_1, \ldots, T_{\ell+1}$ are pairwise isomorphic non-abelian simple groups. From the description of the primitive groups of type SD, we see that $|\Omega| = |T_1|^\ell$ and that $T_1 \times \cdots \times T_\ell$ acts regularly on $\Omega$. Therefore, as above, $T_1 \times \cdots \times T_\ell$ forms a clique in $\Gamma_G$ of cardinality $|\Omega| = n$.

Suppose that $G$ is of type CD. Then $\Omega$ admits a non-trivial Cartesian decomposition, that is, $\Omega = \Delta^\kappa$ for some finite set $\Delta$ and for some positive integer $\kappa \geq 2$, and we have an embedding $G \leq H\mathrm{wr}\mathrm{Sym}(\kappa)$, where the wreath product $H\mathrm{wr}\mathrm{Sym}(\kappa)$ acts on $\Delta^\kappa$ primitively, $H \leq \mathrm{Sym}(\Delta)$ and $H$ is of type SD in its action on $\Delta$. Now,

if the socle of $H$ is isomorphic to $T^{\ell+1}$, for some non-abelian simple group $T$ and for some positive integer $\ell \geq 1$, then the socle of $G$ is isomorphic to $T^{\kappa(\ell+1)}$. In particular, the socle of $G$ contains a subgroup isomorphic to $T^{\kappa\ell}$ acting regularly on $\Omega$ and we may argue as above. $\qquad\square$

In the light of Lemma 3.4 it is clear that the bulk of the argument for proving Theorem 1.3 is dealing with primitive groups of AS and PA type. For dealing with these two cases, we require detailed information on non-abelian simple groups. We conclude this section with a reduction to primitive simple groups.

**Proposition 3.5.** *Suppose that Theorem 1.3 holds true for primitive simple groups. Then Theorem 1.3 holds true.*

*Proof.* In view of Proposition 3.3, we may suppose that $G$ is primitive. Moreover, in view of Lemma 3.4, we may suppose that $G$ is of AS or PA type.

Let $\Omega$ be the domain of $G$. Then $\Omega$ admits a Cartesian decomposition $\Delta^\kappa$, for some $\kappa \geq 1$[n] and $G$ embeds into the wreath product $H\mathrm{wr}\mathrm{Sym}(\kappa)$ endowed with the primitive product action. Replacing $\mathrm{Sym}(\kappa)$ by a suitable transitive subgroup $A$, we may suppose that $G$ embeds into the wreath product $H\mathrm{wr}A$ and $G$ projects surjectively to $A$. Moreover, $H$ is of type AS. Let $T$ be the socle of $H$. Then the socle of $G$ is $T^\kappa$. When $T = M_{11}$ and $|\Delta| = 12$, as we have mentioned in the introduction, Giudici [11] has shown that $G$ has no non-identity semiregular element and hence, for the rest of the argument, we may suppose that $T$ is not $M_{11}$ in its degree 12 action.

Observe that $T$ acts transitively on $\Delta$ because $H$ is primitive on $\Delta$, but $T$ is not necessarily primitive on $\Delta$. Let $\Sigma$ be a non-trivial system of imprimitivity for the action of $T$ on $\Delta$; by choosing the blocks of $\Sigma$ as large as possible, we may assume that $T$ acts primitively on $\Sigma$.

We now prove the first part of the statement of Theorem 1.3. Let $g : \mathbb{N} \to \mathbb{N}$ be a function witnessing that Theorem 1.3 holds for primitive simple groups. Without loss of generality we may suppose that $g(1) = 1$. Define $f : \mathbb{N} \to \mathbb{N}$ by

$$f(k) = \max\{g(\lfloor k^{1/\ell} \rfloor)!^\ell \mid \ell \in \mathbb{N}\}.$$

Observe that $f$ is well-defined because when $\ell \geq k$, we have $\lfloor k^{1/\ell} \rfloor = 1$ and hence $g(\lfloor k^{1/\ell} \rfloor)!^\ell = 1$. In particular,

$$f(k) = \max\{g(\lfloor k^{1/\ell} \rfloor)!^\ell \mid \ell \in \{1, \ldots, k\}\}.$$

Let $k \in \mathbb{N}$. By hypothesis, either $T$ in its action on $\Sigma$ has a semiregular subgroup $X$ of order at least $k^{1/\kappa}$, or $|\Sigma| \leq g(\lfloor k^{1/\kappa} \rfloor)$. Observe that $X$ is also semiregular for the action of $T$ on $\Delta$. Therefore, in the first case, $X^\kappa$ is a semiregular subgroup of $G$ of order at least $(k^{1/\kappa})^\kappa = k$. Assume then $|\Sigma| \leq g(\lfloor k^{1/\kappa} \rfloor)$. Thus $|\Delta| \leq |T| \leq |\Sigma|! \leq g(\lfloor k^{1/\kappa} \rfloor)!$ and $|\Omega| = |\Delta|^\kappa \leq g(\lfloor k^{1/\kappa} \rfloor)!^\kappa \leq f(k)$.

We now prove the second part of the statement of Theorem 1.3. Therefore, we suppose that $G$ has no semiregular subgroup of order at least 4. We use the notation established above. Assume first $\kappa = 1$, that is, $G$ is almost simple. Since we are assuming that Theorem 1.3 holds for simple primitive groups, we deduce that $T$ is isomorphic to $\mathrm{Alt}(5)$, $\mathrm{Alt}(6)$, $M_{11}$ or $\mathrm{PSU}_3(3)$. We have constructed with a computer the abstract group $G$ having socle $T$, we have determined all the primitive actions of these groups and we have verified the veracity of Theorem 1.3. Assume

---

[n]When $\kappa = 1$, $\Omega = \Delta$ and $G$ is of type AS, when $k \geq 2$, $G$ is of type PA.

next $\kappa \geq 2$. If $T$ has a semiregular subgroup of order at least 2, then $T^\kappa \leq G$ has a semiregular subgroup of order at least 4. An inspection on the cases arising in parts (2)–(5), we see that the only group not having a semiregular subgroup of order at least 2 is $T = M_{11}$ in its primitive action of degree 12, which we have already dealt with above. □

In view of Proposition 3.5, for the proof of Theorem 1.3 we may suppose that $G$ is simple and primitive.

## 4. Number theoretic results

We collect in this section some number theoretic results. Remarkably the proof of Theorem 1.3 relies on some deep number theoretic facts, most notably, a quantitative weak version of the *abc* conjecture due to Stewart and Tijdeman [35] for dealing with alternating groups, and an impressive theorem of Siegel [33] on the greatest prime factors of polynomials valuated at integers for dealing with simple groups of Lie type[o].

Given a prime number $p$ and a non-negative integer $x$, we let $x_p$ denote the remainder of $x$ in the division by $p$. We need the famous theorem of Sylvester on prime numbers[p], see for instance [10].

**Theorem 4.1.** *Let $\ell$ be a positive integer. Then the product of $\ell$ consecutive integers greater than $\ell$ is divisible by a prime $p$ greater than $\ell$.*

Let $q$ and $t$ be positive integers. Recall that a ***primitive prime divisor*** for the pair $(q, t)$ is a prime $p$ such that $p \mid q^t - 1$ and $p \nmid q^i - 1$, for all $1 \leq i < t$. Zsigmondy's theorem [38] shows that $q^t - 1$ admits a primitive prime divisor, except when $t = 2$ and $q = 2^m - 1$ is a Mersenne number, or when $(t, q) = (6, 2)$.

**Lemma 4.2.** *Let $m$ be a positive integer with $m \geq 5$ and let $\ell \in \{1, \ldots, m-1\}$. Suppose that, for every prime $p \geq 5$, $\ell_p \leq m_p$. Then either*

  *(1) $\ell \in \{1, m-1\}$ and $m = 2^a \cdot 3^b$, for some $a, b \in \mathbb{N}$, or*
  *(2) $m = 9$ and $\ell \in \{2, 7\}$.*

*Proof.* Suppose that $m$ and $\ell$ satisfy the property:

$$(\dagger) \quad \ell_p \leq m_p, \text{ for every prime } p \geq 5.$$

Now, consider $\ell' = m - \ell$ and let $p \geq 5$ be a prime number. By hypothesis $\ell_p \leq m_p$ and hence $m_p - \ell_p$ is the remainder of $\ell' = m - \ell$ in the division by $p$, that is, $\ell'_p = (m - \ell)_p = m_p - \ell_p \leq m_p$. This shows that, if the pair $(m, \ell)$ satisfies ($\dagger$), then so does $(m, \ell') = (m, m - \ell)$. Therefore, without loss of generality, replacing $\ell$ by $m - \ell$ if necessary, we may suppose that $\ell \leq m/2$.

