CONFLUENTES MATHEMATICI
LYON

Nick GILL and Pierre GUILLOT

The binary actions of alternating groups

Volume 17 (2025), p. 73–89.
https://doi.org/10.5802/cml.101

© Les auteurs, 2025.
Certains droits réservés.
Les articles des *Annales de la Faculté des Sciences de Toulouse* sont mis à disposition sous la license Creative Commons Attribution-NonCommercial-NoDerivs (CC-BY-NC-ND) 4.0 http://creativecommons.org/licenses/by-nc-nd/4.0/

Publication membre du centre
Mersenne pour l'édition scientifique ouverte
http://www.centre-mersenne.org/
e-ISSN : 1793-7434

Confluentes Math.
17 (2025), p. 73-89

THE BINARY ACTIONS OF ALTERNATING GROUPS

NICK GILL AND PIERRE GUILLOT

Abstract. Given a conjugacy class $\mathcal{C}$ in a group G we define a new graph, $\Gamma(\mathcal{C})$, whose vertices are elements of $\mathcal{C}$; two vertices $g, h \in \mathcal{C}$ are connected in $\Gamma(\mathcal{C})$ if $[g, h] = 1$ and either gh^{-1} or hg^{-1} is in $\mathcal{C}$.

We prove a lemma that relates the binary actions of the group G to connectivity properties of $\Gamma(\mathcal{C})$. This lemma allows us to give a complete classification of all binary actions when $G = A_n$, an alternating group on n letters with $n \geqslant 5$.

1. Introduction

Let G be a permutation group on a set Ω. The *relational complexity* of G is the minimum integer $k \geqslant 2$ such that the orbits of G on Ω^r, for any $r \geqslant k$, can be deduced from the orbits of G on Ω^k. (A more precise definition will be given in Section 2.) Permutation groups whose relational complexity is equal to 2 are called *binary*, and the concern of this paper is to contribute to the classification of the finite binary permutation groups.

The motivation for attempting such a classification is rooted in striking results of Cherlin [1] building on work of Lachlan (see, for instance, [10]) which show that the notion of relational complexity can be used to stratify the world of finite permutation groups in a precise sense.

To understand how a particular finite permutation group G fits into this stratification, one needs to know the relational complexity of G, together with another parameter, the *minimal number of relations* of G. Now Cherlin asserts that the stratification has the following property: given integers k and ℓ, the (isomorphism classes of) permutation groups of relational complexity $\leqslant k$ and minimal number of relations $\leqslant \ell$ fall into finitely many infinite families, with finitely many sporadic exceptions; moreover, any permutation group, though considered sporadic in this classification for a given choice of (k, ℓ), will belong to one of the families for the classification corresponding to some choices (k', ℓ') with $k' \geqslant k$ and $\ell' \geqslant \ell$.

We stress that there is not, at present, a single pair (k, ℓ) for which the classification has been made explicit, although Lachlan's classification of homogeneous digraphs all but deals with the pair $(2, 1)$ [9]. Aside from this, though, our understanding of how this stratification works in practice is rather limited.

Over the last few years, a number of papers have been dedicated to the study of *binary primitive permutation groups* (i.e. primitive permutation groups with relational complexity equal to 2) and a full classification of these objects is now known [2, 3, 6, 7, 8, 12].

Extending this work to cover *imprimitive* binary permutation groups seems very difficult. A more reasonable starting point might be to understand the binary actions of important families of (abstract) groups. To this end, we propose to investigate, in a series of papers, the possibility of classifying all binary actions

2020 *Mathematics Subject Classification:* 20D06, 20B25, 20B10.
Keywords: permutation group, binary action, relational complexity, alternating group.

of groups G that are *almost simple*. In this paper we introduce a crucial new tool for this, and use it to deal with the alternating groups.

Our results all rely on the study of a graph which, so far as we are aware, is defined here for the first time: given a conjugacy class $\mathcal{C}$ in a group G we define a graph, $\Gamma(\mathcal{C})$, whose vertices are elements of $\mathcal{C}$; two vertices $g, h \in \mathcal{C}$ are connected in $\Gamma(\mathcal{C})$ if g and h commute and either gh^{-1} or hg^{-1} is in $\mathcal{C}$.

The connection to binary actions is achieved via the following result which is stated again, using slightly different language, as Corollary 2.13.

Lemma 1.1. — *Let G be a transitive permutation group on a set Ω. Let $\mathcal{C}$ be a conjugacy class of elements of prime order p of maximal fixity. Let H be the stabilizer of a point in Ω and let $g \in H \cap \mathcal{C}$. Then H contains all vertices in the connected component of $\Gamma(\mathcal{C})$ that contains g.*

Note that *an element of order p of maximal fixity* is simply an element of G of order p that fixes at least as many points of Ω as any other element of G of order p.

It turns out, for instance, that when $G = A_n$ and $p = 2$, the graph $\Gamma(\mathcal{C})$ is often connected. (Proposition 3.4 gives a precise statement.) This heavily restricts the possible transitive binary actions of $G = A_n$ for which a point-stabilizer has even order.

This fact, together with a further analysis for p odd, is the basis of our main result. Note that, in the following statement, we speak of a binary action, rather than a binary permutation group; this is defined in the obvious way, and allows a simpler formulation here.

Theorem 1.2. — *Let G be the alternating group A_n with $n \geqslant 6$. Assume that there is a binary action of G on the set Ω. Then each orbit of G on Ω is either trivial or regular.*

In a subsequent paper [4], we shall give similar results for simple groups having a single conjugacy class of involutions, among other groups. This will include A_5, for which the above theorem fails to hold.

A third paper with M. Liebeck [5], will fully describe the graph $\Gamma(\mathcal{C})$ when $\mathcal{C}$ is a conjugacy class of involutions in a simple group of Lie type of characteristic 2. It is our hope that $\Gamma(\mathcal{C})$ will become an object of investigation in its own right.

One naturally wonders to what extent the results for A_n extend to S_n. It turns out that the situation is a little different for the symmetric group, as it is possible to exhibit several families of transitive binary actions on Ω, the set of cosets of a subgroup $H < S_n$. For example:

(1) $H = \{1\}$ or $H = A_n$;
(2) $H = \langle g \rangle$ where g is an odd permutation of order 2;
(3) $H \cong S_{n-d}$ where $1 \leqslant d \leqslant n-1$, and the action of S_n on Ω is permutation isomorphic to the natural action on the set of d tuples of elements from $\{1, \ldots, n\}$.

(Note that we say "permutation isomorphic" rather than "permutation equivalent" in item (3) to account for the case $n = 6$.) In an unpublished preprint, the first author has proved that, for $n \geqslant 6$, these are all the non-trivial transitive binary actions of S_n.

2. Background on relational complexity

2.1. **Complexity & some basic criteria.** All groups mentioned in this paper are finite, and all group actions are on finite sets. We consider a group G acting on a finite set Ω (on the right) and we begin by defining the *relational complexity*, $\mathrm{RC}(G,\Omega)$, of the action, which is an integer greater than 1.

There are at least two equivalent definitions of $\mathrm{RC}(G,\Omega)$. The first definition involves *homogeneous relational structures* on Ω, and while it is useful in particular for motivation, we shall work exclusively with a different definition in terms of the action of G on tuples. More information on the first definition, as well as a wealth of results on relational complexity, can be found in [7].

So let $I, J \in \Omega^n$ be n-tuples of elements of Ω, for some $n \geqslant 1$, written $I = (I_1, \ldots, I_n)$ and $J = (J_1, \ldots, J_n)$. For $r \leqslant n$, we say that I and J are *r-related*, and we write $I \underset{r}{\sim} J$, when for each choice of indices $1 \leqslant k_1 < k_2 < \cdots < k_r \leqslant n$, there exists $g \in G$ such that $I^g_{k_i} = J_{k_i}$ for all i. (An alternative terminology is to say that I and J are r-subtuple complete with respect to G.)

