Bull. Aust. Math. Soc. **113** (2026), 467–474
doi:10.1017/S0004972725100695

DERANGEMENTS IN PERMUTATION GROUPS WITH TWO ORBITS

MELISSA LEE✉, TOMASZ POPIEL and GABRIEL VERRET

(Received 2 September 2025; accepted 6 September 2025; first published online 5 December 2025)

Abstract

A classical theorem of Jordan asserts that if a group G acts transitively on a finite set of size at least 2, then G contains a derangement (a fixed-point free element). Generalisations of Jordan's theorem have been studied extensively, due in part to their applications in graph theory, number theory and topology. We address a generalisation conjectured recently by Ellis and Harper ['Orbits of permutation groups with no derangements', Preprint, 2024, arXiv:2408.16064], which says that if G has exactly two orbits and those orbits have equal length $n \geq 2$, then G contains a derangement. We prove this conjecture in the case where n is a product of two primes, and in the case where $n = bp$ with p a prime and $2b \leq p$. We also verify the conjecture computationally for $n \leq 30$.

2020 *Mathematics subject classification*: primary 20B10.

Keywords and phrases: derangement, finite group, permutation group.

1. Introduction

We assume throughout that all groups and sets are finite. Let G be a group acting on a set Ω. A *derangement* is an element of G that fixes no point of Ω. A classical theorem of Jordan [7] asserts that if G acts transitively on Ω and $|\Omega| \geq 2$, then G contains a derangement. Equivalently, a group is never equal to the union of the conjugates of a proper subgroup. Generalisations of this result have been and continue to be studied intensively, due in part to numerous well-known applications [9]. This is intended to be a short note on one such generalisation, so we refer the reader to [3, Ch. 1] for further historical background.

The transitivity assumption in Jordan's theorem is necessary: it is easy to construct examples with G having exactly two orbits but no derangement. However, Ellis and Harper have conjectured that this cannot happen if the two orbits have equal length

The first author acknowledges the support of an Australian Research Council Discovery Early Career Researcher Award (project number DE230100579).

© The Author(s), 2025. Published by Cambridge University Press on behalf of Australian Mathematical Publishing Association Inc. This is an Open Access article, distributed under the terms of the Creative Commons Attribution licence (https://creativecommons.org/licenses/by/4.0/), which permits unrestricted re-use, distribution, and reproduction in any medium, provided the original work is properly cited.

https://doi.org/10.1017/S0004972725100695 Published online by Cambridge University Press

$n \geq 2$ (see [5, Conjecture 2]). They have proved this conjecture in various cases, including:

(i) when G acts primitively on one of its two orbits;
(ii) when G is simple, nilpotent or of order at most 1000;
(iii) when n is a prime power.

Here, we prove Ellis and Harper's conjecture under the assumption that n is a product of two primes, and under the assumption that $n = bp$ with p a prime and $2b \leq p$ (see Corollaries 3.6 and 3.4 respectively). We also verify computationally that the conjecture holds when $n \leq 30$ (see Proposition 3.1).

2. Preliminaries

LEMMA 2.1 [1, Lemma 2.2]. *Let G be a group acting transitively on a set Ω, let p be a prime and let P be a Sylow p-subgroup of G. The minimum length of a P-orbit on Ω is the largest power of p dividing $|\Omega|$.*

LEMMA 2.2. *Let $V = \mathbb{F}_q^d$, where $d \geq 2$ and q is a prime power. Fix a basis for V, let $0 \neq a \in V$ and define $U = \{v \in V \mid a \cdot v = 0\}$. If k is the number of nonzero coefficients of a with respect to the fixed basis, then the number of $(u_1, \ldots, u_d) \in U$ such that $u_1, \ldots, u_d \neq 0$ is equal to*

$$\frac{(q-1)^{d-k+1}}{q}((q-1)^{k-1} - (-1)^{k-1}).$$

In particular, this number is at most $(q-1)^{d-1}$.

