The binary actions of simple groups with a single conjugacy class of involutions

Nick Gill & Pierre Guillot

Abstract

We continue our investigation of binary actions of simple groups. In this paper, we demonstrate a connection between the graph $\Gamma(\mathcal{C})$ based on the conjugacy class $\mathcal{C}$ of the group G, which was introduced in our previous work, and the notion of a strongly embedded subgroup of G. We exploit this connection to prove a result concerning the binary actions of finite simple groups that contain a single conjugacy class of involutions.

§1. Introduction

Let G be a finite group acting on a set Ω. The *relational complexity* of the action is the minimum integer $k \geq 2$ such that the orbits of G on Ω^r, for any $r \geq k$, can be deduced from the orbits of G on Ω^k. (A more precise definition will be given in §2.) An action whose relational complexity is equal to 2 is called *binary*.

The relational complexity of a permutation group is, in principle at least, a formidable tool for the organization and classification of these objects; see, for instance, the introduction of [GG]. By this measure, the binary groups are the simplest permutation groups and they have received intense scrutiny in recent times [Che16, Wis16, GLS22].

Let us briefly summarise our understanding of the binary actions of finite groups. The *primitive* binary actions are completely classified – there are four families, one of which involves a family of almost simple permutation groups (the symmetric groups, in their natural actions). The programme to extend this classification to all *transitive* binary actions is currently focused on the transitive actions of almost simple groups.

In [GG], the transitive binary actions of the alternating groups are completely classified (it turns out that there are very few). In contrast, it is possible to exhibit a number of infinite families of transitive binary actions of the symmetric groups – we do not yet have a full classification of these. The binary actions of the other families of (almost) simple groups remain largely mysterious.

In the current paper we prove three results, all of which contribute to the classification of the binary actions of simple groups. The methods in the current paper build on those developed in [GG]. In particular, in that paper, we have introduced the graph $\Gamma(\mathcal{C})$, where $\mathcal{C}$ is a conjugacy class of a group G: its vertices are elements of $\mathcal{C}$, and 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 $\mathcal{C}$. We have shown how the study of the connected components of $\Gamma(\mathcal{C})$ sheds considerable light on the possible binary actions for G.

Our main result in the present paper concerns a simple group G with a single conjugacy class $\mathcal{C}$ whose elements are involutions. In this setting, there is a connection, thanks to Aschbacher [Asc73] between the connectivity properties of $\Gamma(\mathcal{C})$

and the presence in G of a *strongly embedded subgroup* (i.e. a proper subgroup H, of even order, such that $|H \cap H^g|$ is odd for all $g \in G \setminus H$).

We exploit the fact that the simple groups that contain a strongly embedded subgroup are all known, to prove the following.

Theorem 1.1. *Suppose that G is a simple group that contains a single conjugacy class of involutions, let H be a proper subgroup of G of even order and let Ω be the set of right cosets of H in G. Then the action of G on Ω is binary if and only if we are in one of the following situations:*

1. *$G = \mathrm{SL}_2(2^a)$ with $a \geq 2$ and H is a Sylow 2-subgroup of G;*
2. *$G = {}^2B_2(2^{2a+1})$ with $a \geq 1$ and H is the centre of a Sylow 2-subgroup of G;*
3. *$G = \mathrm{PSU}_3(2^a)$ with $a \geq 2$ and H is the centre of a Sylow 2-subgroup of G.*

For instance, for any prime power q, the group $\mathrm{PSL}_2(q)$ has a single conjugacy class of involutions, and Theorem 1.1 thus provides us with a lot of information about this group and its possible binary actions. To give an example of a complete classification for a given group, the second part of the paper classifies all transitive, binary actions of $\mathrm{PSL}_2(q)$, with q arbitrary and no restriction on the stabilizers. This also completes the picture for alternating groups A_n which were considered in [GG] for $n \geq 6$, since $A_5 \cong \mathrm{PSL}_2(4) \cong \mathrm{PSL}_2(5)$.

Theorem 1.2. *Let $G = \mathrm{PSL}_2(q)$ act on Ω, the set of right cosets of a subgroup $H < G$ and suppose $q \neq 5$. The action is binary if and only if one of the following occurs:*

1. *$H = \{1\}$ and the action is regular;*
2. *$q = 2^a$ for some integer a and H is a Sylow 2-subgroup of G;*
3. *$q = 2^a$ for some odd integer a and $|H| = 3$.*

It is also possible, and much easier, to do the same for the Suzuki groups. At the end of the paper, we prove:

Theorem 1.3. *Let $G = {}^2B_2(2^{2a+1})$, with $a \geq 1$, act on Ω, the set of right cosets of a subgroup $H < G$. The action is binary if and only if one of the following occurs:*

1. *$H = \{1\}$ and the action is regular;*
2. *H is the centre of a Sylow 2-subgroup of G.*

Thus we continue to see, after our initial observations with the alternating groups in [GG], that binary actions of simple groups appear to be rare. A third paper with M. Liebeck (see [GGL]), 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. The answer is that these graphs are "often" connected, again preventing the existence of binary actions in many cases, and highlighting the exceptions.

§2. Background on relational complexity

In this section we gather some basic definitions and results which will be needed in the sequel. See [GG] for proofs and a more leisurely exposition.

Complexity, height & 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.