Now consider the $\ell$ consecutive numbers

$$m, m-1, \ldots, m - \ell + 1.$$

As $m \geq 2\ell$, these numbers are greater than $\ell$ and hence, by Sylvester's theorem, there exists a prime

$$(7) \qquad\qquad\qquad\qquad p > \ell$$

---

dividing $m - i$, for some $i \in \{0, \ldots, \ell - 1\}$. As $i \leq \ell - 1$ and $p \mid m - i$, we have $m_p \leq i \leq \ell - 1$. However, as $p > \ell$, we have $\ell_p = \ell$ and hence we deduce $m_p < \ell_p$. Since $(m, \ell)$ satisfies (†), we have $p < 5$, that is, $p \in \{2, 3\}$.

Assume $\ell = 1$. If $m$ is divisible by a prime $p \geq 5$, then $\ell_p = 1 > m_p = 0$ and hence $(m, \ell)$ does not satisfy (†). Therefore $m = 2^a \cdot 3^b$, for some $a, b \in \mathbb{N}$, and we obtain part (1).

Assume $\ell \geq 2$. From (7), we have $p > \ell \geq 2$. As $p \in \{2, 3\}$, we deduce $p = 3$ and, more importantly, $\ell = 2$. For each prime divisor $r \geq 5$ of $m - 1$ or $m$, we have $m_r \leq 1$ and hence $\ell_r \leq m_r \leq 1$, because $(m, \ell)$ satisfies (†). As $\ell = 2$, the condition $\ell_r \leq 1$ can only be satisfied if and only if $m - 1$ and $m$ are only divisible by the primes 2 and 3. Thus

$$m = 2^a \cdot 3^b \text{ and } m - 1 = 2^{a'} \cdot 3^{b'},$$

for some $a, a', b, b' \in \mathbb{N}$. Since

$$1 = \gcd(m, m - 1) = \gcd(2^a \cdot 3^a, 2^{a'} \cdot 3^{b'}) = 2^{\min(a, a')} \cdot 3^{\min(b, b')},$$

we obtain

- $m = 2^a$ and $m - 1 = 3^{b'}$, or
- $m = 3^b$ and $m - 1 = 2^{a'}$.

We deal with each of these two cases in turn. Assume $m = 2^a$ and $m - 1 = 3^{b'}$. As $m \geq 5$, 3 divides $m - 1 = 2^a - 1$ and hence $a$ is even. Thus $a = 2\alpha$ for some integer $\alpha$. This gives $2^a - 1 = 4^\alpha - 1 = 3^{b'}$. In particular, since 3 divides $4^1 - 1$, $4^\alpha - 1$ has no primitive prime divisors. Using the theorem of Zsigmondy [38], we deduce that this case is impossible unless $m = 4$. However, this contradicts our hypothesis $m \geq 5$. Assume $m = 3^b$ and $m - 1 = 2^{a'}$. Thus $3^b - 1 = 2^{a'}$. In particular, since 2 divides $3^1 - 1$, $3^b - 1$ has no primitive prime divisors. Using the theorem of Zsigmondy [38], we deduce that $b \in \{1, 2\}$. When $b = 1$, $m = 3$ and we contradict our hypothesis $m \geq 5$. When $b = 2$, $m = 9$ and we obtain the exceptional case in (2). □

**Lemma 4.3.** *Let $m$ be a positive integer. If $m \geq 8$, then there exists a prime $p$ with $m/2 < p \leq m - 3$.*

*Proof.* Bertrand's postulate [16, page 498] says that, when $n \geq 4$, there is a prime $p$ satisfying $n < p < 2n - 2$.

In particular, when $m$ even, the proof follows by applying Bertrand's postulate with $n = m/2$. Whereas, when $m$ is odd, the proof follows by applying Bertrand's postulate with $n = (m - 1)/2$. □

**Lemma 4.4.** *Let $m$ be a positive integer. Then $(m/2)^m \geq m!/2$.*

*Proof.* This follows from an inductive argument on $m$. □

The **radical** $\mathrm{rad}(m)$ of a positive integer $m$ is the product of the distinct prime numbers dividing $m$, that is,

$$\mathrm{rad}(m) = \prod_{\substack{p \mid m \\ p \text{ prime}}} p.$$

For instance, $\mathrm{rad}(24) = 2 \cdot 3 = 6$. In our work, we need the following weak form of the abc conjecture, see [35].

**Theorem 4.5.** *There exists a positive constant $\kappa$ such that, if $a$, $b$ and $c$ are coprime positive integers with $c = a + b$, then $c \leq \exp(\kappa \cdot \mathrm{rad}(abc)^{15})$.*

Following [33], given a positive integer $n$, we denote by $P[n]$ the ***greatest prime factor*** of the integer $n$. As customary, we denote with $\Phi_n(x) \in \mathbb{Z}[x]$ the $n^{\mathrm{th}}$ cyclotomic polynomial, that is,

$$\Phi_n(x) = \prod_{\substack{\zeta \text{ primitive } n^{\mathrm{th}} \\ \text{root of unity}}} x - \zeta.$$

**Lemma 4.6.** *Given $n \in \mathbb{N}$ with $n \geq 3$ and $q \in \mathbb{N}$ with $q \geq 2$, there exist two positive constants $c$ and $c'$ depending on $n$ only such that $q^n - 1$ admits a primitive prime divisor $p \geq c \log \log q$ for every $q \geq c'$.*

*Proof.* This follows from a remarkable result of Siegel [33, Satz 7]: Let $f \in \mathbb{Z}[x]$ be a polynomial with integer coefficients and at least 2 distinct roots. Then there exist two positive constants $c_f$ and $c'_f$ depending on $f$ only such that $P[f(q)] \geq c_f \log \log q$, $\forall q \in \mathbb{N}$ with $q \geq c'_f$.

As $n \geq 3$, $\Phi_n(x)$ has $\varphi(n) \geq 2$ distinct roots and hence we may apply Siegel's theorem with $f(x) = \Phi_n(x)$. In particular, there exist two positive constants $c$ and $c'$ depending on $n$ only such that $P[\Phi_n(q)] \geq c \log \log q$, for every integer $q$ with $q \geq c'$. Replacing $c'$ by a larger constant, we may also suppose that $P[\Phi_n(q)] \geq n+1$, for every integer $q \geq c'$. Let $q \in \mathbb{N}$ with $q \geq c'$ and let $p = P[\Phi_n(q)]$.

Following [12, Definition 1], we let $\Phi_n^*(q)$ denote the largest divisor of $\Phi_n(q)$ relatively prime to

$$\prod_{i=1}^{n-1} q^i - 1.$$

Let $r$ be the largest prime divisor of $n$. From [12, Lemma 3.1], we have

$$\Phi_n^*(q) = \begin{cases} \Phi_n(q) & \text{if } r \text{ does not divide } \Phi_n(q), \\ \Phi_n(q)/r & \text{if } r \text{ divides } \Phi_n(q). \end{cases}$$

Since $p > n \geq r$, we deduce that $p$ divides $\Phi_n^*(q)$ and hence, by definition, $p$ is a primitive prime divisor of $q^n - 1$. $\qquad\square$

## 5. Alternating groups and Sporadic groups

In this section we prove Theorem 1.3 when $G = \mathrm{Alt}(m)$ is an alternating group of degree $m \geq 5$ and when $G$ is a sporadic simple group.

We start by dealing with the alternating group $G = \mathrm{Alt}(m)$ with $m \geq 5$. Let $\Omega$ be a $G$-set with $G$ acting faithfully and transitively on $\Omega$ and let $\omega \in \Omega$. As the point stabilizer $G_\omega$ is a subgroup of $G = \mathrm{Alt}(m)$, we deduce that $G_\omega$ acts on the set $\{1, \ldots, m\}$. Now, we consider three cases, depending on whether $G_\omega$ in its action on $\{1, \ldots, m\}$ is intransitive, imprimitive (that is, transitive but not primitive), or primitive. As usual, we let $n = |\Omega|$.