PROOF. Given $j \geq 1$, $m \in \mathbb{F}_q$ and $(a_1, \ldots, a_j) \in \mathbb{F}_q^j$ with $a_1, \ldots, a_j \neq 0$, consider the equation $\sum_{i=1}^{j} a_i x_i = m$. Call a solution $(x_1, \ldots, x_j) \in \mathbb{F}_q^j$ to this equation 'good' if $x_1, \ldots, x_j \neq 0$. First, notice that, because $\mathbb{F}_q$ is a field, the number of good solutions does not depend on $a_1, \ldots, a_j$. Similarly, the number of good solutions depends only on whether $m = 0$ or not. We may thus define $D_m(j)$ to be the number of good solutions to this and, hence, every equation of the given form. For $j \geq 2$,

$$D_0(j) = (q-1)D_{-a_j x_j}(j-1) = (q-1)D_1(j-1).$$

It follows that, for $j \geq 2$,

$$D_1(j) = (q-2)D_1(j-1) + D_0(j-1).$$

Combining these two equations yields, for $j \geq 3$,

$$D_1(j) = (q-2)D_1(j-1) + (q-1)D_1(j-2).$$

This is a second-order linear difference equation for $D_1(j)$; the initial conditions $D_1(1) = 1$ and $D_1(2) = q-2$ yield

$$D_1(j) = \frac{(q-1)^j - (-1)^j}{q} \quad \text{and hence} \quad D_0(j) = (q-1)\frac{(q-1)^{j-1} - (-1)^{j-1}}{q}$$

https://doi.org/10.1017/S0004972725100695 Published online by Cambridge University Press

for all $j \geq 1$. The first assertion of the lemma follows upon observing that the number of $(u_1, \ldots, u_d) \in U$ such that $u_1, \ldots, u_d \neq 0$ is equal to $(q-1)^{d-k} D_0(k)$. Since $a \neq 0$, we have $k \geq 1$ and the second assertion is then easily verified. □

LEMMA 2.3. *Let q be a prime power and let $V = \mathbb{F}_q^d$. If $\mathcal{W}$ is a set of subspaces of V of codimension 1 such that*

(1) $\bigcup_{W \in \mathcal{W}} W = V$ *and*
(2) $\bigcap_{W \in \mathcal{W}} W = \{0\}$,

then $2 \leq d \leq |\mathcal{W}| - q + 1$.

PROOF. The assertion that $d \geq 2$ is immediate, because condition (1) is never satisfied if $d \leq 1$. Let $W_1 \in \mathcal{W}$. If $W_1 \neq \{0\}$, then, by condition (2), there exists $W_2 \in \mathcal{W}$ such that $W_1 \not\leq W_2$. It follows that $W_1 + W_2 = V$ and

$$\dim(W_1 \cap W_2) = \dim(W_1) + \dim(W_2) - \dim(V) = 2(d-1) - d = d - 2,$$

so $W_1 \cap W_2$ has codimension 2 in V. If $W_1 \cap W_2 \neq \{0\}$, then, by condition (2), there exists $W_3 \in \mathcal{W}$ such that $W_1 \cap W_2 \not\leq W_3$. Since W_3 has codimension 1 in V, this implies that $W_3 + (W_1 \cap W_2) = V$ and, by a similar calculation as earlier, $W_1 \cap W_2 \cap W_3$ has codimension 3 in V. Repeating this procedure, we find that $\mathcal{W}$ contains d subspaces $W_1, \ldots, W_d$ with $\bigcap_{i \in \{1,\ldots,d\}} W_i = \{0\}$. By choosing an appropriate basis for V, we can assume that W_i is defined by the linear equation $x_i = 0$. Note that $\bigcup_{i \in \{1,\ldots,d\}} W_i$ consists of the vectors in V with at least one coordinate equal to 0, so $|\bigcup_{i \in \{1,\ldots,d\}} W_i| = q^d - (q-1)^d$. This leaves $(q-1)^d$ elements of V to 'cover' by adjoining further subspaces from $\mathcal{W}$, to satisfy condition (1). Lemma 2.2 implies that adjoining one further subspace from $\mathcal{W}$ covers at most $(q-1)^{d-1}$ further elements. We must therefore adjoin at least another $q-1$ subspaces to satisfy condition (1), so $|\mathcal{W}| \geq d + (q-1)$. □