Now the *relational complexity* of the action of G on Ω, written $\mathrm{RC}(G,\Omega)$, is the smallest integer $k \geqslant 2$ such that whenever $n \geqslant k$ and $I, J \in \Omega^n$ are k-related, then I and J are n-related (or in other words there exists $g \in G$ with $I^g = J$). One can show that such an integer always exists and indeed, it is always less than $|\Omega|$ (or it is 2 if $|\Omega| = 1$ or 2), see [7]. Which brings us to a quick comment about the condition $k \geqslant 2$: there is no universally accepted definition for actions of complexity 1 or 0, as several obvious putative definitions do not agree. In any case, only trivial cases would be deemed to have complexity < 2, and at present the convention is to ignore these, so the minimum complexity that we allow is 2. When $\mathrm{RC}(G,\Omega) = 2$, we say that the action is *binary*.

Example 2.1. — The action of the symmetric group S_d on $\{1, 2, \ldots, d\}$ is obviously binary (a simple, general remark is that one only needs to consider tuples of distinct elements, so in this example we only look at n-tuples with $n \leqslant d$). On the other hand, the complexity of the action of A_d on the same set is $d-1$. To see this, following Cherlin, consider the tuples $(1, 2, \ldots, d-2, d-1)$ and $(1, 2, \ldots, d-2, d)$: these are not $(d-1)$-related, but they are k-related for any $k < d-1$.

Example 2.2. — There are two obvious examples of binary actions, for every group G. First, there is the case when Ω contains a single element; we call this the *trivial* binary action. The other canonical example is the *regular* binary action, that is when $\Omega = G$ with its action on itself by multiplication. It is an easy exercise to check that the latter is indeed binary; indeed one can go further and check that all *semiregular* actions are binary.

We are about to state a basic criterion for binariness that will be of constant use. Before we do this however, it is best to establish the next lemma, revealing the symmetry of a certain situation.

Lemma 2.3. — *Let G be a group. For $i = 1, 2, 3$, let H_i be a subgroup of G, and let $h_i \in H_i$. Assume that $h_1 h_2 h_3 = 1$. Then the following conditions are equivalent:*

(1) *there exist $h'_2 \in H_2 \cap H_1$ and $h'_3 \in H_3 \cap H_1$ such that $h_1 h'_2 h'_3 = 1$;*
(2) *there exist $h'_1 \in H_1 \cap H_2$ and $h'_3 \in H_3 \cap H_2$ such that $h'_1 h_2 h'_3 = 1$;*

(3) *there exist* $h_1' \in H_1 \cap H_3$ *and* $h_2' \in H_2 \cap H_3$ *such that* $h_1'h_2'h_3 = 1$.

Proof. — Assume (1), so that $h_2h_3 = h_2'h_3'$, which we rewrite as $h_3'h_3^{-1} = (h_2')^{-1}h_2 \in H_2 \cap H_3$. We have $(h_3')^{-1}(h_3'h_3^{-1})h_3 = 1$, with $(h_3')^{-1} \in H_1 \cap H_3$ and $h_3'h_3^{-1} \in H_2 \cap H_3$, so we have established (3). All the other implications are similar. □

When we have elements with $h_1h_2h_3 = 1$ as above, and when the equivalent conditions of the lemma fail to hold, we think of the triple (h_1, h_2, h_3) as "minimal" or "optimal", in the sense that it cannot be "improved" to a triple with all three elements taken from the same subgroup. As we shall see presently, the presence of such an optimal triple, with the groups H_i conjugates of a single subgroup H, is an obstruction to the binariness of the action of G on $(G : H)$.

Lemma 2.4 (basic criteria). — *Let G act on Ω. The following conditions are equivalent:*

(1) *There exist $I, J \in \Omega^3$ such that $I \underset{2}{\sim} J$ but $I \underset{3}{\not\sim} J$.*
(2) *There are points $\alpha_i \in \Omega$ with stabilizers H_i, and elements $h_i \in H_i$, for $i = 1, 2, 3$, satisfying:*
   (a) $h_1h_2h_3 = 1$,
   (b) *there do NOT exist $h_2' \in H_2 \cap H_1$, $h_3' \in H_3 \cap H_1$ with $h_1h_2'h_3' = 1$. (See also Lemma 2.3 above.)*
(3) *There are points $\alpha_i \in \Omega$ with stabilizers H_i, for $i = 1, 2, 3$, such that $H_1 \cap H_2 \cdot H_3$ is not included in $H_1 \cap (H_1 \cap H_2) \cdot H_3$.*

In particular, when these conditions hold, the action of G on Ω is not binary.

Proof. — It is clear that (3) is a simple reformulation of (2). Now assume (2), and let us prove (1). Let $\alpha_4 = \alpha_3^{h_1} = \alpha_3^{h_2^{-1}}$, using condition (2a). The triples $(\alpha_1, \alpha_2, \alpha_3)$ and $(\alpha_1, \alpha_2, \alpha_4)$ are 2-related. If they were 3-related, we would find $g \in H_1 \cap H_2$ taking α_3 to α_4, so $h_1g^{-1} \in H_3$, contrary to assumption (2b).

The converse is similar. □

2.2. **Removing the transitivity assumption.** Most results on relational complexity in the literature deal with transitive group actions. Nontransitive actions can be mysterious, but we can at least collect a few easy facts.

Lemma 2.5. — *Suppose G acts on X, and suppose that $Y \subset X$ is stable under the G-action. Then* $\mathrm{RC}(G, Y) \leqslant \mathrm{RC}(G, X)$.

Proof. — Let $k = \mathrm{RC}(G, X)$, and suppose that I, J are n-tuples of elements of Y which are k-related; then of course they are n-tuples of elements of X which are k-related, so they are n-related. Hence the complexity on Y is no greater than k. □

Lemma 2.6. — *Let X, Y be G-sets. Then*

$$\mathrm{RC}\Big(G, X \coprod Y\Big) = \mathrm{RC}\Big(G, X \coprod Y \coprod Y\Big).$$

Here and elsewhere we write $\coprod$ for the disjoint union.

Proof. — We certainly have $\leqslant$ by the previous lemma. Let $k = \mathrm{RC}(G, X \coprod Y)$, and let I, J be two n-tuples of elements of $\Omega = X \coprod Y \coprod Y$ that are k-related. We show they are n-related.

For clarity, let Y_0 and Y_1 denote the two copies of Y here, so $\Omega = X \coprod Y_0 \coprod Y_1$. The canonical bijection $Y_0 \to Y_1$ will be written $y \mapsto y'$.

Re-arranging the indices if necessary, we may assume that I is of the form $I = (x_1, \dots, x_s, y'_1, \dots, y'_t)$ for $x_i \in X \coprod Y_0$, and $y'_i \in Y_1$. Since I and J are 1-related, we can write $J = (z_1, \dots, z_s, w'_1, \dots, w'_t)$ with $z_i \in X \coprod Y_0$ and $w'_i \in Y_1$.

Consider tuples $I_0 = (x_1, \dots, x_s, y_1, \dots, y_t)$ and $J_0 = (z_1, \dots, z_s,\ w_1, \dots, w_t)$, whose entries are in $X \coprod Y_0$. Inspection reveals that they are k-related (the bijection $y \mapsto y'$ is G-equivariant). So they must be n-related. It follows that I and J are n-related. □

So, when studying the complexity of a non-transitive action, we only need one copy of each "type" of orbit. The lemma shows that repetitions do not affect the complexity.