**Lemma 5.1.** *There exists a function $f : \mathbb{N} \to \mathbb{N}$ such that, if $G_\omega$ is intransitive on $\{1, \ldots, m\}$, then either $G$ in its action on $\Omega$ has a semiregular subgroup of order at least $k$ or $n \leq f(k)$. Moreover, either $G$ in its action on $\Omega$ has a semiregular subgroup of order at least 4, or $m = |\Omega| = 6$.*

*Proof.* Let $\kappa$ be the absolute constant arising in Theorem 4.5 and let $f : \mathbb{N} \to \mathbb{N}$ be defined by

$$f(k) = \max\{2k, (\exp(\kappa \cdot (k-1)^{15(k-1)}))^k\}.$$

As $G_\omega$ is intransitive on $\{1, \ldots, m\}$, $G_\omega$ fixes setwise a subset $L$ of $\{1, \ldots, m\}$ having cardinality $\ell$, for some positive integer $\ell$ with $1 \le \ell \le m/2$. Thus $G_\omega \le G \cap (\mathrm{Sym}(L) \times \mathrm{Sym}(\{1, \ldots, m\} \setminus L))$. As $G$ is primitive on $\Omega$, we deduce $G_\omega = G \cap (\mathrm{Sym}(L) \times \mathrm{Sym}(\{1, \ldots, m\} \setminus L))$. Hence we may identify $\Omega$ with the set of $\ell$-subsets of $\{1, \ldots, m\}$ and we may identify the action of $G$ on $\Omega$ with the natural action of $\mathrm{Alt}(m)$ on $\ell$-subsets.

Assume first $\ell = 1$. In this case, $n = m$ and the action of $G$ on $\Omega$ is the natural action of the alternating group $\mathrm{Alt}(m)$ of degree $m$. In particular, $G$ in its action on $\Omega$ has a semiregular subgroup of order $m$ when $m$ is odd, and of order $m/2$ when $m$ is even. Thus, when $m/2 \ge k$ we can guarantee the existence of a semiregular subgroup of sufficiently large cardinality and, when $m/2 < k$, we have $n = m \le f(k)$. For the rest of the argument, we may assume $\ell \ge 2$.

Suppose

(†)  there exists a prime divisor $p$ of $m(m-1)\cdots(m-\ell+1)$ with $p \ge \max(k, \ell+1)$.

As $p$ is prime, there exists $i \in \{0, ..., \ell-1\}$ with $p \mid m - i$. As $i \le \ell - 1 < p$, we have

$$m_p = i \le \ell - 1.$$

Let $x \in \mathrm{Alt}(m) = G$ be a permutation having (in its action on $\{1, \ldots, m\}$) $m_p$ fixed points and $(m - m_p)/p$ disjoint cycles of length $p$. We claim that $X = \langle x \rangle$ is a semiregular subgroup of $G$ in its action on $\Omega$. Indeed, as $X$ has prime order $p$, as $p > \ell$ and $m_p < \ell$, no non-identity element of $X$ fixes setwise any $\ell$-subset. This shows that, when (†) holds, $G$ in its action on $\Omega$ has a semiregular subgroup of order at least $p \ge k$.

Assume $k \le \ell + 1$. As $\ell \le m/2$, by Theorem 4.1, there exists a prime divisor $p$ of $m(m-1)\cdots(m-\ell+1)$ with $p > \ell$. Thus $p \ge \ell + 1 \ge k$ and hence $p \ge \max(k, \ell+1)$. Therefore, in this case, (†) is satisfied.

Assume $k \ge \ell + 2$. Suppose there exists a prime divisor $p$ of $m(m-1)\cdots(m-\ell+1)$ with $p \ge k$. Since $p \ge k \ge \ell + 2$, (†) is satisfied. Finally suppose that there exists no prime divisor $p$ of $m(m-1)\cdots(m-\ell+1)$ with $p \ge k$. In particular, as $\ell \ge 2$, all primes dividing $m(m-1)$ are smaller than $k$. Since the number of primes less than $k$ is at most $k - 1$, we deduce

$$\mathrm{rad}(m(m-1)) \le \prod_{\substack{p \text{ prime} \\ p \le k-1}} p \le (k-1)^{k-1}.$$

Using Theorem 4.5 with $a = 1$, $b = m - 1$ and $c = m$, we get

$$m \le \exp(\kappa \cdot (k-1)^{15(k-1)}).$$

Thus

$$n = |\Omega| = \binom{m}{\ell} \le m^\ell \le m^k \le (\exp(\kappa \cdot (k-1)^{15(k-1)}))^k \le f(k).$$

To conclude the proof, we need to discuss the existence of semiregular subgroups of order at least $k = 4$. If (†) is satisfied with $k = 4$, then we have semiregular subgroups of order at least 5. Notice that, when $\ell \ge 3$, Theorem 4.1 guarantees

that (†) is satisfied with $k = 4$. Indeed, there exists a prime divisor of $m(m-1)\cdots(m-\ell+1)$ with $p \geq \ell+1$. As $p$ is prime, when $\ell \geq 3$, we have $p \geq 4$ and hence $p \geq 5$. Therefore, we may suppose that $\ell \leq 2$. When $\ell = 1$, $G$ has a semiregular subgroup of order $m/2$ if $m$ is even and $m$ if $m$ is odd. These values are less than 4 only when $m = 6$; therefore, we obtain the exceptional case listed in the statement of the lemma. Finally assume $\ell = 2$ and suppose that (†) is not satisfied with $k = 4$. Notice that, for every prime divisor $p \geq 5$, we have $2 = \ell_p \leq m_p$. Then by Lemma 4.2 we get $m = 9$ and $\ell = 2$. When $m = 9$ and $\ell = 2$, observe that a cyclic subgroup of $\mathrm{Alt}(9)$ of order 9 acts semiregularly on the 2-subsets of $\{1,\ldots,9\}$. $\qquad\square$

**Lemma 5.2.** *Suppose that $G_\omega$ is imprimitive on $\{1,\ldots,m\}$. Then $G$ in its action on $\Omega$ has a semiregular subgroup of order $k$ with $n \leq k^{2k}$. Moreover, $G$ in its action on $\Omega$ has a semiregular subgroup of order at least $4$.*

*Proof.* As $G_\omega$ is imprimitive on $\{1,\ldots,m\}$, $G_\omega$ admits a non-trivial system of imprimitivity with $a$ blocks of cardinality $b$, for some positive integers $a$ and $b$ with $1 < a, b < m$ and $m = ab$. Therefore, $G_\omega$ embeds into the imprimitive wreath product $\mathrm{Sym}(b)\mathrm{wr}\mathrm{Sym}(a)$.

From Lemma 4.3, there exists a prime $p$ with $m/2 < p \leq m$. In particular, $p$ is relatively prime to $|G_\omega|$, because $p$ does not divide $b!^a a!$. Therefore, a cyclic subgroup of order $p$ of $G = \mathrm{Alt}(m)$ acts semiregularly on $\Omega$. From Lemma 4.4, we have $p^{2p} \geq m!/2 = |G| \geq |\Omega| = n$. Observe that $p \geq 5$ and hence $G$ contains a semiregular subgroup of order at least 4. $\qquad\square$

**Lemma 5.3.** *Suppose that $G_\omega$ is primitive on $\{1,\ldots,m\}$. Then $G$ in its action on $\Omega$ has a semiregular subgroup of order $k$ with $n \leq k^{2k}$. Moreover, $G$ in its action on $\Omega$ has a semiregular subgroup of order at least $4$ unless one of the following holds*

  *(1) $m = 5$ and $|G_\omega| = 10$,*
  *(2) $m = 6$ and $|G_\omega| = 60$.*

*Proof.* Assume $m \geq 8$. From Lemma 4.3, there exists a prime $p$ with $m/2 < p \leq m-3$. If $p$ divides $|G_\omega|$, then $G_\omega$ contains a cycle of length $p$ in its action on $\{1,\ldots,m\}$. From a classical result of Jordan [7, Theorem 3.3E], we deduce $G_\omega \geq \mathrm{Alt}(m)$, which contradicts the fact that $G$ acts faithfully on $\Omega$. Therefore, $p$ is relatively prime to $|G_\omega|$. In particular, a cyclic subgroup of order $p$ of $G = \mathrm{Alt}(m)$ acts semiregularly on $\Omega$. From Lemma 4.4, we have $p^{2p} \geq m!/2 = |G| \geq |\Omega| = n$. Observe also that $p \geq 5$ and hence $G$ contains a semiregular subgroup of order at least 4.