Let $I, J \in \Omega^n$ be n-tuples of elements of Ω, for some $n \geq 1$, written $I = (I_1, \dots, I_n)$ and $J = (J_1, \dots, J_n)$. For $r \leq n$, we say that I and J are *r-related*, and we write $I \underset{r}{\sim} J$, when for each choice of indices $1 \leq k_1 < k_2 < \cdots < k_r \leq n$, there exists $g \in G$ such that $I_{k_i}^g = J_{k_i}$ for all i.

Now the *relational complexity* of the action of G on Ω, written $\mathrm{RC}(G,\Omega)$, is the smallest integer $k \geq 2$ such that whenever $n \geq k$ 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 [GLS22].

When $\mathrm{RC}(G,\Omega) = 2$, we say that the action is *binary.*

Lemma 2.1 (basic criteria). *[GG, Lemma 2.4] 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) $h_1 h_2 h_3 = 1$,
   (b) there do NOT exist $h_2' \in H_2 \cap H_1$, $h_3' \in H_3 \cap H_1$ with $h_1 h_2' h_3' = 1$.
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.

There is a particular case in which these conditions can be replaced by easier ones. To state this, let us assume that G again acts on Ω, and write G_Λ for the pointwise stabilizer of $\Lambda \subset \Omega$. Define a subset Λ of Ω to be *independent* when $\Lambda' < \Lambda \implies G_\Lambda < G_{\Lambda'}$. The *height* of the action, denoted by $\mathrm{H}(G,\Omega)$, is the maximal size of an independent set. An important example is provided by the action of G on the cosets of H, a *trivial intersection subgroup*, or *TI-subgroup* of G, meaning that $H \cap H^g$ is either H or $\{1\}$, for $g \in G$. In this situation, the height is 1 if H is normal in G and 2 otherwise.

The connection between height and relational complexity is given by the following lemma from [GLS22]:

Lemma 2.2. *Let G act on Ω. Then*

$$\mathrm{RC}(G,\Omega) \leq \mathrm{H}(G,\Omega) + 1\,. \qquad \square$$

One can use this to improve Lemma 2.1:

Lemma 2.3. *Suppose that G acts on Ω, the set of cosets of a TI-subgroup H. Then the conditions of Lemma 2.1 are also equivalent to:*

4. *The action is not binary.*

5. *There are conjugates H_1, H_2 and H_3 of H which are distinct and satisfy $H_1 \cap H_2 \cdot H_3 \neq \{1\}$.*

Proof. As just pointed out, the height of the action is 2, and so the complexity is 2 or 3, by the previous lemma.

Now, the conditions of Lemma 2.1 imply (4). Conversely, if (4) holds, then the complexity is 3 by Lemma 2.2. This implies (1). Indeed, if we were to suppose that (1) fails, then any two n-tuples which are 2-related would be 3-related, and thus they would be n-related also as the complexity is 3, but then by definition this would show that the action is binary.

Now assume (5). By assumption we have $H_1 \cap H_2 = \{1\}$ as well as $H_1 \cap H_3 = \{1\}$, and we see that $H_1 \cap H_2 \cdot H_3$ is not included in $H_1 \cap (H_1 \cap H_2) \cdot H_3 = \{1\}$, so we have condition (3).

Finally, assume (3). To prove that we have (5), we only need to check that the H_i's are distinct. If we had $H_2 = H_3$, then $H_1 \cap H_2 \cdot H_3 = H_1 \cap H_2$ would be included in $H_1 \cap (H_1 \cap H_2) \cdot H_3$, which is absurd. If we had $H_1 = H_3$, then $H_1 \cap H_2 \cdot H_3 = H_1$ and $H_1 \cap (H_1 \cap H_2) \cdot H_1 = H_1$, another contradiction. Assuming $H_1 = H_2$ similarly leads to an absurd conclusion. □

The graph $\Gamma(\mathcal{C})$

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 $yx^{-1} \in \mathcal{C}$.

Example 2.4. While studying the group $\mathrm{PSU}_3(q)$, we shall encounter an example where $\Gamma(\mathcal{C})$ is isomorphic to the set of nonzero cubes in $\mathbb{F}_q$ (where q is even in this instance), with an edge between x and y if and only if $x + y$ is also a cube: see Lemma 3.4. A little later, as we turn our attention to $\mathrm{PSL}_2(q)$, we shall be in a situation where a certain subgraph of $\Gamma(\mathcal{C})$ is similarly defined with squares instead of cubes: see Lemma 4.5. It is easy to produce more examples of this kind, close cousins of the familiar Paley graphs, by considering a semidirect product $G = \mathbb{F}_q \rtimes \mathbb{F}_q^\times$, with the action of $\mathbb{F}_q^\times$ of your choice.

Some vocabulary in order to state the main result. 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 theorem is Corollary 2.16 from [GG]. It asserts that, in the case of transitive, binary actions, each stabilizer must contain a component group. Note that *an element of maximal p-fixity* is 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.

Theorem 2.5. *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.*

If 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 $H = G$.

Remark 2.6. For the convenience of the reader who does not have [GG] at hand to consult the proof of the theorem, and who might find the result surprising, we offer a couple of comments. A statement in [GHS19] was the starting point, and after a series of elementary reformulations, the graph-theorical language has eventually appeared. Here is an intermediate lemma, which is essentially equivalent to the theorem, and might feel more familiar, at least to some readers: suppose that G acts on Ω, that p is a prime, and that g and h are commuting p-elements of G with the property that $\langle g\rangle$, $\langle h\rangle$ and $\langle gh^{-1}\rangle$ are conjugate subgroups of G. We write $K = \langle g, h\rangle$. Suppose that

1. $|\mathrm{Fix}(K)| < |\mathrm{Fix}(g)|$;
2. g has maximal p-fixity.