REMARK 2.4. Note that the upper bound in Lemma 2.3 is tight. Indeed, for $i \in \{1, \ldots, d\}$, let W_i be the subspace defined by $x_i = 0$. Note that $\bigcap_{i \in \{1,\ldots,d\}} W_i = \{0\}$. Let $\mathcal{U}$ be the set of subspaces that are strictly between V and $W_1 \cap W_2$. Since $W_1 \cap W_2$ has codimension 2 in V, we have $|\mathcal{U}| = q + 1$. It is easy to check that $\bigcup_{U \in \mathcal{U}} U = V$ and that $\mathcal{U} \cap \{W_1, \ldots, W_d\} = \{W_1, W_2\}$, and hence $\mathcal{U} \cup \{W_1, \ldots, W_d\}$ has size $d + q - 1$ and satisfies both conditions of Lemma 2.3. Moreover, it is not hard to show using Lemma 2.2 that, up to conjugacy in $\mathrm{GL}(V)$, this is the unique tight example, but we will not need this fact.

Given a group G acting (not necessarily faithfully) on a set Ω and $\omega \in \Omega$, we write G_ω for the point stabiliser of ω in Ω. Given $g \in G$ and a subset $\Delta \subseteq \Omega$ preserved by G, we write G_Δ for the setwise stabiliser of Δ in G and g^Δ for the permutation induced by g on Δ. We also let $G^\Delta := \{g^\Delta : g \in G\}$.

Let $n \geq 1$ and let T be a nonabelian finite simple group. Recall that the full wreath product $\mathrm{Aut}(T) \wr S_n$ has socle $K := T_1 \times \cdots \times T_n$, where each T_i is isomorphic to T.

https://doi.org/10.1017/S0004972725100695 Published online by Cambridge University Press

Moreover, $\{T_1, \dots, T_n\}$ is the set of minimal normal subgroups of $T_1 \times \cdots \times T_n$, and hence $\mathrm{Aut}(T) \wr S_n$ acts on $\{T_1, \dots, T_n\}$ by conjugation. Given $G \leq \mathrm{Aut}(T) \wr S_n$, the stabiliser G_{T_1} of T_1 acts on T_1, and the induced permutation group $G_{T_1}^{T_1}$ is naturally identified with a subgroup of $\mathrm{Aut}(T_1)$. In particular, we have $T_1^{T_1} = \mathrm{Inn}(T_1)$ under this identification.

PROPOSITION 2.5. *With notation as above, if*

(1) $\mathrm{Inn}(T_1) \leq G_{T_1}^{T_1}$ *and*
(2) G *acts primitively on* $\{T_1, \dots, T_n\}$,

then either $G \cap K = 1$, $G \cap K \cong T$ *or* $K \leq G$.

PROOF. Let φ_i be the natural projection from K to T_i and let

$$K_i := \ker \varphi_i = T_1 \times \cdots \times T_{i-1} \times 1 \times T_{i+1} \times \cdots \times T_n.$$

Note that $\mathrm{Inn}(T_1)$ is the unique minimal normal subgroup of $G_{T_1}^{T_1}$, because $\mathrm{Inn}(T_1) \leq G_{T_1}^{T_1} \leq \mathrm{Aut}(T_1)$. Since $G \cap K$ is a normal subgroup of G_{T_1}, it follows that $(G \cap K)^{T_1}$ is normal in $G_{T_1}^{T_1}$ and so either $(G \cap K)^{T_1} = 1$ or $\mathrm{Inn}(T_1) \leq (G \cap K)^{T_1}$. If $(G \cap K)^{T_1} = 1$, then $G \cap K \leq K_1$. Since G acts transitively on $\{T_1, \dots, T_n\}$, this implies that $G \cap K \leq K_i$ for every $i \in \{1, \dots, n\}$, and thus $G \cap K = 1$, as required. We may thus assume that $\mathrm{Inn}(T_1) \leq (G \cap K)^{T_1}$, that is, the restriction $\varphi_1 : G \cap K \to T_1$ is surjective and thus $(G \cap K)/(G \cap K_1) \cong T$.