Assume now $m < 8$. Here the proof follows from a computer computation with the invaluable help of the computer algebra system `magma` [2]. $\qquad\square$

**Corollary 5.4.** *There exists a function $f : \mathbb{N} \to \mathbb{N}$ such that, if $k$ is a positive integer and $G$ is an alternating group $\mathrm{Alt}(m)$ with $m \geq 5$ acting faithfully and transitively on a set of cardinality $n$, then either $G$ has a semiregular subgroup of order at least $k$, or $n \leq f(k)$. Moreover, $G$ has a semiregular subgroup of order at least $4$ unless one of the following holds*

  *(1) $m = 5$, $G_\omega$ is primitive on $\{1,\ldots,m\}$ and $|G_\omega| = 10$,*
  *(2) $m = 6$, $G_\omega$ is primitive on $\{1,\ldots,m\}$ and $|G_\omega| = 60$.*

*Proof.* Let $G = \mathrm{Alt}(m)$, let $\Omega$ be the domain of $G$ and let $\omega \in \Omega$. When $G_\omega$ is intransitive on $\{1, \ldots, m\}$ the result follows from Lemma 5.1, when $G_\omega$ is imprimitive on $\{1, \ldots, m\}$ the result follows from Lemma 5.2 and when $G_\omega$ is primitive on $\{1, \ldots, m\}$ the result follows from Lemma 5.3. $\qquad\square$

We conclude this section by dealing with the sporadic simple groups.

**Lemma 5.5.** *Let $G$ be a sporadic simple group acting faithfully and transitively on a set of cardinality $n$. Then either $G$ has a semiregular subgroup of order $k$ with $k^{2k} \geq n$, or $G = M_{11}$ and $n = 12$. Moreover, $G$ has a semiregular subgroup of order at least 4 unless $G = M_{11}$ and $n = 12$.*

*Proof.* Let $\omega$ be a point in the domain $\Omega$ of $G$ and let $G_\omega$ be the stabilizer of $\omega$.

Let $p_1$ and $p_2$ be the two largest prime divisors of the order of $G$ with $p_2 < p_1$. Using the order of the sporadic simple groups [6], we have $p_2 > 4$ and $p_1^{2p_1} > p_2^{2p_2} \geq |G| \geq |\Omega| = n$. In particular, if $G_\omega$ is relatively prime to $p_1$ or to $p_2$, then the lemma follows immediately. Therefore, we may suppose that $p_1 p_2$ divides $|G_\omega|$.

Suppose that $G$ is not the Monster. Let $M$ be a maximal subgroup of $G$ with $G_\omega \leq M$. Using the information on [6], we see that the order of $M$ is divisible by $p_1 p_2$ only in one of the following cases:

- $G = Co_2$ and $M \cong M_{23}$,
- $G = Co_3$ and $M \cong M_{23}$,
- $G = McL$ and $M \cong M_{22}$,
- $G = HS$ and $M \cong M_{22}$,
- $G = M_{24}$ and $M \cong M_{23}$ or $M \cong \mathrm{PSL}_2(23)$,
- $G = M_{23}$ and $M \cong 23 : 11$,
- $G = M_{12}$ and $M \cong M_{11}$ or $M \cong \mathrm{PSL}_2(11)$,
- $G = M_{11}$ and $M \cong \mathrm{PSL}_2(11)$.

Except when $G = M_{11}$, for each of these cases, we have constructed with the help of a computer the permutation representation of $G$ on the cosets of $M$ and we have found a semiregular subgroup of order $k \geq 4$ with $k^{2k} \geq |G|$.

The group $G = M_{11}$ in its action on degree 12 (on the right cosets of $\mathrm{PSL}_2(11)$) has no non-identity semiregular subgroups.[q] In particular, we obtain the exception listed in the statement of this lemma.

Finally, suppose $G$ is the Monster group $\mathbb{M}$.[r] Here, $p_1 = 71$ and $p_2 = 59$. From [36, Section 3.6] and [37], we see that the classification, up to isomorphism and up to conjugacy, of the maximal subgroups of $G$ is complete except for a few open cases. In particular, if $M$ is a maximal subgroup of $\mathbb{M}$, then either $M$ is in [36, Section 3.6], or the socle of $M$ is $\mathrm{PSL}_2(13)$ or $\mathrm{PSL}_2(16)$. Therefore, from this list, we deduce that $G$ has no maximal subgroup whose order is divisible by $p_2 p_1 = 59 \cdot 71$. $\qquad\square$

## 6. SIMPLE GROUPS OF LIE TYPE

Given a positive integer $x$, we let $\pi(x)$ denote the set of prime divisors of $x$. Moreover, given a finite group $G$, we let $\pi(G)$ denote the set of prime divisors of the order of $G$. For instance, when $G = \mathrm{Alt}(5)$, we have $\pi(G) = \{2, 3, 5\}$.

---

[q]This fact was first proved by Giudici [11].
[r]It has been recently announced a complete classification of the maximal subgroups of the Monster, see [15].

In this section we prove Theorem 1.3 when $G$ is a simple groups of Lie type. Our main tool, besides the number theoretic results in Section 4, is a result of Liebeck, Praeger and Saxl [24, Theorem 4].[s] We phrase it tailored to our current needs.

**Theorem 6.1.** *Let $T$ be a simple group of Lie type and let $M$ be a proper subgroup of $T$. Suppose that $|M|$ is divisible by each of the primes or prime powers indicated in the second or third column in* [24, Tables 10.1–10.5]. *Then the possibilities for $M$ are as given* [24, Tables 10.1–10.5].

For the rest of this section, we let $T$ be a simple group of Lie type acting primitively and faithfully on a set $\Omega$ and let $\omega \in \Omega$. We apply Theorem 6.1 with $M = T_\omega$. In particular, our proof of Theorem 1.3 for the action of $T$ on $\Omega$ splits into two major cases:

Case 1: $|T_\omega|$ is not divisible by some prime power indicated in the second or third column in Tables 10.1–10.5 of [24],

Case 2: $|T_\omega|$ is divisible by each prime power indicated in the second and third column in Tables 10.1–10.5 of [24].

In reading Tables 10.1–10.5 in [24], we are only concerned in the case that $M$ is a maximal subgroup of $T$, because $M = T_\omega$ and $T$ is primitive on $\Omega$. Moreover, we are only interested in *simple* Lie groups (see Proposition 3.3) and hence in these tables we are not concerned with groups that are not simple.

In Case 1, the number theoretic results in Section 4 will show that $|T_\omega|$ is not divisible by a large prime, which yields a large semiregular subgroup for the action of $T$ on $\Omega$. Case 2 requires a detailed analysis on the pairs $(T, M)$ arising in Tables 10.1–10.5 of [24].

Since we are aiming to determine the innately transitive groups with no semiregular subgroups of order at least 4, both cases require special care. Therefore, in order to avoid cumbersome arguments, we deal with this special case with an ad-hoc argument in Section 6.2.

Before embarking into these proofs, we make another observation again tailored to our needs. One remarkable application of [24, Theorem 4] is a classification of all pairs $(T, M)$, where $T$ is a simple group of Lie type and $M$ is a proper subgroup of $T$ with $\pi(T) = \pi(M)$. All of these pairs are reported in [24, Table 10.7]. Here, we report in Table 1 lines 3, 4, 5 and 6 of [24, Table 10.7], because these play a special role in our arguments for dealing with Case 2.

**Lemma 6.2.** *Let $T = \mathrm{PSp}_{2m}(q)'$ be acting primitively and faithfully on a set $\Omega$ and let $\omega \in \Omega$.[t] Assume that $T$ and $T_\omega$ are as in the first line of Table 1. Then $T$ contains a semiregular subgroup of order at least $m \log_2 q + 1$.*

*Moreover, $T$ in its action on $\Omega$ has a semiregular subgroup of order at least 4, unless $(m, q) = (2, 2)$.*

*Proof.* We deal with the case $(m, q) = (2, 2)$ separately. Indeed, we have verified the veracity of the statement with `magma` [2]. For the rest of the proof, we suppose $(m, q) \neq (2, 2)$ and hence $T = \mathrm{PSp}_{2m}(q)$.

---

[s]This result has already played an important role in other investigations on group actions on graphs. In particular, it is one of the ingredients for the proof of the Babai-Godsil conjecture on the asymptotic enumeration of Cayley digraphs [26].