Then the action of G on Ω is not binary. This is Lemma 2.12 in [GG].

Example 2.7. While most uses of the theorem in this paper will exploit the fact that $\Gamma(\mathcal{C})$ has sometimes large connected components, thus preventing the stabilizers in certain binary actions from being too small, and thereby giving an obstruction to the very existence of nontrivial binary actions, here is an easy situation where we can do the opposite. Suppose that $\mathcal{C}$ is a conjugacy class of involutions in a group G, let $h \in \mathcal{C}$ and $H = \langle h\rangle$, and suppose that $\Gamma(\mathcal{C})$, the graph described above, does not have a single edge. Then it is an easy consequence of Lemma 2.3 that in this case the action of G on the set of right cosets of H in G is binary.

To see that such actions exist, let $G = \mathrm{PSL}_n(q)$ with nq odd and take $\mathcal{C}$ to be the conjugacy class of involutions that are the projective image of a matrix in $\mathrm{SL}_n(q)$ with a (-1)-eigenspace of dimension $n-1$ and a 1-eigenspace of dimension 1. It is easy to see that if $g, h \in \mathcal{C}$ then gh has a 1-eigenspace of dimension at least $n-2$.

Thus, for $n \geq 5$, the graph $\Gamma(\mathcal{C})$ is edgeless and the group $\mathrm{PSL}_n(q)$ has a transitive binary action with a point-stabilizer of order 2.

The problem of classifying all simple groups G with a conjugacy class $\mathcal{C}$ of involutions for which $\Gamma(\mathcal{C})$ is edgeless is a tantalising one!

A few lemmas

We shall need four lemmas from [GLS22].

Lemma 2.8. *[GLS22, Lemma 1.6.2] Let $H < B < G$. Then $\mathrm{RC}(G,(G:H)) \geq \mathrm{RC}(B,(B:H))$. In particular, if the action of G on $(G:H)$ is binary, so is the action of B on $(B:H)$.*

Lemma 2.9. *[GLS22, Lemma 1.7.1] Let G be transitive on Ω and let M be a point-stabilizer in this action. Let Λ be a non-trivial orbit of M. Then*

$$\mathrm{RC}(G,\Omega) \geq \mathrm{RC}(M,\Lambda).$$

Lemma 2.10. *[GLS22, Lemma 1.8.1] Let G be a Frobenius permutation group on Ω (that is, G acts transitively on Ω, $G_\omega \neq 1$ for every $\omega \in \Omega$ and $G_{\omega\omega'} = 1$ for every $\omega, \omega' \in \Omega$ with $\omega \neq \omega'$). If G is binary, then a Frobenius complement has order equal to 2.*

In the next lemma 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 2.11. *[GLS22, Lemma 1.7.8] Let G act on Ω and suppose that $\Lambda \subset \Omega$. Suppose, moreover, that G_Λ, the setwise stabilizer of Λ in G, acts 2-transitively on Λ. If the action of G on Ω is binary, then the action of G^Λ is the full symmetric group on Λ.*

§3. Groups with a single class of involutions

In this section we prove Theorem 1.1.

Strongly embedded subgroups

Consider a finite group G containing a single class of involutions $\mathcal{C}$. In this case $\Gamma(\mathcal{C})$ is the *involution commuting graph* of G.

We need a definition: a proper, even order subgroup N of G is called *strongly embedded* if $|N \cap N^g|$ is odd for every $g \in G \setminus N$. Now the following proposition follows immediately from the main result of Aschbacher in [Asc73]:

Proposition 3.1. *Suppose that G is a finite group containing a single class of involutions $\mathcal{C}$, let X be a connected component of $\Gamma(\mathcal{C})$ and let N be the normalizer in G of X. Either $X = \mathcal{C}$ or else $N \cap \langle \mathcal{C} \rangle$ is strongly embedded in $\langle \mathcal{C} \rangle$.*

Assume from now on that G is simple, so that $\langle \mathcal{C} \rangle = G$. The alternative of the proposition is thus: either $\Gamma(\mathcal{C})$ has a single component group which is all of G, or N is strongly embedded in G.

However, the latter case is severely restricted. Indeed, the Bender-Suzuki theorem [Ben71, Suz62, Suz64], together with Glauberman's Z^*-theorem [Gla66], yields the following:

Proposition 3.2. *Suppose that G is a simple group containing a strongly embedded subgroup. Then G is isomorphic to $\mathrm{PSL}_2(q)$, ${}^2B_2(q)$ or $\mathrm{PSU}_3(q)$ where $q = 2^a$ and $a \geq 2$.*

It is now easy to deduce:

Proposition 3.3. *Suppose that G is a simple group acting on the set of cosets of a subgroup H of even order. Assume that the action is binary, and that $H \neq G$. If G has a single conjugacy class of involutions, then G is isomorphic to $\mathrm{PSL}_2(q)$, ${}^2B_2(q)$ or $\mathrm{PSU}_3(q)$ where, in all three cases, $q = 2^a$ and $a \geq 2$. Moreover, in all three cases, H contains the centre of a Sylow 2-subgroup of G.*