For $i \in \{1, \dots, n\}$, let $G_i = G \cap K_i$. Define an equivalence relation $\sim$ on $\{T_1, \dots, T_n\}$ by $T_i \sim T_j$ if and only if $G_i = G_j$. This equivalence relation is G-invariant so, by condition (2), the induced partition is either the universal one or the partition into singletons. We now consider these two cases separately.

Case 1: $G_i = G_j$ *for all* $i, j \in \{1, \dots, n\}$. Since $K_1 \cap \cdots \cap K_n = 1$, we have $G_1 = 1$, so the restriction $\varphi_1 : G \cap K \to T_1$ is injective. We saw earlier that it is surjective, and hence it is an isomorphism and $G \cap K \cong T$, as required.

Case 2: $G_i \neq G_j$ *for all* i, j *with* $i \neq j$. We saw earlier that $(G \cap K)/G_1 \cong T$. Together with condition (2), this implies that $(G \cap K)/G_i \cong T$ for all $i \in \{1, \dots, n\}$. We now proceed by induction. Suppose that $1 \leq m < n$ is such that $(G \cap K)/(G_1 \cap \cdots \cap G_m) \cong T^m$. Let $N = (G_1 \cap \cdots \cap G_m)G_{m+1}$. Note that $G_1 \cap \cdots \cap G_m$ and G_{m+1} are both normal subgroups of $G \cap K$, and hence so is N. Since $(G \cap K)/G_{m+1} \cong T$ is simple, we must have $N = G \cap K$ or $N = G_{m+1}$. If $N = G_{m+1}$, then $G_1 \cap \cdots \cap G_m \leq G_{m+1}$. Since $(G \cap K)/(G_1 \cap \cdots \cap G_m) \cong T^m$ has precisely m normal subgroups of index $|T|$, it follows that $G \cap K$ has precisely m normal subgroups of index $|T|$ containing $G_1 \cap \cdots \cap G_m$. The latter are precisely $G_1, \dots, G_m$, so we must have $G_{m+1} = G_i$ for some $i \in \{1, \dots, m\}$, which is a contradiction. Therefore, $N = G \cap K$. It follows that

$$\begin{aligned}(G \cap K)/(G_1 \cap \cdots \cap G_{m+1}) \\ \cong (G \cap K)/(G_1 \cap \cdots \cap G_m) \times (G \cap K)/G_{m+1} \cong T^m \times T \cong T^{m+1}.\end{aligned}$$

https://doi.org/10.1017/S0004972725100695 Published online by Cambridge University Press

This completes the induction and yields $(G \cap K)/(G_1 \cap \cdots \cap G_n) \cong T^n$. Since $G \cap K \leq K \cong T^n$, it follows that $G \cap K = K$ and hence $K \leq G$, as required. □

Given a group G acting on a set Ω, let

$$\nu(G) = \frac{|\bigcup_{\omega \in \Omega} G_\omega|}{|G|}.$$

Note that this is exactly the proportion of nonderangements in G.

LEMMA 2.6. *If G is a group acting on a set $\Omega = \Omega_1 \cup \cdots \cup \Omega_k$ where each of the subsets $\Omega_1, \ldots, \Omega_k$ is preserved by G, then*

$$\nu(G) \leq \sum_{i \in \{1,\ldots,k\}} \nu(G^{\Omega_i}).$$

PROOF. For each $i \in \{1, \ldots, k\}$, let K_i be the kernel of the action homomorphism from G to $\mathrm{Sym}(\Omega_i)$. We have