[t]Observe that $T$ is defined as the derived subgroup of $\mathrm{PSp}_{2m}(q)$, for including the case $(m, q) = (2, 2)$, where $\mathrm{PSp}_4(2) \cong \mathrm{Sym}(6)$.

| Line | $T$ | $M$ | Remarks |
|---|---|---|---|
| 1 | $\mathrm{PSp}_{2m}(q)'$ | $\Omega_{2m}^-(q) \trianglelefteq M$ | $m$ and $q$ even |
|  |  |  | $\mathbf{N}_T(\Omega_{2m}^-(q))$ in the Aschbacher class $\mathcal{C}_8$ |
| 2 | $\mathrm{P}\Omega_{2m+1}(q)$ | $\Omega_{2m}^-(q) \trianglelefteq M$ | $m$ even and $q$ odd |
|  |  |  | $\mathbf{N}_T(\Omega_{2m}^-(q))$ in the Aschbacher class $\mathcal{C}_1$ |
| 3 | $\mathrm{P}\Omega_{2m}^+(q)$ | $\Omega_{2m-1}(q) \trianglelefteq M$ | $m$ even |
|  |  |  | $\mathbf{N}_T(\Omega_{2m-1}(q))$ in the Aschbacher class $\mathcal{C}_1$ |
| 4 | $\mathrm{PSp}_4(q)'$ | $\mathrm{PSp}_2(q^2) \trianglelefteq M$ | $\mathbf{N}_T(\mathrm{PSp}_2(q^2))$ in the Aschbacher class $\mathcal{C}_3$ |

TABLE 1. Lines 3, 4, 5 and 6 of [24, Table 10.7]

As $q$ is even, we have $T = \mathrm{Sp}_{2m}(q)$. Since $T_\omega$ is maximal in $T$,

$$T_\omega = \mathbf{N}_T(\Omega_{2m}^-(q)) = \mathrm{SO}_{2m}^-(q) = \Omega_{2m}^-(q).2.$$

Let $q = 2^f$, for some positive integer $f$. Fixing a suitable basis of the $\mathbb{F}_q$-vector space $V = \mathbb{F}_q^{2m}$, we may suppose that the symplectic form $\varphi$ preserved by $T$ has matrix

$$\begin{pmatrix} 0 & I \\ I & 0 \end{pmatrix},$$

where $I$ is the $m \times m$-identity matrix. Suppose that $2^{fm} - 1$ admits a primitive prime divisor and let $p$ be the largest such prime divisor. Let $A \in \mathrm{GL}_m(q)$ be an element having order $p$ and let

$$g = \begin{pmatrix} A & 0 \\ 0 & (A^{-1})^T \end{pmatrix}.$$

An easy computation shows that $g$ preserves $\varphi$ and hence $g \in \mathrm{Sp}_{2m}(q) = T$. Every non-identity element of $X = \langle g \rangle$ fixes only two distinct non-trivial subspaces of $V$, namely, $V_1 = \langle e_1, \ldots, e_m \rangle$ and $V_2 = \langle e_{m+1}, \ldots, e_{2m} \rangle$, where $e_1, \ldots, e_{2m}$ is the canonical basis of $V = \mathbb{F}_q^{2m}$.

Assume, by contradiction, that $X$ has a $T$-conjugate in $T_\omega = \mathrm{SO}_{2m}^-(q)$. Replacing $T_\omega$ by a suitable $T$-conjugate, we may suppose that $X \le T_\omega$. Let $Q$ be the quadratic form preserved by $T_\omega$. Since $X$ acts irreducibly on $V_1$ and on $V_2$ and since $X$ preserves $Q$, we deduce that either $V_i$ is totally singular for $Q$ or $V_i$ is non-degenerate for $Q$. Since $Q$ has Witt defect 1 and since $\dim_{\mathbb{F}_q}(V_i) = m$, we deduce that $V_i$ is non-degenerate and hence the quadratic form $Q$ restricted to $V_i$ induces a non-degenerate quadratic form $Q_i$. As $X$ acts irreducibly on $V_i$ and as $X$ preserves $Q_i$, we deduce from [17] that $Q_i$ has Witt defect 1.[u] As $Q = Q_1 \oplus Q_2$ and as $Q_1, Q_2$ have both Witt defect 1, we deduce that $Q$ has Witt defect 0, which is a contradiction. This contradiction has shown that no $T$-conjugate of $X$ lies in $T_\omega$ and hence $X$ acts semiregularly on $\Omega$. Since $|X| = p \ge fm + 1 = m \log_2 q + 1$, the first part of the lemma follows in this case.

Suppose that $2^{fm} - 1$ does not admit a primitive prime divisor. From [38], this implies $(f, m) \in \{(1, 2), (3, 2), (1, 6)\}$. We have computed with a computer the size of semiregular subgroups in these cases and in each case there is a semiregular subgroup of order at least $m \log_2 q + 1$.

---

[u]From [17], the group $\mathrm{SO}_m^+(q)$ does not contain elements acting irreducibly on the underlying vector space.

It remains to discuss the existence of semiregular subgroups of order at least 4. When $4 \leq m \log_2 q + 1$, this follows from the first part of the lemma. If $m \log_2 q + 1 \leq 3$, then $(m, q) = (2, 2)$. □

**Lemma 6.3.** *Let* $T = \mathrm{P}\Omega_{2m+1}(q)$ *be acting primitively and faithfully on a set* $\Omega$ *and let* $\omega \in \Omega$*. Assume that* $T$ *and* $T_\omega$ *are as in the second line of Table* 1*. Then* $T$ *contains a semiregular subgroup of order at least* $(q^{m/2} + 1)/4$ *when* $q \equiv 3 \pmod 4$ *and* $m/2$ *is odd, and of order at least* $(q^{m/2} + 1)/2$ *in all other cases.*

*Moreover,* $T$ *in its action on* $\Omega$ *has a semiregular subgroup of order at least* 4*.*

*Proof.* Clearly, $T = \Omega_{2m+1}(q)$, because $\Omega_{2m+1}(q)$ is centerless. Here $T_\omega$ is the stabilizer of a non-singular 1-dimensional subspace $\langle v \rangle$ of $V = \mathbb{F}_q^{2m+1}$ such that the non-degenerate orthogonal form $Q$ for $T = \mathrm{P}\Omega_{2m+1}(q) = \Omega_{2m+1}(q)$ restricted to $\langle v \rangle^\perp$ has Witt defect 1. Let $w \in V \setminus \{0\}$ such that the quadratic form $Q$ restricted to $\langle w \rangle^\perp$ has Witt defect 0. Thus the orthogonal decomposition $V = \langle w \rangle \perp \langle w \rangle^\perp$ gives rise to an embedding of $\Omega_1(q) \times \Omega_{2m}^+(q) = \Omega_{2m}^+(q)$ in $\Omega_{2m+1}(q) = T$. The vector space $W = \langle w \rangle^\perp$ is endowed with the non-degenerate quadratic form $Q_{|W}$ having Witt defect zero and hence $W$ admits a direct sum decomposition

$$W = W_1 \oplus W_2,$$

where $\dim_{\mathbb{F}_q}(W_i) = m$ and the quadratic form $Q_{|W}$ restricted to $W_i$ has Witt defect 1. Using this orthogonal decomposition, we deduce the embedding $\Omega_m^-(q) \times \Omega_m^-(q) \leq \Omega_{2m}^+(q)$. By [17], $\Omega_m^-(q)$ contains a cyclic subgroup of order $(q^{m/2} + 1)/2$ acting as a scalar in $\mathbb{F}_{q^m}$, when the $\mathbb{F}_q$-vector space $W_i \cong \mathbb{F}_q^m$ is identified with the additive group of the field $\mathbb{F}_{q^m}$. Let $x_i$ be a generator of this cyclic subgroup. Let

$$\ell \in \left\{ 0, \ldots, \frac{q^{m/2} + 1}{2} - 1 \right\}$$

be a divisor of $(q^{m/2} + 1)/2$ and suppose that $x_i^\ell$ fixes a 1-dimensional subspace of $W_i$. Then $x_i^\ell$ has $m$ eigenvalues in $\mathbb{F}_q$ and hence

$$\frac{q^{m/2} + 1}{2\ell}$$

divides $q - 1$. Observe that

$$\gcd((q^{m/2} + 1)/2, q - 1) = \begin{cases} 2 & \text{when } q \equiv 3 \pmod 4 \text{ and } m/2 \text{ is odd,} \\ 1 & \text{otherwise.} \end{cases}$$

Moreover, when $q \equiv 3 \pmod 4$ and $m/2$ is odd, $x_i^{(q^{m/2}+1)/4}$ is the scalar matrix $-1$. Therefore $\langle x_i \rangle / \{1, -1\}$ acts semiregularly on the 1-dimensional subspaces of $W_i$ when $q \equiv 3 \pmod 4$ and $m/2$ is odd, and $\langle x_i \rangle$ acts semiregularly on the 1-dimensional subspaces of $W_i$ in all the remaining cases.