Proof. Theorem 2.5 and Propositions 3.1 and 3.2 yield the first part. The only thing that needs to be proved is that, when G is in one of the three listed families of simple groups, H must contain the centre of a Sylow 2-subgroup of G. This follows from the fact that the centre of a Sylow 2-subgroup of G is elementary-abelian and so its non-trivial elements are all connected to each other in $\Gamma(\mathcal{C})$ where $\mathcal{C}$ is the unique class of involutions in G. □

Let us list some simple groups with a single class of involutions. First, the alternating groups and the sporadics (using [CCN+85]):

$$A_5, A_6, A_7, M_{11}, M_{22}, M_{23}, J_1, J_3, McL, O'N, Ly, Th. \tag{3.1}$$

Second, groups of Lie type (using [GLS98]):

$$\mathrm{PSL}_2(q), {}^2B_2(q), {}^2G_2(q), \mathrm{PSU}_3(q), G_2(q_o), {}^3D_4(q_o). \tag{3.2}$$

(Here we write q_o to mean that q must be odd.) Note that we are not claiming that these lists are exhaustive. For instance [CCN+85] tells us that $\mathrm{PSU}_4(3)$ has a single class of involutions.

For any such group G, except the three families of exceptions listed in the proposition, we see that G does not have a single transitive, binary action with proper stabilizers of even order. This result contributes to the general impression that binary actions of simple groups are rare.

At this point, however, we do meet actual examples of nontrivial binary actions, taking G as imposed by the proposition, and H to be the centre of a Sylow 2-subgroup. To see this, let us turn to the proof of Theorem 1.1

The proof

For convenience, we repeat the statement which was given in the introduction.

Theorem. *Suppose that G is a simple group that contains a single conjugacy class of involutions, let H be a proper subgroup of G of even order and let Ω be the set of right cosets of H in G. Then the action of G on Ω is binary if and only if we are in one of the following situations:*

1. *$G = \mathrm{PSL}_2(2^a)$ with $a \geq 2$ and H is a Sylow 2-subgroup of G;*
2. *$G = {}^2B_2(2^{2a+1})$ with $a \geq 1$ and H is the centre of a Sylow 2-subgroup of G;*
3. *$G = \mathrm{PSU}_3(2^a)$ with $a \geq 2$ and H is the centre of a Sylow 2-subgroup of G.*

We embark on the proof, which will occupy the rest of this section. From Proposition 3.3, we see that we may conduct the proof assuming that G is isomorphic to one of $\mathrm{PSL}_2(q)$, ${}^2B_2(q)$ or $\mathrm{PSU}_3(q)$ where, in all three cases, $q = 2^a$ and $a \geq 2$. Moreover, in all three cases, H contains the centre of a Sylow 2-subgroup of G.

Some binary actions. We start by proving that if H is as small as possible, i.e. H is equal to the centre of a Sylow 2-subgroup of G, then the action of G on Ω is binary (note that if $G = \mathrm{PSL}_2(q)$, then a Sylow 2-subgroup of G is equal to its own centre). Note first that, in all cases, G acts 2-transitively by conjugation on the set of conjugates of H; moreover, distinct conjugates of H intersect trivially and so we use Lemma 2.3 to confirm that the action of G on Ω is binary. We must show that if H_1, H_2 and H_3 are distinct conjugates of H, then $H_1.H_2 \cap H_3 = \{1\}$.

In the case where $G = \mathrm{PSL}_2(q)$, then, since q is even, we have $G = \mathrm{SL}_2(q)$ and we use 2-transitivity to take H_1 (resp. H_2) as the set of strictly upper-triangular (resp. lower-triangular) matrices. Now observe that, for $a, b \in \mathbb{F}_q$,

$$\begin{pmatrix} 1 & a \\ & 1 \end{pmatrix} \begin{pmatrix} 1 & \\ b & 1 \end{pmatrix} = \begin{pmatrix} 1+ab & a \\ b & 1 \end{pmatrix}.$$

An element $g \in \mathrm{SL}_2(q)$ has order dividing 2 if and only if $\mathrm{trace}(g) = 0$; we conclude that the element on the right hand side of the above equation has order dividing 2 if and only if a or b is equal to 0. Using the fact that distinct conjugates of H intersect trivially, we conclude, as required, that $H_1.H_2 \cap H_3 = \{1\}$ whenever H_1, H_2 and H_3 are distinct conjugates of H.

When $G = \mathrm{PSU}_3(q)$ we use the fact that if H_1 and H_2 are distinct conjugates of H, then $\langle H_1, H_2 \rangle \cong \mathrm{SL}_2(q)$ and we use the calculation for $G = \mathrm{SL}_2(q)$ to conclude that $H_1.H_2 \cap H_3 = \{1\}$ once again, as required.

Finally, when $G = {}^2B_2(q)$, we use [Suz62, §13] to write down two conjugates of H, using the natural embedding of H in $\mathrm{Sp}_4(q)$. Recall that $q = 2^{2a+1}$ for some positive integer a and we set θ to be the automorphism of $\mathbb{F}_q$ given by $\alpha \mapsto \alpha^{2^{a+1}}$. Now the conjugates of H can be written as:

$$H_1 = \left\{ h_1 = \begin{pmatrix} 1 & & & \\ & 1 & & \\ \beta_1 & & 1 & \\ \beta_1^\theta & \beta_1 & & 1 \end{pmatrix} \mid \beta_1 \in \mathbb{F}_{2^{2a+1}} \right\};$$

$$H_2 = \left\{ h_2 = \begin{pmatrix} 1 & & \beta_2 & \beta_2^\theta \\ & 1 & & \beta_2 \\ & & 1 & \\ & & & 1 \end{pmatrix} \mid \beta_2 \in \mathbb{F}_{2^{2a+1}} \right\}.$$