$$\begin{aligned}\nu(G) = \frac{|\bigcup_{\omega \in \Omega} G_\omega|}{|G|} &\leq \sum_{i \in \{1,\ldots,k\}} \frac{|\bigcup_{\omega \in \Omega_i} G_\omega|}{|G|} = \sum_{i \in \{1,\ldots,k\}} \frac{|\bigcup_{\omega \in \Omega_i} G_\omega^{\Omega_i}| \cdot |K_i|}{|G^{\Omega_i}| \cdot |K_i|} \\ &= \sum_{i \in \{1,\ldots,k\}} \frac{|\bigcup_{\omega \in \Omega_i} G_\omega^{\Omega_i}|}{|G^{\Omega_i}|} = \sum_{i \in \{1,\ldots,k\}} \nu(G^{\Omega_i}),\end{aligned}$$

as required. □

3. Main results

Throughout this section, let G be a permutation group on a set Ω of size $2n$, and assume that G has exactly two orbits, Ω_1 and Ω_2, each of length n.

PROPOSITION 3.1. *If $2 \leq n \leq 30$, then G has a derangement.*

PROOF. Note that the transitive groups of degree at most 30 are known [6] and readily accessible in Magma [2]. The proof is supported by the Magma code available on the first author's GitHub [8]; the process that we now describe is carried out for each degree $n \in \{2, \ldots, 30\}$ using the function `HalfTransitiveDerangements`. If G has no derangements, then [5, Corollary 4] implies that there exist transitive but imprimitive permutation groups G_1 and G_2 of degree n such that $G^{\Omega_i} \cong G_1$ for $i \in \{1, 2\}$. We begin by constructing each transitive but imprimitive permutation group H of degree n and directly counting the number of nonderangements in H (by computing the support of a representative of each conjugacy class of H). By Lemma 2.6, the proportion of nonderangements in G is bounded above by the sum of the proportions of the nonderangements in G_1 and G_2, which we compute for each pair (G_1, G_2) using the aforementioned data. If this proportion is less than 1, then G certainly has a derangement, so we discard the pair (G_1, G_2). For each remaining pair (G_1, G_2), we know that G must be a subdirect product of G_1 and G_2. The property of

https://doi.org/10.1017/S0004972725100695 Published online by Cambridge University Press

being a subdirect product is preserved when taking supergroups, so we simply traverse the upper layers of the subgroup lattice of $G_1 \times G_2$, stopping whenever we find a group that is not a subdirect product, until we have constructed all subdirect products of G_1 and G_2 (up to conjugacy in $G_1 \times G_2$). Finally, we exhibit a derangement in each subdirect product either by random search or by checking each conjugacy class. □

LEMMA 3.2. *Let p be a prime, let P be a Sylow p-subgroup of G and let $n = bp^k$. If $b < p$, then P has $2b$ orbits of length p^k.*

PROOF. By Lemma 2.1, the minimum length of a P^{Ω_i}-orbit is p^k. Since $b < p$, we have $n < p^{k+1}$, and hence every P^{Ω_i}-orbit has length exactly p^k and the result follows. □

LEMMA 3.3. *Let p be a prime, let P be a Sylow p-subgroup of G, let $|P| = p^d$ and let $n = bp$ with $b < p$. Then P has $2b$ orbits of length p, P is elementary abelian and we have $|\{P_\omega \mid \omega \in \Omega\}| \leq 2b$. Moreover, if P does not contain a derangement, then we have $2 \leq d \leq |\{P_\omega \mid \omega \in \Omega\}| - p + 1 \leq 2b - p + 1$.*

PROOF. Note that $\bigcap_{\omega\in\Omega} P_\omega = 1$ because G is a permutation group on Ω. By Lemma 3.2, P has $2b$ orbits of length p. It follows that for every $\omega \in \Omega$, we have $|P : P_\omega| = p$, so P_ω is a normal (and maximal) subgroup of P. This implies that P is elementary abelian (because P has trivial Frattini subgroup) and that $|\{P_\omega \mid \omega \in \Omega\}| \leq 2b$. If P does not contain a derangement, then $\bigcup_{\omega\in\Omega} P_\omega = P$ and Lemma 2.3 implies that $2 \leq d \leq |\{P_\omega \mid \omega \in \Omega\}| - p + 1$. □

COROLLARY 3.4. *If $n = bp$ with p a prime and $2b \leq p$, then G has a derangement.*