Lemma 2.7. — *Let G act on $X \coprod Y$. Suppose the action on X is either free (semi-regular) or trivial. Then*

$$\mathrm{RC}\Big(G, X \coprod Y\Big) = \mathrm{RC}(G, Y)\,.$$

Proof. — We treat the first case, leaving trivial actions for the reader as an exercise. From the previous lemma, or alternatively by an obvious induction, we may as well assume that the action on X is regular, so it is in particular binary.

We only need to show $\leqslant$. Let I, I' be n-tuples of elements of $X \coprod Y$, say $I = (x_1, \dots, x_s, y_1, \dots y_t)$ and $I' = (x'_1, \dots, x'_s, y'_1, \dots y'_t)$ in obvious notation. Assume that I, I' are k-related, where $k \geqslant 2$ is the complexity of Y. There is nothing to prove if $s = 0$.

As the action on X is binary, we may as well assume that $x'_i = x_i$ for all i. Further, suppose $g \in G$ is such that $(x_1, y_j)^g = (x_1, y'_j)$. As the action is free, we must have $g = 1$ and $y'_i = y_i$, so $I = I'$. □

We shall see later that the following corollary applies in particular to the alternating groups.

Corollary 2.8. — *Let G be a group whose only transitive, binary actions are the regular one and the trivial one. Then any binary action of G is a disjoint union of copies of the regular action, and copies of the trivial action.*

2.3. **Another criterion for binary actions.** We start with a lemma adapted from [6]. In the lemma G acts on Ω with $\Lambda \subset \Omega$. We write G_Λ for the setwise stabilizer of Λ, $G_{(\Lambda)}$ for the pointwise stabilizer of Λ and $G^\Lambda = G_\Lambda / G_{(\Lambda)}$ for the permutation group induced by G on Λ.

Lemma 2.9. — *Suppose there is a subset $\Lambda \subset \Omega$ with more than 2 elements, and with the following properties: there is a permutation τ of Λ with $\tau \notin G^\Lambda$ and there are permutations $\eta_1, \eta_2, \dots, \eta_r$ of Λ such that:*

(1) *$g_i := \tau\eta_i \in G^\Lambda$,*
(2) *the support of τ and that of η_i are disjoint, for all i,*
(3) *every $\lambda \in \Lambda$ is fixed by at least one η_i.*

Then the action of G on Ω is not binary.

Proof. — Let $\lambda_1, \dots, \lambda_t$ be the elements of Λ, and consider the tuples $I = (\lambda_1, \dots, \lambda_t)$ and $J = (\lambda_1^\tau, \dots, \lambda_t^\tau)$. The assumption that $\tau \notin G^\Lambda$ means that there is no element of G taking I to J, and so it is enough to show that these are 2-related.

Without loss of generality, let us look at the first two entries in the tuples. There are 4 cases. If $\lambda_1^\tau = \lambda_1$ and also $\lambda_2^\tau = \lambda_2$, the identity takes (λ_1, λ_2) to $(\lambda_1^\tau, \lambda_2^\tau)$. If $\lambda_1^\tau = \lambda_1$ but $\lambda_2^\tau \neq \lambda_2$, then λ_2 and λ_2^τ are in the support of τ, so they are not in the support of η_j for all j. Now choose η_i fixing λ_1. Thus η_i takes $(\lambda_1^\tau, \lambda_2^\tau)$ to itself, and the element $g_i = \tau\eta_i \in G^\Lambda$ takes (λ_1, λ_2) to $(\lambda_1^\tau, \lambda_2^\tau)$. There is another symmetric case.

Finally, suppose $\lambda_1^\tau \neq \lambda_1$ and $\lambda_2^\tau \neq \lambda_2$. All four points mentioned are thus in the support of τ, so not in the support of any η_i, or in other words they are fixed by every η_i. So $g_1 = \tau\eta_1$, for example, does the job. □

In the coming example, and in the rest of the paper, we use the notion $\mathrm{Fix}(g)$ for the set of fixed points of $g \in G$ in some action which is implicit from the context.

Example 2.10. — Again let G act on Ω. Suppose g and h are two elements of G which commute, and let

$$\Lambda = \mathrm{Fix}(g) \cup \mathrm{Fix}(h) \cup \mathrm{Fix}(gh^{-1}).$$

(The union might not be disjoint.) Then Λ is stable under the actions of g and h, because these two commute.

By construction g and h induce the same permutation τ on $\mathrm{Fix}(gh^{-1})$; extend it to be the identity outside of $\mathrm{Fix}(gh^{-1})$, so we can look at it as a permutation of Λ. Next, let η_1 be the permutation induced by g on $\mathrm{Fix}(h)$, again viewed as a permutation of Λ, and symmetrically let η_2 be the permutation induced by h on $\mathrm{Fix}(g)$, viewed as a permutation of Λ.

Let us check whether the conditions of the lemma are met. First, the supports of τ and η_i are certainly disjoint: by definition η_1 only moves points that are fixed by h and so also by τ if these points are in $\mathrm{Fix}(gh^{-1})$, which is where τ could be nontrivial. Similarly for η_2.

Next, the permutation induced on Λ by g is $\tau\eta_1$, so $\tau\eta_1 \in G^\Lambda$, and similarly for $\tau\eta_2$. We have conditions (1) and (2).

As for condition (3), take $\lambda \in \Lambda$. If λ lies neither in $\mathrm{Fix}(g)$ nor $\mathrm{Fix}(h)$, then it is fixed by both η_1 and η_2, by their definition. If $\lambda \in \mathrm{Fix}(g)$, then either $\lambda \in \mathrm{Fix}(gh^{-1})$ (in which case it is fixed by h as well, so by everything), or $\lambda \notin \mathrm{Fix}(gh^{-1})$, so it is fixed by τ by definition and so, being fixed by $h = \tau\eta_2$, it must be fixed by η_2.

We have the three conditions of the lemma. The conclusion is that *if we can only prove that $\tau \notin G^\Lambda$, and that Λ has more than two elements, then the action will not be binary.*

The integer $|\mathrm{Fix}(g)|$ will be called the *fixity* of $g \in G$. For a prime p we s ay that g, an element of order p, has *maximal p-fixity* when no element of G of order p fixes more points than g in the action under scrutiny. Also, the next statement uses the notation $\mathrm{Fix}(K)$ for the set of common fixed points of all the elements of the subgroup K of G.

Corollary 2.11. — *Suppose that G acts on the set of cosets of a subgroup H, that p is a prime, and that there exists K an elementary-abelian subgroup of G of order p^2 satisfying the following properties:*

(1) *$K = \langle g, h\rangle$ for some p-elements of maximal p-fixity, $g, h \in G$;*
(2) *$\langle g\rangle$, $\langle h\rangle$ and $\langle gh^{-1}\rangle$ are conjugate subgroups of G;*
(3) *$K \cap H = \langle g\rangle$.*

Then the action of G on the cosets of H is not binary.

Proof. — Put $\Omega = (G : H)$, and let α denote H as an element of Ω, so that the stabilizer of α is H. Thus, we see that $\alpha \notin \mathrm{Fix}(K)$ but, since $K \cap H = \langle g \rangle$, we certainly have $\alpha \in \mathrm{Fix}(g)$. The rest of the argument relies entirely on the fact that $|\mathrm{Fix}(K)| < |\mathrm{Fix}(g)|$.

As in Example 2.10, we introduce $A = \mathrm{Fix}(g)$, $B = \mathrm{Fix}(h)$ and $C = \mathrm{Fix}(gh^{-1})$, and we put

$$\Lambda = A \cup B \cup C\,.$$

Here we have $A \cap B = A \cap C = B \cap C = A \cap B \cap C = \mathrm{Fix}(K)$.