If we multiply the two matrices, h_1 and h_2, given in H_1 and H_2, then we obtain

$$h_1.h_2 = \begin{pmatrix} 1 & 0 & \beta_2 & \beta_2^\theta \\ 0 & 1 & 0 & \beta_2 \\ \beta_1 & 0 & 1+\beta_1\beta_2 & \beta_1\beta_2^\theta \\ \beta_1^\theta & \beta_1 & \beta_1^\theta\beta_2 & 1+\beta_1\beta_2+\beta_1^\theta\beta_2^\theta \end{pmatrix}.$$

One can check directly that $(h_1h_2)^2 = 1$ if and only if $\beta_1 = 0$ or $\beta_2 = 0$. This implies that $h_1.h_2$ lies in a conjugate of H if and only if $h_1 = 1$ or $h_2 = 1$. This confirms that $H_1.H_2 \cap H_3 = \{1\}$ for any distinct conjugate, H_3, of H, as required.

No other examples. For the remainder we assume that H is a proper subgroup of G that properly contains the centre of P, a Sylow 2-subgroup of G. Our job is to show that, in this case, the action of G on Ω is not binary.

First, note that in all cases, $N_G(Z(P)) = P \rtimes T$, where T is a group of size $q-1$ (for $G = \mathrm{SL}_2(q)$ or $G = {}^2B_2(q)$) or $(q^2-1)/\gcd(q+1,3)$ (for $G = \mathrm{PSU}_3(q)$).

Assume, first, that $G = \mathrm{SL}_2(q)$ or $G = {}^2B_2(q)$. Then T acts on P fixed-point-freely and so $N_G(Z(P))$ is a Frobenius group with Frobenius kernel P and a Frobenius complement T. What is more, since distinct conjugates of $Z(P)$ generate G in this case, we conclude that H normalizes $Z(P)$. If $H \neq O_2(H)$, the largest normal 2-subgroup of H, then this means that H, too, is a Frobenius group with kernel $O_2(H)$ and a Frobenius complement T_H isomorphic to a subgroup of T; in particular $|T_H| \geq 3$.

Now, distinct conjugates of $N_G(Z(P))$ intersect in a conjugate of T and it follows that there exist distinct conjugates of H that intersect in a conjugate of T_H. This implies that there is an orbit of H on which H acts as a Frobenius group with stabilizer T_H. Now Lemma 2.10 implies that the action of H on this orbit is not binary and Lemma 2.9 implies that the action of G on Ω is not binary, as required.

We conclude that if $G = \mathrm{SL}_2(q)$ or $G = {}^2B_2(q)$, then $H = O_2(H)$. If $G = \mathrm{SL}_2(q)$ this implies that $H = Z(P)$, a contradiction and this case is done. Thus assume that $G = {}^2B_2(q)$ and $H = O_2(H)$; in particular $Z(P) < H \leq P$, for P some Sylow 2-subgroup of G.

We need an explicit matrix representation of a Sylow 2-subgroup of G. We define

$\theta : \mathbb{F}_{2^{2a+1}} \to \mathbb{F}_{2^{2a+1}}, \zeta \mapsto \zeta^{2^{a+1}}$ and set

$$U_2 := \left\{ \begin{pmatrix} 1 & & & \\ \alpha & 1 & & \\ \alpha^{1+\theta}+\beta & \alpha^\theta & 1 & \\ \alpha^{2+\theta}+\alpha\beta+\beta^\theta & \beta & \alpha & 1 \end{pmatrix} \mid \alpha, \beta \in \mathbb{F}_{2^{2a+1}} \right\};$$

$$\tau := \begin{pmatrix} & & & 1 \\ & & 1 & \\ & 1 & & \\ 1 & & & \end{pmatrix}.$$

Referring to [Suz62, §13], we find that we can define G to equal $\langle U_2, U_2^\tau \rangle$ and both U_2 and U_2^τ are then Sylow 2-subgroups of G. If we identify P with U_2, then Z, the centre of U_2, becomes the set of elements for which $\alpha = 0$.

Now observe that

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

We identify h_2 (resp. h_3, h_1) with the first (resp. second, third) of these matrices. Note that h_2 and h_3 are of order 4 while h_1 is of order 2.

The element h_2 is in U_2 (set $\alpha = 1$ and $\beta = 0$ in the description above). Since distinct Sylow 2-subgroups of G intersect trivially, U_2 is the unique Sylow 2-subgroup containing h_2. Likewise we write U_1 (resp. U_3) for the unique Sylow 2-subgroup containing h_1 (resp. h_3). Note that U_2 is a set of lower-triangular matrices and $U_3 = U_2^\tau$ is a set of upper-triangular matrices and, since h_3 is neither upper- nor lower-triangular, we can see that U_1, U_2, U_3 are distinct.

We know that G contains a unique class of involutions and we also use the easy fact that G contains a unique conjugacy class of cyclic subgroups of order 4. Thus we can assume that H_1 (resp. H_2, H_3) contains h_1 (resp. h_2, h_3). But now, since U_1, U_2 and U_3 are distinct, the same is true of H_1, H_2 and H_3. But $h_1 \in H_1 \cap H_2 \cdot H_3$ and so Lemma 2.3 yields the result.