Let $g = x_1 \oplus x_2 \in \Omega_{2m}^+(q) \leq \Omega_{2m+1}(q)$ and let $X = \langle g \rangle$. Now, $X$ has order $(q^{m/2} + 1)/4$ when $q \equiv 3 \pmod 4$ and $m/2$ is odd, and $X$ has order $(q^{m/2} + 1)/2$ in all other cases. From the discussion above, we see that every non-identity element of $X$ fixes only the 1-dimensional subspace $\langle w \rangle$ and hence it is a derangement for the action on $\Omega$.

It remains to discuss the existence of semiregular subgroups of order at least 4. When $m \geq 4$, this follows from the first part of the proof. Suppose then $m = 2$. Let $\varepsilon = 2$ when $q \equiv 1 \pmod 4$ and $\varepsilon = 4$ when $q \equiv 3 \pmod 4$. Now, $(q+1)/\varepsilon \geq 4$

only when $q \notin \{3, 5, 7, 11\}$. Finally, when $m = 2$ and $q \in \{3, 5, 7, 11\}$, we may use a regular unipotent element of $\Omega_5(q)$ to obtain a semiregular subgroup of order 9 when $q = 3$ and of order $q$ when $q \in \{5, 7, 11\}$. $\qquad \square$

**Lemma 6.4.** *Let* $T = \mathrm{P}\Omega_{2m}^+(q)$ *be acting primitively and faithfully on a set* $\Omega$ *and let* $\omega \in \Omega$. *Assume that* $T$ *and* $T_\omega$ *are as in the third line of Table 1. Then* $T$ *contains a semiregular subgroup of order at least* $(q^{m/2} + 1)/4$ *when* $q \equiv 3 \pmod 4$ *and* $m/2$ *is odd, and of order at least* $(q^{m/2} + 1)/\gcd(2, q - 1)$ *in all other cases.*

*Moreover,* $T$ *in its action on* $\Omega$ *has a semiregular subgroup of order at least* 4.

*Proof.* Here $T_\omega = \mathbf{N}_T(\Omega_{2m-1}(q))$ and hence $T_\omega$ is the stabilizer of a non-singular 1-dimensional subspace $V = \mathbb{F}_q^{2m}$. Observe that when $q$ is even, $\Omega_{2m-1}(q) = \mathrm{Sp}_{2m-2}(q)$. Moreover, $m \geq 4$, because $\mathrm{P}\Omega_4^+(q) \cong \mathrm{PSL}_2(q) \times \mathrm{PSL}_2(q)$ is not simple.

The vector space $V$ is endowed with a non-degenerate quadratic form having Witt defect zero. Therefore, $V$ admits a direct sum decomposition

$$V = V_1 \oplus V_2,$$

where $\dim_{\mathbb{F}_q}(V_i) = m$ and the quadratic form restricted to $V_i$ has Witt defect 1. Using this orthogonal decomposition, we deduce the embedding $\Omega_m^-(q) \times \Omega_m^-(q) \leq \Omega_{2m}^+(q)$. Now, by [17], $\Omega_m^-(q)$ contains a cyclic subgroup of order

$$\frac{q^{m/2} + 1}{\gcd(2, q - 1)}$$

acting as a scalar in $\mathbb{F}_{q^m}$, when the $\mathbb{F}_q$-vector space $V_i \cong \mathbb{F}_q^m$ is identified with $\mathbb{F}_{q^m}$. (The argument here is similar to the proof of Lemma 6.3.) Let $x_i$ be a generator of this cyclic subgroup. Let $\ell \in \{0, \ldots, (q^{m/2} + 1)/\gcd(2, q - 1) - 1\}$ be a divisor of $(q^{m/2} + 1)/\gcd(2, q - 1)$ and suppose that $x_i^\ell$ fixes a 1-dimensional subspace of $V_i$. Then $x_i^\ell$ has $m$ eigenvalues in $\mathbb{F}_q$ and hence

$$\frac{q^{m/2} + 1}{\ell \gcd(2, q - 1)}$$

divides $q - 1$. Observe that

$$\gcd((q^{m/2} + 1)/\gcd(2, q - 1), q - 1) = \begin{cases} 2 & \text{when } q \equiv 3 \pmod 4 \text{ and } m/2 \text{ is odd,} \\ 1 & \text{otherwise.} \end{cases}$$

Moreover, when $q \equiv 3 \pmod 4$ and $m/2$ is odd, $x_i^{(q^{m/2}+1)/4}$ is the scalar matrix $-1$. Therefore $\langle x_i \rangle / \{1, -1\}$ acts semiregularly on the 1-dimensional subspaces of $V_i$ when $q \equiv 3 \pmod 4$ and $m/2$ is odd, and $\langle x_i \rangle$ acts semiregularly on the 1-dimensional subspaces of $V_i$ in all the remaining cases.

Let $\tilde{g} = x_1 \oplus x_2 \in \Omega_{2m}^+(q)$, let $g$ be the projective image of $\tilde{g}$ in $\mathrm{P}\Omega_{2m}^+(q)$ and let $X = \langle g \rangle$. Now, $X$ has order $(q^{m/2} + 1)/4$ when $q \equiv 3 \pmod 4$ and $m/2$ is odd, and $X$ has order $(q^{m/2} + 1)/\gcd(2, q - 1)$ in all other cases. From the discussion above, we see that every non-identity element of $X$ is a derangement for the action on the non-degenerate 1-dimensional subspaces of $V = \mathbb{F}_q^{2m}$.

It remains to discuss the existence of semiregular subgroups of order at least 4. As $m \geq 4$, this follows from the first part of the proof. $\qquad \square$

**Lemma 6.5.** *Let* $T = \mathrm{PSp}_4(q)'$ *be acting primitively and faithfully on a set* $\Omega$ *and let* $\omega \in \Omega$. *Assume that* $T$ *and* $T_\omega$ *are as in the fourth line of Table 1. Then* $T$

*contains a semiregular subgroup of order at least $q^2$ when $q$ is odd and of order at least $\log_2 q + 1$ when $q$ is even.*

*Moreover, $T$ in its action on $\Omega$ has a semiregular subgroup of order at least $4$, except when $q = 2$.*

*Proof.* Without loss of generality, we may suppose that the alternating form defining $T = \mathrm{PSp}_4(q)$ is

$$\begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{pmatrix}.$$

Suppose that $q$ is odd. The unipotent elements of $T_\omega$ lie in $\mathrm{PSp}_2(q^2)$ because $q$ is odd. Hence the non-identity unipotent elements of $T_\omega$ have two Jordan blocks of size 2, because $\mathrm{PSp}_2(q^2)$ preserves an extension field. Now, consider the subgroup $X$ of $T$ consisting of the matrices

$$\begin{pmatrix} 1 & 0 & a & b \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \forall a, b \in \mathbb{F}_q.$$

The non-identity elements of $X$ have two Jordan blocks of size 1 and one Jordan block of size 2. Therefore, except for the identity, none of the elements of $X$ is $T$-conjugate to an element of $T_\omega$. Therefore $X$ is a semiregular subgroup of order $q^2$.

Suppose that $q$ is even. Write $q = 2^f$, for some positive integer $f$. Thus $T = \mathrm{Sp}_4(q)$ and $\mathrm{Sp}_2(q^2) \trianglelefteq T_\omega = \mathrm{Sp}_2(q^2) : 2$. The elements of odd order of $T_\omega$ lie in $\mathrm{Sp}_2(q^2)$ and hence the elements of odd order of $T_\omega$ have either zero or two (with multiplicity two) eigenvalues in $\mathbb{F}_q$. Assume that $2^f - 1$ is divisible by a primitive prime divisor $p$ with $p \neq 3$. From [38], this implies $f \notin \{2, 6\}$. Clearly, $p \geq f + 1$. Let $\lambda \in \mathbb{F}_q^*$ having order $p$. Now, consider the subgroup $X$ of $T$ consisting of the matrices

$$\begin{pmatrix} a & 0 & 0 & 0 \\ 0 & a^2 & 0 & 0 \\ 0 & 0 & a^{-1} & 0 \\ 0 & 0 & 0 & a^{-2} \end{pmatrix}, \forall a \in \langle \lambda \rangle \subseteq \mathbb{F}_q^*.$$

As $p \neq 3$, the non-identity elements of $X$ have four distinct eigenvalues. Therefore, except for the identity, none of the elements of $X$ is $T$-conjugate to an element of $T_\omega$. Therefore $X$ is a semiregular subgroup of order $p \geq f + 1$. We have verified with a computer that, when $f \in \{2, 6\}$, the group $T = \mathrm{Sp}_4(q)$ admits a semiregular subgroup of order at least $f$.