We use the fact that $\langle g \rangle$, $\langle h \rangle$ and $\langle gh^{-1} \rangle$ are conjugate subgroups of G. Thus, there is an integer r such that

$$|\mathrm{Fix}(g)| = |\mathrm{Fix}(h)| = \left|\mathrm{Fix}(gh^{-1})\right| = r.$$

Put $r' = |\mathrm{Fix}(K)|$, so $r' < r$ by hypothesis. We deduce from the calculations above that the size of Λ is $3r - 3r' + r' = 3(r - r') + r' > 2$.

Now let τ, η_1 and η_2 be as in Example 2.10, and let us prove that the permutation τ is not induced by an element $x \in G$; this will suffice. Assume for a contradiction that x exists. As τ is not the identity ($\mathrm{Fix}(gh^{-1})$ being nonempty and not equal to $\mathrm{Fix}(g)$), we see that the order of x is divisible by p. Thus some power of x, say $s \in G$, is a p-element and fixes at least as many points as x. By definition, τ is the identity on $\Lambda - C$, and it is also the identity on $\mathrm{Fix}(K)$, so in the end we see that τ fixes all the elements of $A \cup B$, as does x. However, the size of $A \cup B$ is $r + (r - r') > r$, which means that s is a p-element of G that fixes more elements of Ω than g. This is a contradiction and we are done. □

2.4. **The graphs on conjugacy classes.** Let us recast the above criteria in terms of certain graphs and their connected components. Let $\mathcal{C}$ be a conjugacy class of p-elements in G. We define $\Gamma(\mathcal{C})$ to be the graph whose vertices are the elements of $\mathcal{C}$, and with an edge between $x, y \in \mathcal{C}$ if and only if

(1) x and y commute,
(2) either $xy^{-1} \in \mathcal{C}$ or $yx^{-1} \in \mathcal{C}$.

When $g \in \mathcal{C}$, the *component group of g in* $\Gamma(\mathcal{C})$ is the subgroup of G generated by all the elements in the connected component of $\Gamma(\mathcal{C})$ containing g. The *component groups of* $\Gamma(\mathcal{C})$ are the various groups thus obtained by varying g; they are all conjugate in G. The next corollary asserts that, in the case of transitive, binary actions, each stabilizer must contain a component group.

Remark 2.12. — This result, which is central in our developments and has already been cited in the literature before publication, was numbered 2.16 in the arxiv version of the present paper.

Corollary 2.13. — *Let G act on the set of cosets of a subgroup H, and assume that the action is binary. Let p be a prime dividing $|H|$, and let $\mathcal{C}$ be a conjugacy class of p-elements of G of maximal p-fixity. Then for any $g \in \mathcal{C} \cap H$, the component group of g in $\Gamma(\mathcal{C})$ is contained in H.*

In particular, suppose that $\Gamma(\mathcal{C})$ is connected and that G is simple. Then H must contain the subgroup generated by $\mathcal{C}$, which is normal, and we conclude in this situation that $H = G$.

Proof. — We show that $\mathcal{C} \cap H$ and $\mathcal{C} \smallsetminus H$ are not connected to each other in the graph $\Gamma(\mathcal{C})$. Indeed, suppose that $g \in \mathcal{C} \cap H$, $h \in \mathcal{C} \setminus H$ and that g and h are connected by an edge in $\Gamma(\mathcal{C})$. Then $K = \langle g, h \rangle$ is an elementary-abelian p-subgroup of G satisfying all of the suppositions of Corollary 2.11. We conclude that the action of G is not binary, a contradiction. □

3. Alternating groups

In this section we prove Theorem 1.2, which was stated in the introduction, and whose notation we borrow.

Corollary 2.8 allows us to assume that the action of G is transitive. So we consider the action of G on the cosets of a subgroup H; we suppose that $H \neq 1$ and our aim is to prove that $H = G$.

The first step of the proof will show that $H = G$ if we know that the order of H is even – this step will be completed at the end of the next subsection. After this, we shall show that assuming H to have odd order leads to a contradiction.

3.1. Involutions.

Here we collect facts about the graphs $\Gamma(\mathcal{C})$ when $\mathcal{C}$ is a conjugacy class of involutions in A_n, reaching a complete description of the connected components. The first step of the proof of Theorem 1.2 will then be trivial to complete, thanks to Corollary 2.13.

A *quad* is a permutation of the form $(ab)(cd)$, with a, b, c, d distinct. It will be useful, for what follows, to keep in mind that there are just three quads with support $\{a, b, c, d\}$, which are the non-identity elements in a Klein group which acts regularly on $\{a, b, c, d\}$.

When $q = (ab)(cd)$ and $q' = (ab)(c'd')$, with $\{c, d\} \cap \{c', d'\} = \emptyset$, we say that the quads q and q' are *related by the exchange* $(cd) \leftrightarrow (c'd')$.

Lemma 3.1. — *Let $\mathcal{C}$ be a conjugacy class of involutions in S_n. Let $s, t \in \mathcal{C}$. Then there is an edge in $\Gamma(\mathcal{C})$ between s and t if and only if there is an integer k, quads $q_1, \ldots, q_k$ with disjoint supports satisfying $s = q_1, \ldots, q_k$, and quads $q'_1, \ldots, q'_k$ with disjoint support satisfying $t = q'_1, \ldots, q'_k$, such that for every i we have either:*

1. *q_i and q'_i have the same support and are distinct, or*
2. *q_i and q'_i are related by the exchange $(x_i y_i) \leftrightarrow (u_i v_i)$, where x_i and y_i (resp. u_i and v_i) are fixed by t (resp. by s), and all the elements x_i, y_i, u_i, v_i thus introduced as i varies are distinct.*

In particular, if the size of the support of s is not divisible by 4, then there is no edge in $\Gamma(\mathcal{C})$ at all.

Proof. — Suppose there is an edge between s and t. The group $K = \langle s, t \rangle$ is a Klein group, and we may write the disjoint union

$$\{1, 2, \ldots, n\} = A \cup B \cup C \cup D \cup E$$

according to the types of orbits of K. More precisely, let A be the set of elements with trivial stabilizer, so that the action of K on A is free (semiregular). Each orbit of K on A contains just 4 elements, with s and t acting on them as distinct quads. In other words, the restriction of s to A is given by a product $q_1, \ldots, q_a$ of quads with disjoint supports, while t is given by $q'_1, \ldots, q'_a$, and q_i has the same support as q'_i.

The set E will be that of fixed points of K. Now let B resp. C resp. D be the set of elements whose stabilizer is $\langle s\rangle$ resp. $\langle t\rangle$ resp. $\langle st\rangle$. The action of t on B is given by a product $\beta_1,\dots,\beta_b$ where each β_i is a transposition (that is $\beta_i=(xy)$ for some $x,y\in B$), while s acts trivially on B. Similarly, the action of s on C is given by $\gamma_1,\dots,\gamma_c$ while t acts trivially on C, and finally st acts trivially on D, on which s and t both act as $\delta_1,\dots,\delta_d$. Restricting to $B\cup C\cup D$, we may write

$$s=\gamma_1,\dots,\gamma_c\,\delta_1,\dots,\delta_d\,,\quad t=\beta_1,\dots,\beta_b\,\delta_1,\dots,\delta_d\,,\quad st=\gamma_1,\dots,\gamma_c\,\beta_1,\dots,\beta_b\,.$$

Using that s, t and st are conjugate to one another, we conclude that $b=c=d=\ell$, say. Consider now the quad $\delta_i\gamma_i$ for $1\leqslant i\leqslant\ell$, as well as the quad $\delta_i\beta_i$. If $\gamma_i=(x_iy_i)$ and $\beta_i=(u_iv_i)$, then the quads are related by the exchange $(x_iy_i)\leftrightarrow(u_iv_i)$. This proves the existence of the quads as announced.

For the converse, one simply works backwards. □

When a conjugacy class $\mathcal{C}$ of S_n has edges in its graph, it must therefore be contained in A_n rather than just S_n. Moreover, $\mathcal{C}$ then still forms a conjugacy class of A_n.