PROPOSITION 3.5. *If $n = pq$ with $p > q$ primes and q does not divide $p - 1$, then G has a derangement.*

PROOF. Assume for a contradiction that G does not have a derangement. Let P be a Sylow p-subgroup of G and write $|P| = p^d$. By Lemma 3.3, P has $2q$ orbits of length p, P is elementary abelian, $|\{P_\omega \mid \omega \in \Omega\}| \leq 2q$ and

$$2 \leq d \leq |\{P_\omega \mid \omega \in \Omega\}| - p + 1 \leq 2q - p + 1.$$

Suppose first that $|P^{\Omega_i}| \leq p$ for some $i \in \{1, 2\}$. This implies that $P_\omega = P_{\omega'}$ for every $\omega, \omega' \in \Omega_i$, namely $|\{P_\omega \mid \omega \in \Omega_i\}| = 1$, and hence $|\{P_\omega \mid \omega \in \Omega\}| \leq q + 1$, which contradicts the facts that $2 \leq d \leq |\{P_\omega \mid \omega \in \Omega\}| - p + 1$ and $q < p$. Therefore, $|P^{\Omega_i}| \geq p^2$ for both $i \in \{1, 2\}$.

By [5, Corollary 4], each G^{Ω_i} is imprimitive and so preserves a block system consisting of either p blocks of size q or q blocks of size p. In the former case, $G^{\Omega_i} \leq S_q \wr S_p$, so $|P^{\Omega_i}| \leq p$, which contradicts $|P^{\Omega_i}| \geq p^2$. (Here, we abuse notation and write $\leq$ to mean 'is isomorphic to a subgroup of'.) Therefore, each G^{Ω_i} preserves a system $\mathcal{B}_i$ of q blocks of size p, so $G^{\Omega_i} \leq S_p \wr S_q$. Choose $B \in \mathcal{B}_i$. Then we have $G^{\Omega_i} \leq (G^{\Omega_i})^B_B \wr (G^{\Omega_i})^{\mathcal{B}_i}$, with $(G^{\Omega_i})^B_B$ a transitive subgroup of $\mathrm{Sym}(B) \cong S_p$ and $(G^{\Omega_i})^{\mathcal{B}_i}$ a transitive subgroup of $\mathrm{Sym}(\mathcal{B}_i) \cong S_q$. Since p is prime, it follows from classical results of Burnside [4, Ch. IX, Theorem IX] that either $(G^{\Omega_i})^B_B \leq \mathrm{AGL}(1, p)$ or $(G^{\Omega_i})^B_B$ is almost simple.

https://doi.org/10.1017/S0004972725100695 Published online by Cambridge University Press

Suppose first that $(G^{\Omega_i})^{\mathcal{B}}_B$ is almost simple, and note that the socle T of $(G^{\Omega_i})^{\mathcal{B}}_B$ is transitive and, in particular, p divides $|T|$. Let $K = \mathrm{soc}((G^{\Omega_i})^{\mathcal{B}}_B \wr S_q) \cong T^q$. By Proposition 2.5, either $G^{\Omega_i} \cap K = 1$, $G^{\Omega_i} \cap K \cong T$ or $K \leq G^{\Omega_i}$. If $G^{\Omega_i} \cap K = 1$ or $G^{\Omega_i} \cap K \cong T$, then $|P^{\Omega_i}| \leq p$, which contradicts $|P^{\Omega_i}| \geq p^2$. If $K \leq G^{\Omega_i}$, then p^q divides $|G^{\Omega_i}|$ and $q \leq d$, contradicting $d \leq 2q - p + 1$, $q < p$ and $q \neq p - 1$.