It remains to discuss the existence of semiregular subgroups of order at least 4. When $q$ is odd this is clear because $q^2 \geq 4$. When $q$ is even and $\log_2 q + 1 \geq 4$, this is also clear. When $q$ is even and $\log_2 q + 1 \leq 3$, we have $q \in \{2, 4\}$. We have verified with a computer that when $q = 4$, $T$ in its action on $\Omega$ has a semiregular subgroup of order 15. □

6.1. **Semiregular subgroups of large order.** Recall that $T$ is a simple group of Lie type acting primitively and faithfully on a set $\Omega$ and $\omega \in \Omega$. Moreover, we apply Theorem 6.1 with $M = T_\omega$.

**Lemma 6.6.** *There exists a function $f : \mathbb{N} \to \mathbb{N}$ such that, if $T$ is a simple group of Lie type acting primitively and faithfully on a set $\Omega$, then either $T$ in its action on $\Omega$ has a semiregular subgroup of order at least $k$ or $|\Omega| \leq f(k)$.*

*Proof.* The proof follows easy with a careful inspection on Tables 10.1–10.5 in [24]. Here we use the notation from [24] and we give details only for a few cases, all other cases are dealt with similarly.

Suppose $T = \mathrm{PSL}_n(q)$. Assume $n \geq 6$ even and let $\Pi = \{q_n, q_{n-1}\}$. From [24, Table 10.1], we deduce that, with the exception of $T = \mathrm{PSL}_6(2)$, there exists no proper subgroup $M$ of $T$ with $|M|$ divisible by each prime in $\Pi$. Since we may exclude $\mathrm{PSL}_6(2)$ from this asymptotic result, we deduce that $|T_\omega|$ is not divisible by some prime $p$ in $\Pi$. In particular, $T$ has a semiregular subgroup of order at least $p$. By using Lemma 4.6, $p$ tends to infinity as $|T|$ tends to infinity. Assume $n \geq 5$ is odd and let $\Pi = \{q_n, q_{n-1}, q_{n-2}\}$. From [24, Table 10.1], we deduce that, with the exception of $T = \mathrm{PSL}_7(2)$, there exists no proper subgroup $M$ of $T$ with $|M|$ divisible by each prime in $\Pi$. In particular, we may argue as above for dealing with this case. The argument for $\mathrm{PSL}_2(q)$, $\mathrm{PSL}_3(q)$ and $\mathrm{PSL}_4(q)$ is entirely similar, using Table 10.3 in [24].

Suppose $T = \mathrm{PSp}_{2m}(q)'$. Assume $m \geq 3$ odd and let $\Pi = \{q_{2m-2}, q_{2m-2}, q_{2m}\}$. From [24, Table 10.1], we deduce that, with the exception of $T = \mathrm{PSp}_6(2)$, there exists no proper subgroup $M$ of $T$ with $|M|$ divisible by each prime in $\Pi$. Since we may exclude $\mathrm{PSp}_6(2)$ from this asymptotic result, we deduce that $|T_\omega|$ is not divisible by some prime $p$ in $\Pi$. In particular, $T$ has a semiregular subgroup of order at least $p$. By using Lemma 4.6, $p$ tends to infinity as $|T|$ tends to infinity. Assume $m \geq 4$ is even and let $\Pi = \{q_{2m}, q_{2m-2}, q_{2m-4}\}$. From [24, Table 10.1], we deduce that, with the exception of $T = \mathrm{PSp}_8(2)$, the only maximal with $|M|$ divisible by each prime in $\Pi$ satisfies $M = \mathbf{N}_T(\Omega_{2m}^-(q))$. In particular, if $T_\omega$ is not divisible by some prime in $\Pi$, then we deduce that $T$ has semiregular subgroups of large order from Lemma 4.6. Therefore, we just need to consider the action of $T = \mathrm{PSp}_{2m}(q)$ on the right cosets of $T_\omega = \mathbf{N}_T(\Omega_{2m}^-(q))$. Lemma 6.2 deals exactly with this action and indeed, it shows that $T$ contain semiregular subgroups having order that tends to infinity as $|T|$ tends to infinity. The argument for $\mathrm{PSp}_4(q)$ is similar and uses Table 10.3 in [24] and Lemma 6.5.

Suppose $T = \mathrm{P\Omega}_{2m+1}(q))$. Assume $m \geq 3$ odd and let $\Pi = \{q_{2m-2}, q_{2m-2}, q_{2m}\}$. From [24, Table 10.1], we deduce that there exists no proper subgroup $M$ of $T$ with $|M|$ divisible by each prime in $\Pi$. We deduce then that $|T_\omega|$ is not divisible by some prime $p$ in $\Pi$. In particular, $T$ has a semiregular subgroup of order at least $p$. By using Lemma 4.6, $p$ tends to infinity as $|T|$ tends to infinity. Assume $m \geq 4$ is even and let $\Pi = \{q_{2m}, q_{2m-2}, q_{2m-4}\}$. From [24, Table 10.1], we deduce that the only maximal with $|M|$ divisible by each prime in $\Pi$ satisfies $M = \mathbf{N}_T(\Omega_{2m}^-(q))$. In particular, if $T_\omega$ is not divisible by some prime in $\Pi$, then we deduce that $T$ has semiregular subgroups of large order from Lemma 4.6. Therefore, we just need to consider the action of $T = \mathrm{P\Omega}_{2m+1}(q)$ on the right cosets of $T_\omega = \mathbf{N}_T(\Omega_{2m}^-(q))$. Lemma 6.3 deals exactly with this action and indeed, it shows that $T$ contain semiregular subgroups having order that tends to infinity as $|T|$ tends to infinity.

The argument for all other Lie type groups is similar and it is omitted.      □

Observe that the result in our Section 6.1 can be seen as an asymptotic improvement of Corollary 6 in [24].

6.2. **Semiregular subgroups of order at least four.** We report here [24, Corollary 7]. Again, we only state it for our current needs.

**Lemma 6.7.** *Let $T$ be a simple group of Lie type and assume*

$$T \neq \mathrm{PSL}_2(8), \mathrm{PSL}_3(3), \mathrm{PSU}_3(3), \mathrm{PSp}_4(8), \ or \ \mathrm{PSL}_2(p)$$

*with $p$ a Mersenne prime. Then there is a collection $\Pi$ of prime numbers of $|T|$, such that for $M < T$, if $\Pi \subseteq \pi(M)$, then $\pi(T) = \pi(M)$ and $M$ is given in Table 10.7 in [24]. Moreover, every prime in $\Pi$ is at least 5, except in the following cases.*

| $T$ | $\Pi$ |
|---|---|
| $\mathrm{PSL}_2(p)$, $p$  prime, $p = 2^a 3^b - 1$, $b > 0$ | $\{3, p\}$ |
| $\mathrm{PSU}_4(2)$ | $\{3, 5\}$ |
| $\mathrm{PSU}_5(2)$ | $\{3, 5, 11\}$ |

**Lemma 6.8.** *Let $T$ be a simple group of Lie type acting primitively and faithfully on a set $\Omega$. Then either $T$ contains a semiregular subgroup of order at least 4, or one of the following holds*

*(1) $T \cong \mathrm{PSL}_2(4) \cong \mathrm{PSL}_2(5)$ and $|\Omega| = 6$,*
*(2) $T \cong \mathrm{PSL}_2(9)$ and $|\Omega| = 6$,*
*(3) $T \cong \mathrm{PSU}_3(3)$ and $|\Omega| = 36$.*

*Proof.* Let $\omega \in \Omega$ and set $M = T_\omega$.

Suppose first that $T$ is isomorphic to

$$\mathrm{PSL}_2(8), \mathrm{PSL}_3(3), \mathrm{PSU}_3(3), \mathrm{PSp}_4(8), \mathrm{PSU}_4(2), \mathrm{PSU}_5(2)$$

or to a group in [24, Table 10.7], except for the first seven rows. In this case, the proof follows with a computer computation with the algebra system `magma`. Indeed, in each of these cases, the group $T$ is small and the result can be verified with the auxiliary help of a computer by constructing with a case-by-case analysis the primitive permutation representations under consideration and by checking the existence of semiregular subgroups of order at least 4. Therefore, for the rest of the proof, we may suppose that $T$ is not isomorphic to any of these groups.[v]

Suppose $T = \mathrm{PSL}_2(p)$, with $p$ prime. If $\gcd(|M|, p) = 1$, then a Sylow $p$-subgroup of $T$ acts semiregularly on $\Omega$. Therefore, as $p \geq 4$ (because $p$ is prime), we deduce that $T$ has a semiregular subgroup of order at least 4. If $p$ divides $|M|$, then $M$ is a Borel subgroup of $T$ and the action of $T$ on $\Omega$ is permutation equivalent to the action of $T$ on the points of the projective line. Therefore, $T$ has a semiregular element of order $(p + 1)/2$. Now, $(p + 1)/2 \geq 4$, except when $p = 5$: this is the exception in (1). Therefore, for the rest of the proof, we may suppose that $T$ is not isomorphic to $\mathrm{PSL}_2(p)$, with $p$ prime.