Example 3.2. — Let $\mathcal{C}$ denote the conjugacy class of a single quad in A_n (or S_n, this is the same). Assuming that $n\geqslant 6$, we show that $\Gamma(\mathcal{C})$ is connected. Let us write $s\equiv t$ when s and t are connected by an edge. We can begin by computing $(12)(34)\equiv(14)(23)\equiv(14)(56)\equiv(16)(45)\equiv(23)(45)$, by four applications of the last lemma.

Swapping 1 and 2 in this computation (or in other words, conjugating everything by (12)), we get a path between $(21)(34)=(12)(34)$ and $(13)(45)$. Swapping 1 and 3 gives a path between $(32)(14)\equiv(12)(34)$ and $(21)(45)$, and finally, swapping 1 and 4 produces a path between $(42)(31)\equiv(12)(34)$ and $(23)(15)$.

We have shown that, for every subset Λ of $\{1,2,3,4,5\}$ of cardinality 4, there is a path connecting $(12)(34)$ to a quad q with support equal to Λ. Since all quads with the same support are connected to each other, we conclude that if q is a quad with support contained in $\{1,2,3,4,5\}$, then there is a path from $(12)(34)$ to q.

Now more generally, suppose the support of q is $\{a,b,c,d\}$ with $a<b<c<d$, and that $d\geqslant 6$. Then there are two elements x and y with $1\leqslant x<y<d$ which are fixed by q. We have $q\equiv(ab)(cd)\equiv(ab)(xy)$, and the maximal element in the support of $(ab)(xy)$ is less than d. Iterating, we have a path between q and a quad whose support is in $\{1,2,3,4,5\}$ as above. We have shown the existence of a path between $(12)(34)$ and any quad.

We note that this result does not hold when $n=5$. In this case the graph $\Gamma(\mathcal{C})$ is made up of five disjoint triangles, each corresponding to three quads with a shared fixed point.

The next lemma provides a statement in which only one quad is modified at a time (note that, in the notation of Lemma 3.1, the quads q_i and q_i' are distinct for all i). The arguments in the previous example will then generalize almost immediately.

Lemma 3.3. — *Let $\mathcal{C}$ be a conjugacy class of involutions in A_n, and let*

$$s=q_1,\dots,q_k\quad\text{and}\quad t=q_1'q_2,\dots,q_k$$

be elements of $\mathcal{C}$. Assume that $q_1,\dots,q_k$ (resp. $q_1',q_2,\dots,q_k$) are quads with disjoint supports. Assume, moreover, that q_1' is any quad such that either q_1 and

q_1' have the same support, or q_1 and q_1' are related by an exchange $(xy) \leftrightarrow (uv)$, where x and y are fixed by t, and u and v are fixed by s.

Then s and t belong to the same connected component of $\Gamma(\mathcal{C})$.

Proof. — Of course there is nothing to prove if $q_1' = q_1$, so assume $q_1' \neq q_1$. Let $s_0 = s$ and $s_3 = t$. We shall introduce $s_1, s_2 \in \mathcal{C}$ such that there is an edge between s_j and s_{j+1} for $j = 0, 1, 2$.

Let $i > 1$ and let $q_i = (ab)(cd)$. Put $q_i' = (ac)(bd)$, $q_i'' = (ad)(bc)$. In this way, the quads q_i, q_i' and q_i'' are the three distinct quads with support $\{a, b, c, d\}$.

When $i = 1$, we have already q_1 and q_1'; if $q_1' = (ab)(cd)$, we introduce $q_1'' = (ad)(bc)$, so that q_i' and q_i'' are distinct, of the same support.

Now let

$$s_1 = q_1'q_2', \ldots, q_k' \quad \text{and} \quad s_2 = q_1''q_2'', \ldots, q_k''.$$

Applying Lemma 3.1 several times shows the existence of an edge between s_j and s_{j+1}, for $j = 0, 1, 2$. Note that, for $i > 0$, the quads involved are q_i, q_i', q_i'', q_i, which all have the same support, while for $i = 0$, the quads are q_1, q_1', q_1'', q_1', the first two either have the same support or are related by an exchange of fixed points, while the support does not change afterwards. □

Proposition 3.4. — *Let $\mathcal{C}$ be a conjugacy class of involutions in A_n. Suppose that the elements of $\mathcal{C}$ are products of k quads with disjoint support (or equivalently that the support of an element of $\mathcal{C}$ is a set of size $4k$). Then:*

(1) *if $n \neq 4k+1$, the graph $\Gamma(\mathcal{C})$ is connected,*
(2) *if $n = 4k+1$, the graph $\Gamma(\mathcal{C})$ has n connected components. One of these is $\mathcal{C} \cap A_{n-1}$.*

Proof.

(1). — Suppose first that $n = 4k$. Let $s \in \mathcal{C}$. We say that s *involves* the transposition τ if, when we write s as the product of distinct transpositions of disjoint support, τ occurs in the product. The element s involves $(1a)$ for some a; if $a \neq 2$, then s also involves $(2b)$ where $b \neq 1$. In this case $s = (1a)(2b)q_2 \cdots q_k$ where q_i is a quad for $i > 1$. By the last lemma, we have a path from s to $(12)(ab)q_2, \ldots, q_k$.

Thus we may in fact suppose that s involves (12). Continuing, we can force the presence of (34) and then (56) and so on, until we have reached $(12)(34)\cdots(4k-1, 4k)$, following a path starting from s.

Now suppose alternatively that $n \geqslant 4k+2$. Let $s \in \mathcal{C}$, and let the support of s be $\{a_1, a_2, \ldots, a_{4k}\}$ with $a_i < a_{i+1}$. The argument of the previous paragraph applies, and gives a path between s and $t = (a_1a_2)(a_3a_4)\ldots(a_{4k-1}a_{4k})$. Let F denote the set of fixed points of t and $A = F \cup \{a_1, a_2, a_3, a_4\}$. Then A is left stable by the action of t, and certainly $\{1, 2, 3, 4\} \subset A$; also note $|A| \geqslant 6$ by the assumption on n. If $q = (a_1a_2)(a_3a_4)$ is the quad induced on A by t, then the computations of Example 3.2 show that there is a sequence of moves from q to $(12)(34)$; that is, there is a sequence of quads in A, say $q_1 = q, q_2, \ldots, q_\ell = (12)(34)$, such that the last lemma applies between q_iu and $q_{i+1}u$, where $u = (a_5a_6)\ldots(a_{4k-1}a_{4k})$, for each index i. This shows the existence of a path between $t = q_1u$ and $q_\ell u = (12)(34)(a_5a_6)\ldots(a_{4k-1}a_{4k})$. Iterating, we have a path leading to $(12)(34)\ldots(4k-1, 4k)$. □

(2). — Now suppose $n = 4k+1$, so that if $s \in \mathcal{C}$, then s has just one fixed point a with $1 \leqslant a \leqslant n$. Any permutation commuting with s must leave a fixed. Suppose $a = n$ to start with. Then the connected component of $\Gamma(\mathcal{C})$ containing s only comprises involutions of A_{n-1}, and by (1) this connected component is in fact $\mathcal{C} \cap A_{n-1}$. Similarly, each other choice of a gives a connected component. □

Having worked out these connected components, we return to the proof of Theorem 1.2, with the notation introduced right after its statement.

So suppose that H has even order, and let $\mathcal{C}$ be a conjugacy class of involutions of maximal 2-fixity. By Corollary 2.13, we know that H contains a component group of $\Gamma(\mathcal{C})$. Using the fact that we are assuming $n \geqslant 6$ and that A_n is simple for $n \geqslant 5$, Proposition 3.4 implies that the component groups must be all of A_n when $n = 4k$ or $n \geqslant 4k+2$, so that $H = G$ in this case.