The more difficult case of $\mathrm{PSU}_3(q)$. We are left with the possibility that $G = \mathrm{PSU}_3(q)$. We set $q \geq 4$, since G is simple. We let H and Ω be as in the statement of Theorem 1.1 with the added assumption that H properly contains $Z(P)$, the centre of P, a Sylow 2-subgroup of G; we assume that the action of G on Ω is binary and will argue so as to obtain a contradiction.

We start with general information about $\mathrm{PSU}_3(q)$. Let $\{e_1, w, f_1\}$ be a hyperbolic basis for $V = (\mathbb{F}_{q^2})^3$ with respect to a non-degenerate Hermitian form and define three subgroups of the associated special isometry group, $\mathrm{SU}_3(q)$:

$$P^\dagger = \left\{ \begin{pmatrix} 1 & a_1 & a_2 \\ & 1 & a_1^q \\ & & 1 \end{pmatrix} \mid a_1, a_2 \in \mathbb{F}_{q^2} \text{ and } a_2 + a_2^q + a_1^{q+1} = 0 \right\}$$

$$T^\dagger = \left\{ \begin{pmatrix} t & & \\ & t^{q-1} & \\ & & t^{-q} \end{pmatrix} \mid t \in \mathbb{F}_{q^2} \text{ and } t \neq 0 \right\}$$

$$L^\dagger = \left\{ \begin{pmatrix} a & & b \\ & 1 & \\ c & & d \end{pmatrix} \mid a, b, c, d \in \mathbb{F}_q \text{ and } ad - bc = 1 \right\}$$

Now we can take P to be the projective image of $P^\dagger$ with $Z(P)$ being the projective image of the subgroup for which $a_1 = 0$ and $a_2 \in \mathbb{F}_q$. Then $N_G(P)$ is the projective image of $P^\dagger \rtimes T^\dagger$.

Another fact about G that will be useful is that for any nonzero $c \in \mathbb{F}_{q^2}^\times$, the action of G on pairs of isotropic vectors (v, w) such that $\langle v, w \rangle = c$ is transitive. This follows easily from Witt's theorem.

We must consider two possibilities:

Case (1) : H contains two distinct conjugates of $Z(P)$. Since, as we saw above, G acts 2-transitively on the set of conjugates of $Z(P)$, there is a unique conjugacy class of subgroups of G generated by 2 distinct conjugates of $Z(P)$; this class includes L, the projective image of $L^\dagger$, a subgroup of G isomorphic to $\mathrm{SL}_2(q)$.

Thus, in this first case, we assume that H contains L. Consulting [BHR13, Tables 8.5 and 8.6] we see that H normalizes L and $|H : L|$ divides $(q+1)/\gcd(3, q+1)$. Now define $Q^\dagger$ to be the subgroup of $P^\dagger$ obtained by restricting a_1 to $\mathbb{F}_q$ in the definition above. Then $Q^\dagger$ is a group of order q^2 and we take Q to be its projective image in G. Define Λ to be the subset of Ω whose elements are subsets of $H.Q$. Then Λ is a set of size q, on which Q acts transitively.

Let $R^\dagger = T^\dagger \cap L^\dagger$, so elements of $R^\dagger$ are diagonal matrices in $\mathrm{SU}_3(q)$ whose entries are in $\mathbb{F}_q$; let R be the projective image of $R^\dagger$ in G and notice that R is a cyclic subgroup of H of order $q-1$. Now R normalizes Q and hence, for all $q_1 \in Q$ and $r \in R$, there exists $q_2 \in Q$ such that

$$(Hq_1)r = (Hr)q_2 = Hq_2.$$

Thus R acts on Λ. Indeed, since $R < H$, R acts on $\Lambda \setminus \{H\}$, a set of size $q-1$. We claim that, for $q \in Q$ and $r \in R$, $(Hq)r = Hq$ if and only if $Hq = H$ or $r = 1$. To see this, observe first that an element of H is the projective image of a matrix of form

$$h^\dagger = \begin{pmatrix} as & & bs \\ & 1/s^2 & \\ cs & & ds \end{pmatrix}$$

where $a, b, c, d \in \mathbb{F}_q$, $s \in \mathbb{F}_{q^2}$, $ad - bc = 1$ and $s^{q+1} = 1$. Fixing this $h^\dagger$, we find that for $q^\dagger \in Q^\dagger$, we have

$$h^\dagger q^\dagger = \begin{pmatrix} as & aa_1 s & aa_2 s + bs \\ 0 & 1/s^2 & a_1/s^2 \\ cs & ca_1 s & ca_2 s + ds \end{pmatrix}$$

for some $a_1 \in \mathbb{F}_q$, $a_2 \in \mathbb{F}_{q^2}$ with $a_1^2 + a_2 + a_2^q = 0$. Notice that if we vary the element $h^\dagger$ but fix $q^\dagger$, then the quotient of the non-zero elements of the middle row of $h^\dagger q^\dagger$ is fixed and equal to a_1. In particular all elements which project onto Hq have this quotient equal to a_1.

Finally, fixing this $q^\dagger$ and $h^\dagger$, we find that for $r^\dagger \in R^\dagger$

$$h^\dagger q^\dagger r^\dagger = \begin{pmatrix} ras & aa_1 s & (aa_2 s + bs)/r \\ 0 & 1/s^2 & a_1/(rs^2) \\ crs & ca_1 s & (ca_2 s + ds)/r \end{pmatrix}$$

for some $r \in \mathbb{F}_q^*$. Notice that for this element, the quotient of the non-zero elements of the middle row is equal to a_1/r. We conclude that $(Hq)r = Hq$ if and only if $a_1/r = a_1$, which is if and only if $a_1 = 0$ or $r = 1$. But if $a_1 = 0$, then $Hq = H$ and the claim follows.