We must therefore have $(G^{\Omega_i})^{\mathcal{B}}_B \leq \mathrm{AGL}(1, p)$, hence $G^{\Omega_i} \leq \mathrm{AGL}(1, p) \wr S_q$ for both $i \in \{1, 2\}$. Let Q be a Sylow q-subgroup of G. Since q does not divide $p - 1$, it does not divide $|\mathrm{AGL}(1, p)| = p(p - 1)$, hence $|Q^{\Omega_i}| = q$. It follows from Lemma 2.1 that all orbits of Q^{Ω_i} have length q and thus $|Q : Q_\omega| = q$ for every $\omega \in \Omega$. Let $\omega_i \in \Omega_i$ and $g \in Q_{\omega_i}$. Note that g stabilises the block of $\mathcal{B}_i$ containing ω_i, and hence, since g is a q-element, g must also stabilise the remaining $q - 1$ blocks of $\mathcal{B}_i$. It follows that $g^{\Omega_i} \in \mathrm{AGL}(1, p)^q$, but q does not divide $|\mathrm{AGL}(1, p)|$, hence $g^{\Omega_i} = 1$. This implies that $g \in Q_\omega$ for every $\omega \in \Omega_i$, so $Q_{\omega_i} \leq Q_\omega$ for every $\omega \in \Omega_i$. Since $|Q_\omega| = |Q_{\omega_i}|$, we have $Q_\omega = Q_{\omega_i}$ for every $\omega \in \Omega_i$. This implies that Q has at most two distinct point stabilisers, so it must contain a derangement (because it cannot be equal to the union of two proper subgroups). □

COROLLARY 3.6. *If $n = pq$ with p, q primes, then G has a derangement.*

PROOF. If $p = q$, then the result follows from [5, Corollary 5], so we assume that $p > q$. If q does not divide $p - 1$, then the result follows from Proposition 3.5, so we assume that q divides $p - 1$. If $q = p - 1$, then $p = 3$ and $q = 2$, and the result follows from Proposition 3.1. Otherwise, $q \leq (p - 1)/2$ and the result follows from Corollary 3.4. □

Acknowledgements

Melissa Lee and Tomasz Popiel are grateful to Gabriel Verret and The University of Auckland for their hospitality during a research visit in January 2025, when this work was initiated. We thank Scott Harper for helpful comments on an earlier draft of the paper.

References

[1] J. Bamberg, A. Bors, A. Devillers, M. Giudici, C. E. Praeger and G. F. Royle, 'Orbits of Sylow subgroups of finite permutation groups', *J. Algebra* **607** (2022), 107–133.
[2] W. Bosma, J. Cannon and C. Playoust, 'The Magma algebra system. I. The user language', *J. Symbolic Comput.* **24**(3–4) (1997), 235–265.
[3] T. C. Burness and M. Giudici, *Classical Groups, Derangements and Primes*, Australian Mathematical Society Lecture Series, 25 (Cambridge University Press, Cambridge, 2016).
[4] W. Burnside, *Theory of Groups of Finite Order* (Cambridge University Press, Cambridge, 1897).
[5] D. Ellis and S. Harper, 'Orbits of permutation groups with no derangements', Preprint, 2024, arXiv:2408.16064.
[6] A. Hulpke, 'Constructing transitive permutation groups', *J. Symbolic Comput.* **39**(1) (2005), 1–30.
[7] C. Jordan, 'Recherches sur les substitutions', *J. Math. Pures Appl. (9)* **17** (1872), 351–367.
[8] M. Lee, 'Derangements', code accompanying this paper (2025). https://github.com/melissa-maths/derangements.
[9] J.-P. Serre, 'On a theorem of Jordan', *Bull. Amer. Math. Soc. (N.S.)* **40**(4) (2003), 429–440.

https://doi.org/10.1017/S0004972725100695 Published online by Cambridge University Press

MELISSA LEE, School of Mathematics,
Monash University, Clayton, Victoria 3800, Australia
e-mail: melissa.lee@monash.edu

TOMASZ POPIEL, School of Mathematics,
Monash University, Clayton, Victoria 3800, Australia
e-mail: tomasz.popiel@monash.edu

GABRIEL VERRET, Department of Mathematics,
University of Auckland, Private Bag 92019, Auckland 1142, New Zealand
e-mail: g.verret@auckland.ac.nz

https://doi.org/10.1017/S0004972725100695 Published online by Cambridge University Press