Likewise, when $n = 4k+1$ the same proposition guarantees that $A_{n-1} \subset H$. The natural action of A_n on $\{1, \ldots, n\}$ is obviously primitive, so A_{n-1} is maximal in A_n, and thus we have either $H = A_n$ or $H = A_{n-1}$. In the latter case however, the action of G on the cosets of H is nothing but the natural action itself, which is not binary (Example 2.1). This contradiction shows that $H = G$ in all cases when H has even order.

3.2. **When H is not a 3-group.** We continue the proof of Theorem 1.2, now assuming that the order of H is odd, and we seek a contradiction. First, we assume the existence of a prime number $p > 3$ which divides the order of H (in other words, we exclude the case when H is a 3-group).

We caution the reader that, in the arguments below, all references to cycle structure are made with respect to the natural action of A_n, while questions of fixity are related to the action on $(G : H)$.

Lemma 3.5. — *The group H contains p-cycles.*

Proof. — Let $\mathcal{C}$ be a conjugacy class of p-elements of G of maximal p-fixity, in the action of G on the cosets of H. Certainly we can find $g \in \mathcal{C} \cap H$.

There is nothing to prove if the elements of $\mathcal{C}$ are p-cycles, so assume that $g = c_1 c_2, \ldots, c_k$ where $k > 1$ and each c_i is a p-cycle. Note that this means that $\mathcal{C}$ contains all permutations which can be written as the product of k disjoint p-cycles. Let $x \in \{2, 3, \ldots, p-2\}$ (this is possible as $p > 3$). Now introduce

$$h = c_1^x c_2^{-1}, \ldots, c_k^{-1} \in \mathcal{C}\,.$$

We have $[g, h] = 1$ and $gh^{-1} = c_1^{1-x} c_2^2, \ldots, c_k^2 \in \mathcal{C}$, and we see that g and h are connected by an edge in $\Gamma(\mathcal{C})$. By Corollary 2.13, we know that $h \in H$. However, we have

$$gh = c_1^{1+x} \in H$$

and we are done. □

It will be useful to recall a few general facts about p-cycles. It seems more convenient to provide a direct argument rather than refer to the literature, and the following proposition has benefited from a conversation on MathOverflow (to be more precise, a question asked by Robinson and an answer from Müller [11]). The fourth point of the proposition is of a somewhat different nature.

Proposition 3.6.

(1) *Let K be a subgroup of A_p, where p is prime, which is generated by two p-cycles. If K is not abelian, then the order of K is even.*
(2) *Let $s, t \in A_n$ be two cycles with supports S and T. Assume that $S \cap T$, $S \smallsetminus T$ and $T \smallsetminus S$ are all nonempty. Then the group generated by s and t has even order.*
(3) *Let K be a subgroup of A_n of odd order, and let $s, t \in K$ be p-cycles, where p is a prime. Then either the supports of s and t are disjoint, or $\langle s \rangle = \langle t \rangle$. In particular, s and t commute.*
(4) *Let p be an odd prime, and let s and t be two p-cycles. Then $\langle s \rangle$ and $\langle t \rangle$ are conjugate in A_n.*

Proof.

(1). — First, we note that the action of K on $\{1, \dots, p\}$ is obviously primitive. We will deduce that K is simple. Indeed, if N is a nontrivial, normal subgroup of K, then it must be transitive (by primitivity), and in particular its order must be a multiple of p. Hence it contains a Sylow p-subgroup of K (since the order of such a subgroup is not divisible by p^2), and it follows that N contains all the p-cycles in K, hence $N = K$.

We could rely on the Feit–Thompson theorem to argue that, if the order of K were to be odd, then K would be solvable as well as simple, hence K would have to be abelian. However, we can avoid using such a strong result and appeal to Burnside's theorem on transitive permutation groups of prime degree p: this asserts that K must be solvable or 2-transitive. Since K is simple, if K is not abelian, then we must have that K is 2-transitive, and thus its order is certainly even. □

(2). — Pick any $x \in S \smallsetminus T$; pick $y \in T \smallsetminus S$ such that $y^t \in S$; and finally, pick $z \in S \cap T$ such that $z^t \in T \smallsetminus S$.

There is an integer i such that $x^{s^i} = z$, and of course $y^{s^i} = y$. Apply t and obtain that $x^{s^i t} \in T \smallsetminus S$ while $y^{s^i t} \in S$. Then pick an integer j such that $y^{s^i t s^j} = x$, and observe that $x^{s^i t s^j} = x^{s^i t} \in T \smallsetminus S$. Finally, pick an integer k so that $x^{s^i t s^j t^k} = y$, and note that $y^{s^i t s^j t^k} = x^{t^k} = x$.

The permutation $g = s^i t s^j t^k \in \langle s, t \rangle$ thus exchanges x and y, so its order must be even.

(3). — If the supports of s and t are not disjoint, then they must be equal, by (2). In this case, by (1), s and t must commute. It is then elementary that $\langle s \rangle = \langle t \rangle$.

(4). — First we show that, for any p-cycle s, there exists a permutation τ of signature -1 such that s^τ is a power of s. For this, it is notationally more convenient to consider $s = (0, 1, \dots, p-1)$ in the symmetric group of the set $\{0, 1, \dots, p-1\}$. For any integer k, we have

$$s^k = (0, k, 2k, \dots, (p-1)k)$$

where the entries are understood modulo p. Now pick for k a generator of the cyclic group $(\mathbb{Z}/p\mathbb{Z})^\times$, and let τ be the permutation defined by $i^\tau = ki$ (modulo p). Then $s^\tau = s^k$, but τ is just the cycle $(1, k, k^2, \dots, k^{p-2})$ of length $p-1$, so the signature of τ is -1, as claimed.

We turn to the proof of statement (4) itself. Certainly there exists $\sigma \in S_n$ with $s^\sigma = t$. There is nothing to prove if $\sigma \in A_n$. If the signature of σ is -1, it suffices to pick a permutation τ with signature -1 which satisfies $t^\tau = t^k$ for some k (such a permutation exists by the above paragraph), so that $\sigma\tau \in A_n$ and $s^{\sigma\tau} = t^k$. Thus $\langle s\rangle^{\sigma\tau} = \langle t\rangle$. □

We return to the proof of Theorem 1.2 and recall that $p > 3$ is a prime dividing $|H|$. As the order of H is assumed to be odd, we deduce from Proposition 3.6 (3) the existence of p-cycles $c_1, \dots, c_s$ with disjoint supports such that any p-cycle in H is a power of some c_i. The subgroup $E = \langle c_1, \dots, c_s\rangle \subset H$ is elementary abelian and normal.

We shall use Lemma 2.4 to prove that the action of G on the cosets of H is not binary, which is the required contradiction.

We may as well assume that $c_1 = (1, 2, \dots, p)$, and we put $h_1 = c_1$. Consider $\sigma = (p-2, p-1, p) \in A_n$ and

$$h_2 = h_1^\sigma = (1, 2, \dots,\ p-3,\ p-1,\ p,\ p-2).$$

It is easy to see that

$$h_1 h_2 = (2, 4, 6, \dots, p-3, 1, 3, 5, \dots,\ p-4, p-1, p-2, p)\,.$$

We put $h_3 = (h_1h_2)^{-1}$ so that $h_1h_2h_3 = 1$, and h_3 is a p-cycle. By (4) of Proposition 3.6, we may choose $\tau \in A_n$ so that h_1^τ is a power of h_3; moreover we can choose τ with support in $\{1, 2, \dots, p\}$ (by applying the proposition to A_p rather than A_n). Thus if we put $H_1 = H$, $H_2 = H^\sigma$ and $H_3 = H^\tau$, then $h_i \in H_i$ for $i = 1, 2, 3$, and H_i is the stabilizer of some coset of H in G.