Since $|R| = |\Lambda \setminus \{H\}| = q - 1$, the claim implies that R acts transitively on $\Lambda \setminus \{H\}$ and we conclude that the group $Q \rtimes R$ acts 2-transitively on Λ.

Then Lemma 2.11 implies that, since the action of G on Ω is binary, G must contain a section isomorphic to A_{q-1}, the alternating group on $q-1$ letters; but now [KL90, Proposition 5.3.7] implies that this is impossible for $q \geq 8$. Thus $G = \mathrm{PSU}_3(4)$ and [GAP16] confirms that here too we have a contradiction, as required.

Case (2): H contains a unique conjugate of $Z(P)$. In particular $Z(P) < H \leq B := N_G(Z(P))$. The group B is the Borel subgroup of G and, using its well-known structure, we see that $H = Q \rtimes T_1$ where $Z(P) \leq Q \leq P$ and T_1 is a (possibly trivial) group of order dividing $(q^2-1)/\gcd(q+1,3)$. We shall first prove that we can reduce to the case $Q = P$, and then that we can assume that the order of T_1 divides $q+1$. At this point, the action of G on $(G : H)$ can be understood more concretely, and we will conclude by direct arguments.

(a) To begin with, we shall consider the action of B on $(B : H)$. By Lemma 2.8, it is also binary. We shall use this to prove, using the apparatus of component groups again, that H must contain P.

Note that H contains $Z(P)$ which is normal in B and hence lies in the kernel of the action of B on $(B : H)$. Define $\overline{B} := B/Z(P)$ and $\overline{H} := H/Z(P)$ and observe that $\overline{B} = \overline{P} \rtimes \overline{T}$ where $\overline{P}$ is elementary-abelian of order q^2 and $\overline{T}$ is a cyclic group of order $(q^2-1)/\gcd(q+1,3)$; similarly we can take $\overline{H} = \overline{Q} \rtimes \overline{T_1}$ where $1 \leq \overline{Q} \leq \overline{P}$ and $1 \leq \overline{T_1} \leq \overline{T}$. Also, the conjugation action of $\overline{T}$ on $\overline{P}$ can be described as follows: if we use the entry a_1 in the description of $P^\dagger$ to identify $\overline{P}$ with $\mathbb{F}_{q^2}$, then the action of the element which is the image of $\mathrm{diag}(t, t^{q-1}, t^{-q})$ is by multiplication by t^{q-2}. By assumption the action of $\overline{B}$ on $(\overline{B} : \overline{H})$ is binary.

Suppose, first, that $\overline{Q} = \{1\}$. In this case $\overline{H} = \overline{T_1}$ is non-trivial by assumption and $\overline{T_1} < \overline{B_1} := \overline{P} \rtimes \overline{T_1} \leq \overline{B}$. But now the action of $\overline{B_1}$ on $(\overline{B_1} : \overline{T_1})$ is a Frobenius action and hence, by Lemma 2.10, is not binary (note that $|\overline{T_1}|$ is odd). Now Lemma 2.8 implies that the action of $\overline{B}$ on $(\overline{B} : \overline{H})$ is not binary and so the same is true of the action of B on $(B : H)$, a contradiction.

Suppose, instead, that $\overline{Q} \neq \{1\}$. In particular $\overline{Q}$ contains an involution g. We claim that the component group of g is $\overline{P}$, so that $\overline{Q} = \overline{P}$ by Theorem 2.5. The claim is very easy when q is of the form $q = 2^{2a}$, for in this case, the non-identity elements of $\overline{P} = \mathbb{F}_{q^2}$ form the unique conjugacy class $\mathcal{C}$ of involutions in $\overline{B}$, and it is a direct consequence of the definitions that $\Gamma(\mathcal{C})$ is connected (it is in fact a complete graph). The component group of g is generated by $\mathcal{C}$ and so it is clearly $\overline{P}$.

When $q = 2^{2a+1}$, there are three conjugacy classes of involutions in $\overline{B}$, and the class $\mathcal{C}$ of $1 \in \mathbb{F}_{q^2} = \overline{P}$ comprises all the cubes in $\mathbb{F}_{q^2}^\times$ (it is also the image of the map $t \mapsto t^{q-2}$ on $\mathbb{F}_{q^2}^\times$ considered above). Lemma 3.4 below shows that the component group of 1 is then $\overline{P}$. If we see $\mathbb{F}_{q^2}^\times$ as the disjoint union of the three conjugacy classes $\mathcal{C}, \mathcal{C}'$ and $\mathcal{C}''$, then multiplication by any $x \in \mathbb{F}_{q^2}^\times$ provides an automorphism of the disjoint union of the graphs $\Gamma(\mathcal{C})$, $\Gamma(\mathcal{C}')$ and $\Gamma(\mathcal{C}'')$, and it follows easily that the conclusions of Lemma 3.4 can be extended to the other conjugacy classes.

We have established that $\overline{H} = \overline{P} \rtimes \overline{T_1}$. Here $\overline{H}$ is normal in $\overline{B}$ and so the action of $\overline{B}$ on $(\overline{B} : \overline{H})$ is binary, and a contradiction will not be found. Thus we return to considering the action of G on $(G : H)$ directly. As announced, however, now we know that H contains P, and in fact that $H = P \rtimes T_1$.