We are now in the position to use Lemma 6.7. There exists a set $\Pi$ of three prime numbers, each at least 5, with the property that either $\Pi \nsubseteq \Pi(M)$, or $\Pi \subseteq \pi(M)$ and $(T, M)$ is one of the pairs in the first seven rows of Table 10.7 in [24]. In the first case we are done, because $T$ has a semiregular subgroup of order at least $5 \geq 4$. If $(T, M)$ are as in lines 3, 4, 5 and 6 of [24, Table 10.7], then the result follows from Lemmas 6.2–6.5. Therefore it remains to consider the lines 1, 2 and 7 of [24, Table 10.7]. In lines 1 and 2, the group $T$ is alternating and hence only $\mathrm{Alt}(5), \mathrm{Alt}(6), \mathrm{Alt}(8)$ are of interest here. A computation yields that only the

---

[v]Observe that the exceptional case (3) arises when analyzing these small groups.

examples in (1) and (2) have no semiregular subgroup of order at least 4. Finally, in line 7, we have $T = \mathrm{PSL}_2(p)$ with $p$ prime, which we have dealt with above. $\square$

## REFERENCES

[1] J. Bamberg, C. E. Praeger, Finite permutation groups with a transitive minimal normal subgroup, *Proc. London Math. Soc. (3)* **89** (2004), 71–103.

[2] W. Bosma, J. Cannon, C. Playoust, The Magma algebra system. I. The user language, *J. Symbolic Comput.* **24** (3-4) (1997), 235–265.

[3] J. N. Bray, D. F. Holt, C. M. Roney-Dougal, *The maximal subgroups of the low dimensional classical groups*, London Mathematical Society Lecture Note Series **407**, Cambridge University Press, Cambridge, 2013.

[4] D. Bubboloni, P. Spiga, Th. Weigel, *Normal 2-coverings of the finite simple groups and their generalizations*, Springer Lecture Notes in Mathematics, to appear.

[5] P. J. Cameron, C. Y. Ku, Intersecting families of permutations, *European J. Combin.* **24** (2003), 881–890.

[6] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, R. A. Wilson, An ATLAS of Finite Groups Clarendon Press, Oxford, 1985; reprinted with corrections 2003.

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

[8] P. Erdős, C. Ko, R. Rado, Intersection theorems for systems of finite sets, *The Quarterly Journal of Mathematics* **12** (1961), 313–320.

[9] P. Erdős, P. Pàlfy, M. Szegedy, $a \pmod{p} \le b \pmod{p}$ for all primes $p$ implies $a = b$, *Amer. Math. Monthly* **94** (1987), 169–170.

[10] D. Hanson, On a theorem of Sylvester and Schur, *Canadian Mathematical Bulletin* **16** (1973), 195–199.

[11] M. Giudici, Quasiprimitive groups with no fixed point free elements of prime order, *Journal of the London Mathematical Society* **67** (2003), 73–84.

[12] S. P. Glasby, F. Lübeck, A. Niemeyer, C. E. Praeger, Primitive prime divisors and the $n$-th cyclotomic polynomial, *J. Aust. Math. Soc.* **102** (2017), 122–135.

[13] C. Godsil, K. Meagher, *Erdős-Ko-Rado Theorems: Algebraic Approaches*, Cambridge studies in advanced mathematics **149**, Cambridge University Press, 2016.

[14] R. M. Guralnick, Zeros of permutation characters with applications to prime splitting and Brauer Groups, *J. Algebra* **131** (1990), 294–302.

[15] H. Dietrich, M. Lee, T. Popiel, The maximal subgroups of the Monster, arXiv:2304.14646.

[16] G. H. Hardy, E. M. Wright, *An introduction to the theory of numbers*, fifth edition, Oxford Science publications, Clarendon Press, Oxford, 1979.

[17] B. Huppert, Singer-Zyklen in Klassischen Gruppen, *Math. Z.* **117** (1970), 141–150.

[18] W. Jehne, Kronecker classes of algebraic number fields, *J. Number Theory* **9** (1977), 279–320.

[19] N. Klinghen, Zahlkörper mit gleicher Primzerlegung, *J. Reiner Angew. Math.* **299** (1978), 342–384.

[20] N. Klinghen, *Arithmetical Similarities, Prime decompositions and finite group theory*, Oxford Mathematical Monographs, Clarendon Press, Oxford, 1998.

[21] K. Meagher, A. S. Razafimahatratra, P. Spiga, On triangles in derangement graphs, *J. Comb. Theory Ser. A* **180** (2021), Paper No. 105390.

[22] B. Larose, C. Malvenuto, Stable sets of maximal size in Kneser-type graphs, *European J. Combin.* **25** (2004), 657–673.

[23] C. H. Li, S. J. Song, V. Raghu Tej Pantangi, Erdős-Ko-Rado problems for permutation groups, *arXiv preprint arXiv:2006.10339*, 2020.

[24] M. W. Liebeck, C. E. Praeger, J. Saxl, Transitive Subgroups of Primitive Permutation Groups, *J. Algebra* **234** (2000), 291–361.

[25] M. W. Liebeck, C. E. Praeger, J. Saxl, On the O'Nan-Scott theorem for finite primitive permutation groups, *J. Australian Math. Soc. (A)* **44** (1988), 389–396.

[26] J. Morris, P. Spiga, Asymptotic enumeration of Cayley digraphs, *Israel J. Math. 242* (2021), 401–459.

[27] P. M. Neumann, The concept of primitivity in group theory and the second memoir of Galois, *Arch. Hist. Exact Sci.* **60** (2006), 379–429.

[28] C. E. Praeger, Finite quasiprimitive graphs, in: *Surveys in Combinatorics*, London Math. Soc. Lecture Note Ser. 241, Cambridge University, Cambridge (1997), 65–85.

[29] C. E. Praeger, Covering subgroups of groups and Kronecker classes of fields, *J. Algebra* **118**,(1988) 455–463.

[30] C. E. Praeger, Kronecker classes of field extensions of small degree, *J. Austral. Math. Soc. Ser. A* **50** (1991), 297–315.

[31] C. E. Praeger, Kronecker classes of fields and covering subgroups of finite groups, *J. Austral. Math. Soc. Ser. A* **57** (1994), 17–34.

[32] J. P. Serre, On a theorem of Jordan, *Bull. Amer. Math. Soc.* **40** (2003), 429–440.

[33] C. L. Siegel, Approximation algebraischer Zahlen, *Math. Z.* **10** (1921) 173–213.

[34] P. Spiga, The Erdős-Ko-Rado theorem for the derangement graph of the projective general linear group acting on the projective space, *J. Combin. Theory Ser. A* **166** (2019), 59–90.

[35] C. L. Stewart, R. Tijdeman, On the Oesterlé-Masser conjecture, *Monatsh, Math.* **102** (1986), 251–257.

[36] R. A. Wilson, Maximal subgroups of sporadic groups. *Finite simple groups: thirty years of the atlas and beyond*, 57–72, Contemp. Math., 694, Amer. Math. Soc., Providence, RI, 2017.

[37] R. A. Wilson, The uniqueness of $PSU_3(8)$ in the Monster, *Bull. Lond. Math. Soc.* **49** (2017), 877–880.

[38] K. Zsigmondy, Zur Theorie der Potenzreste, *Monatsh. Math. Phys.* **3** (1892), 265–284.

MARCO FUSARI, DIPARTIMENTO DI MATEMATICA "FELICE CASORATI", UNIVERSITY OF PAVIA, VIA FERRATA 5, 27100 PAVIA, ITALY
*Email address*: `lucamarcofusari@gmail.com`

ANDREA PREVITALI, DIPARTIMENTO DI MATEMATICA E APPLICAZIONI, UNIVERSITY OF MILANO-BICOCCA, VIA COZZI 55, 20125 MILANO, ITALY
*Email address*: `andrea.previtali@unimib.it`

PABLO SPIGA, DIPARTIMENTO DI MATEMATICA E APPLICAZIONI, UNIVERSITY OF MILANO-BICOCCA, VIA COZZI 55, 20125 MILANO, ITALY
*Email address*: `pablo.spiga@unimib.it`