Note that, since h_1 and h_2 are clearly not powers of each other, the same is true of h_1h_2 and so H_1, H_2 and H_3 are distinct.

We now apply (2) from Lemma 2.4. As we assume that we are dealing with a binary action, we conclude that it must be possible to pick $h_2' \in H_1 \cap H_2$ and $h_3' \in H_3$ such that $h_1h_2'h_3' = 1$.

Just as $H_1 = H$ has the normal subgroup $E_1 = E = \langle h_1, c_2, \dots, c_s\rangle$, the subgroup H_i has the normal subgroup $E_i = \langle h_i, c_2, \dots, c_s\rangle$, for $i = 2, 3$ (this remark uses the observation that for $i > 1$, we have $c_i^\sigma = c_i^\tau = c_i$). It follows that $H_1 \cap H_2$ normalizes $E_1 \cap E_2 = \langle c_2, \dots, c_s\rangle$, as well as E_1 and E_2 individually. If $\Lambda \subset \{1, 2, \dots, n\}$ denotes the (disjoint) union of the supports of the elements c_i for $1 \leqslant i \leqslant s$, we see that $H_1 \cap H_2$ preserves Λ but also $\Lambda \smallsetminus \{1, \dots, p\}$ – the latter being the union of the supports of the c_i's for $1 < i \leqslant s$. As a result, $H_1 \cap H_2$ preserves $\Delta = \{1, \dots, p\}$.

In particular, h_2' induces a permutation of Δ, and the latter must normalize both $\langle h_1\rangle$ and $\langle h_2\rangle$. However, we have the following lemma.

Lemma 3.7. — *Let N_i be the normalizer of $\langle h_i\rangle$ in S_p, for $i = 1, 2$. Then $N_1 \cap N_2$ is trivial for $p > 5$, and has order 4 for $p = 5$.*

We postpone the proof of the lemma and explain how we derive a contradiction. Indeed, as H, and so also h_2', has odd order, the lemma implies that h_2' is the identity on Δ. By inspection of the relation $h_1h_2'h_3' = 1$, we deduce that h_3' also preserves Δ and indeed that $h_3' = h_1^{-1}$ on Δ. Then h_3' is in the setwise stabilizer of Δ in H_3 and acts as a p-cycle on Δ; thus h_3' acts on Δ as a power of h_3. Since h_1^{-1} is clearly not a power of h_3 we obtain a contradiction.

This contradiction concludes the proof of Theorem 1.2 in the case under consideration, namely when H has odd order but is not a 3-group.

Proof of Lemma 3.7. — We give a proof for $p \geqslant 11$, as it allows for an easier exposition; the cases $p = 5$ and $p = 7$ can be worked out by direct computation (we have used a computer for this, for safety). Again it is more convenient to work in the symmetric group of $\mathbb{Z}/p\mathbb{Z} = \{0, 1, \ldots, p-1\}$, and so we consider

$$h_1 = (0, 1, \ldots, p-1), \quad \sigma = (p-3, p-2, p-1),$$

and

$$h_2 = h_1^\sigma = (0, 1, \ldots, p-4,\ p-2, p-1, p-3).$$

We pick a permutation g which normalizes both $\langle h_1 \rangle$ and $\langle h_2 \rangle$, and we wish to show that $g = 1$.

It is classical that the normalizer of $\langle h_1 \rangle$ consists of all permutations g with $x^g = kx + t$ for $x \in \mathbb{Z}/p\mathbb{Z}$, where $k \in (\mathbb{Z}/p\mathbb{Z})^\times$ and $t \in \mathbb{Z}/p\mathbb{Z}$. With this notation, we have $h_1^g = h_1^k$.

Now let $\ell \in (\mathbb{Z}/p\mathbb{Z})^\times$ be such that $h_2^g = h_2^\ell$. First we show that $k = \ell$. For this, we put $s = h_2^g$ and study the values of the form $x^s - x$ for $0 \leqslant x < p$. More precisely, put

$$S = \{x : x^s - x = k \bmod p\}, \quad T = \{x : x^s - x = \ell \bmod p\};$$

we shall show that $S \cap T \neq \emptyset$. On the one hand, for $x = y^g$ with $0 \leqslant y < p-4$, we have

$$x^s - x = (y^{h_2})^g - y^g = (y+1)^g - y^g = k\,.$$

And so the size of S is at least $p-4$. On the other hand, we have $s = h_2^\ell$. It is obvious that, if $0 \leqslant x \leqslant p-4$ and $0 \leqslant x + \ell \leqslant p-4$, then $x^{h_2^\ell} = x + \ell$; this implies that, for the same values of x and for $x+\ell > p-1$, we have $x^{h_2^\ell} = x+\ell$ modulo p. We have found that $x^s - x = \ell$ modulo p for all but 6 values of x, namely, the exceptions could occur when $x \in \{p-3, p-2, p-1\}$ or when $x + \ell \in \{p-3, p-2, p-1\}$. In other words the size of T is no less than $p-6$. We see that S must intersect T nontrivially, lest we should conclude that $p \leqslant 10$. We have proved that $k = \ell$ modulo p.

Next we write $(h_1^k)^{\sigma^g} = (h_1^g)^{\sigma^g} = (h_1^\sigma)^g = h_2^g = h_2^k = (h_1^\sigma)^k = (h_1^k)^\sigma$. In particular from $(h_1^k)^{\sigma^g} = (h_1^k)^\sigma$ we see that $\sigma^g\sigma^{-1}$ centralizes the p-cycle h_1^k, and so also h_1 itself. However, we have recalled the description of the normalizer of $\langle h_1 \rangle$, from which it follows that the centralizer of h_1 is $\langle h_1 \rangle$. As σ is a 3-cycle, we see that $\sigma^g\sigma^{-1}$ moves at most 6 points, and so it cannot be a p-cycle with $p \geqslant 7$. The only element in $\langle h_1 \rangle$ which is not a p-cycle is the identity, so we conclude that $\sigma^g = \sigma$.

Thus g preserves the support of σ, and the permutation g_0 induced by g on this support is a power of σ. Consider the possibility $g_0 = \sigma$. This leads to the equations

$$\begin{cases} k(p-3) + t = p-2 \\ k(p-2) + t = p-1 \\ k(p-1) + t = p-3. \end{cases}$$

which have no solutions $k, t \in \mathbb{Z}/p\mathbb{Z}$ unless $p = 3$. Similarly, $g_0 = \sigma^{-1}$ leads to a contradiction. There remains only $g_0 = 1$. Writing the associated system of equations shows readily that $k = 1$ and $t = 0$, so that $g = 1$. □

3.3. **When H is a 3-group.** We finish the proof of Theorem 1.2 in the remaining case, that is, when $G = A_n$ acts on the cosets of a subgroup H which is a non-trivial 3-group. We asssume that the action is binary and look for a contradiction.

In the course of the proof, we shall rely on the following lemma (which we only need for $p = 3$ of course):

Lemma 3.8. — *Let p be an odd prime, and let $k \geqslant 2$. Let $\mathcal{C}$ denote the conjugacy class, in the group A_{pk}, containing all products of k different p-cycles with disjoint supports. Suppose that the component groups of $\Gamma(\mathcal{C})$ have even order. Then for all $\ell \geqslant k$ and all $n \geqslant p\ell$, the component groups of $\Gamma(\mathcal{C}')$ have even order, where $\mathcal{C}'$ is the conjugacy class, in the group A_n, of a product of ℓ different p-cycles with disjoint supports.*

Proof. — By induction it is enough to prove this for $\ell = k + 1$ and any $n \geqslant (k + 1)p$. Let c be any p-cycle with support disjoint from $\{1, 2, \ldots, pk\}$.

If $g, h \in \mathcal{C}$ are joined by an edge in $\Gamma(\mathcal{C})$, we put $g' = gc$ and $h' = hc^{-1}$. Then $g', h' \in \mathcal{C}'$, $[g', h'] = 1$, and $g'(h')^{-1} = (gh^{-1})c^2 \in \mathcal{C}'$ (since p is odd). Thus g' and h' are joined by an edge in $\Gamma(\mathcal{C}')$.

It follows readily that, if g, h are in the same component of $\Gamma(\mathcal{C})$, then gc and $hc^{\pm 1}$ are in the same component of $\Gamma(\mathcal{C}')$, for some sign ± 1. The result follows. □

Lemma 3.9. — *For $n \geqslant 9$, the subgroup H must contain 3-cycles.*

Proof. — Let $\mathcal{C}$ denote a conjugacy class of 3-elements of G of maximal 3-fixity and note that $H \cap \mathcal{C} \neq \emptyset$. There is nothing to prove if $\mathcal{C}$ contains 3-cycles, so assume that $\mathcal{C}$ is the conjugacy class of $c_1, \ldots, c_k$ where each c_i is a 3-cycle and $k > 1$.

It is easy to check that, when $\mathcal{C}$ is the conjugacy class of $(123)(456)(789)$ in A_9, then the graph $\Gamma(\mathcal{C})$ is connected. In particular, it has a single component group which is the whole of A_9. It follows from the previous lemma that, for $k \geqslant 3$, the component groups of $\Gamma(\mathcal{C})$ have even order. This is absurd, as H contains such a group by Corollary 2.13.

Thus we must only consider the possibility $k = 2$. In $\Gamma(\mathcal{C})$ we see that, if $n \geqslant 9$, then $h_1 = (123)(456)$ is connected to $h_2 = (123)(789)$ and h_2 is, in turn, connected to $h_3 = (123)(465)$. Thus h_1 and h_3 are in the same connected component of $\Gamma(\mathcal{C})$; moreover, the product of these two elements is (132). By Corollary 2.13, we see that H contains 3-cycles. □

Now we complete the proof of Theorem 1.2. Assume, first, that H contains a 3-cycle. We deduce again from Proposition 3.6 (3) (which holds for $p = 3$ as well) the existence of 3-cycles $c_1, \ldots, c_s$ with disjoint supports such that any 3-cycle in H is a power of some c_i. The subgroup $E = \langle c_1, \ldots, c_s \rangle \subset H$ is elementary abelian and normal. We will now assume that $s \geqslant 2$, leaving the case $s = 1$, which is similar but easier, to the reader.

We assume that $c_1 = (123)$ and $c_2 = (456)$. Put $\sigma = (23)(14)$, $\tau = (234)$ and define $h_1 = c_1$, $h_2 = c_1^\sigma = (432)$ and $h_3 = h_1^\tau = (134)$. We have $h_1 h_2 h_3 = 1$ and $h_i \in H_i$ for $i = 1, 2, 3$, where $H_1 = H$, $H_2 = H^\sigma$ and $H_3 = H^\tau$.

As above, we now apply Lemma 2.4(2). We conclude that it must be possible to pick $h_2' \in H_1 \cap H_2$ and $h_3' \in H_3$ such that $h_1 h_2' h_3' = 1$.

We note that $c_2^\sigma = (156)$ and $c_2^\tau = (256)$, while $c_i^\sigma = c_i^\tau = c_i$ for $i > 2$. Following the argument for $p > 3$, we arrive at the conclusion that h_2' stabilizes $\Delta = \{1, 2, 3, 4, 5, 6\}$, and that it must normalize both $\langle h_1, c_2 \rangle$ and $\langle h_2, c_2^\sigma \rangle$. A direct computation shows that the intersection of the normalizers in A_6 of these subgroups has order 4; as h_2' has odd order, we conclude that h_2' induces the identity of Δ. A similar reasoning and computation with h_3' shows that this permutation is also the identity on Δ.

This is absurd, however, as we see from the identity $h_1 h_2' h_3' = 1$, since h_1 is not the identity on Δ. This completes the proof of Theorem 1.2 in the case where H is a 3-group containing a 3-cycle. Lemma 3.9 then yields the proof provided $n \geqslant 9$.

We are left with the case when $n \in \{6, 7, 8\}$. If $n = 6$ and H contains a 3-cycle, then we are already done. If $n = 6$ and H does not contain a 3-cycle, then $H = \langle h \rangle$ where h is the product of two 3-cycles. But now the action of $G = A_6$ on the set of cosets of H is permutation isomorphic (via an exceptional outer automorphism) to the action of $G = A_6$ on the set of cosets of a subgroup H' generated by a 3-cycle, so the proof is complete in this case too.

Finally if $n \in \{7, 8\}$, then there exists $M \cong A_6$ such that $H < M < G$. We know that the action of M on the set of cosets of H in M is not binary and so the same is true for the action of G by [7, Lemma 1.7.2]. This final contradiction concludes the proof of Theorem 1.2 when $n \geqslant 6$.

References

[1] Gregory Cherlin. Sporadic homogeneous structures. In *The Gelfand Mathematical Seminars, 1996–1999. Dedicated to the memory of Chih-Han Sah*, pages 15–48. Birkhäuser, 2000.

[2] Gregory Cherlin. On the relational complexity of a finite permutation group. *J. Algebr. Comb.*, 43(2):339–374, 2016.

[3] Francesca Dalla Volta, Nick Gill, and Pablo Spiga. Cherlin's conjecture for sporadic simple groups. *Pac. J. Math.*, 297(1):47–66, 2018.

[4] Nick Gill and Pierre Guillot. The binary actions of simple groups with a single conjugacy class of involutions. *J. Group Theory*, 28(1):215–240, 2025.

[5] Nick Gill, Pierre Guillot, and Martin W. Liebeck. The binary actions of simple groups of Lie type of characteristic 2. *Pac. J. Math.*, 336(1-2):113–135, 2025.

[6] Nick Gill, Francis Hunt, and Pablo Spiga. Cherlin's conjecture for almost simple groups of Lie rank 1. *Math. Proc. Camb. Philos. Soc.*, 167(3):417–435, 2019.

[7] Nick Gill, Martin W. Liebeck, and Pablo Spiga. *Cherlin's conjecture for finite primitive binary permutation groups*, volume 2302 of *Lecture Notes in Mathematics*. Springer, 2022.

[8] Nick Gill and Pablo Spiga. Binary permutation groups: alternating and classical groups. *Am. J. Math.*, 142(1):1–43, 2020.

[9] Alistair H. Lachlan. Finite homogeneous simple digraphs. In *Proceedings of the Herbrand symposium (Marseilles, 1981)*, volume 107 of *Studies in Logic and the Foundations of Mathematics*, pages 189–208. North-Holland Publishing Co., 1982.

[10] Alistair H. Lachlan. Homogeneous structures. In *Proceedings of the International Congress of Mathematicians, Vols. 1, 2 (Berkeley, Calif., 1986)*, pages 314–321. American Mathematical Society, 1987.

[11] Peter Müller. Permutation groups containing non-commuting p-cycles, 2014. MathOverflow, `https://mathoverflow.net/a/172529/801`, (version: 2014-06-25).

[12] Joshua Wiscons. A reduction theorem for primitive binary permutation groups. *Bull. Lond. Math. Soc.*, 48(2):291–299, 2016.

Manuscript received 24th May 2024,
revised 14th February 2025,
accepted 22nd May 2025.

Nick GILL
School of Mathematics and Statistics, The Open University, Walton Hall, Milton Keynes, MK7 6AA, UK
nick.gill@open.ac.uk

Pierre GUILLOT
IRMA, 7 rue René Descartes, 67084 Strasbourg, France
guillot@math.unistra.fr