(b) Next we claim that the order of T_1 must, in fact, divide $(q+1)/\gcd(q+1,3)$.

To see this, we note that it is easy to find H_1, a conjugate of H, such that $H \cap H_1 = T_1$ and now Lemma 2.9 implies that the action of H on $(H : T_1)$ is binary. If $|T_1| > 1$ and $|T_1|$ divides $q-1$, then the action of H on $(H : T_1)$ is Frobenius and Lemma 2.10 gives a contradiction. If $|T_1| > 1$ and $|T_1|$ does not divide $q-1$, then T_1 has a subgroup T_0 of order $\gcd(|T_1|, q+1/\gcd(q+1,3))$ satisfying the conditions of Lemma 3.5 below with $N = P$ and $K = Z(P)$. Thus $T_1 = T_0$ and the claim follows.

(c) Let $T_1^\dagger$ denote the preimage of T_1 in $\mathrm{SU}_3(q)$. The group $T_1^\dagger$ can be identified with a subgroup of $\mathbb{F}_{q^2}^\times$ in various ways, for example *via* $\mathrm{diag}(t, t^{q-1}, t^{-q}) \mapsto t$; in any case, there is a unique subgroup $T_1' \subset \mathbb{F}_{q^2}^\times$ having the same order as $T_1^\dagger$.

Assume, first, that $T_1^\dagger$ is non-trivial and pick $x \in T_1'$ with $x \neq 1$. We write X for the set of equivalence classes of isotropic vectors in V under the relation $v \sim tv$ for $t \in T_1'$. Then G acts on X, transitively, and with stabilizers conjugate to $P \rtimes T_1$, so we work with this action and show that it admits tuples that are 2-related but not 3-related (condition (1) from Lemma 2.1).

For this, pick $y \in \mathbb{F}_{q^2}$ such that $x + x^q = y^{q+1}$, so that $v = (x, y, 1)$ and $v' = (1, y, x)$ are isotropic. The tuples will be $([e_1], [f_1], [v])$ and $([e_1], [f_1], [v'])$, where the notation $[-]$ refers to the equivalence class. One sees easily that the tuples are 2-related, using the transitivity of the action of G on pairs of isotropic vectors with a fixed hermitian product, and the fact that x is taken from T_1'. Suppose now that $g \in G$ were to take one triple to the other; as g fixes the lines spanned by e_1 and f_1, respectively, it is of the form $\mathrm{diag}(t, t^{q-1}, t^{-q})$, and the condition is thus that there should exist $s \in T_1'$ such that

$$(tx, t^{q-1}y, t^{-q}) = (s, sy, sx)\,.$$

In particular $t^{-q} = sx$, and so raising to the power $q+1$ (remembering that x and s are in T_1' and so have order dividing $q+1$), we get $t^{-q} = t$ so $t = sx$. Comparing with $tx = s$ we get $x^2 = 1$ so $x = 1$, a contradiction.

We are left with the case when $T_1^\dagger$ is trivial. This means, first, that $q = 2^{2a}$ and, second, that $H = P$. In this situation $\mathrm{PSU}(3,q) = \mathrm{SU}(3,q)$, so we can consider the action of G on the set of isotropic vectors; this set may be identified with Ω, with its action by G, as the stabilizer of an isotropic vector is H. We shall write down two triples of isotropic vectors which are 2-related but not 3-related, showing that the action cannot be binary. For a vector $v = (x, y, z)$, writing $\langle -, - \rangle$ for the Hermitian product, we have $\langle v, v \rangle = xz^q + x^q z + yy^q$, and $\langle e_1, v \rangle = z$ while $\langle f_1, v \rangle = x$. Now we pick any x with $x + x^q = 1$ and $y \neq 1$ such that $yy^q = 1$, and we define $v = (x, y, 1)$, $v' = (x, 1, 1)$. The vectors v, v' are isotropic, and the triples (e_1, f_1, v) and (e_1, f_1, v') are 2-related, as follows again from the fact that G acts transitively on pairs of isotropic vectors with constant hermitian product. However, these triples are not 3-related, as an element of G fixing e_1 and f_1 must be the identity.

This concludes the study of the group $\mathrm{PSU}(3,q)$ and the proof of Theorem 1.1.

Auxiliary results

During the above argument, we have relied on two lemmas which we present now. First we have:

Lemma 3.4. *Let $q = 2^{2a+1}$, and let C be the set of cubes in $\mathbb{F}_{q^2}^\times$.*

1. *Let Γ be the graph on C in which two elements $x, y \in C$ are joined by an edge if and only if $x + y \in C$. Then Γ is connected.*

2. *The additive group $\mathbb{F}_{q^2}$ is generated by C.*

Proof. (1) Note that C is a subgroup of $\mathbb{F}_{q^2}^\times$. Any $c \in C$ gives rise to a graph automorphism φ_c of Γ given by multiplication by c. When c is a neighbour of 1, we see that φ_c must stabilize the connected component Δ containing 1; as a result, if $c = c_1 c_2 \cdots c_s$ where each c_i is a neighbour of 1, we also have $\varphi_c(\Delta) = \Delta$, and in particular $c = \varphi_c(1) \in \Delta$. Thus it suffices to prove that C is generated as a group by the neighbours of 1, in order to conclude that $\Delta = C$.

Any element $x \in \mathbb{F}_q^\times$ is a cube, and $x+1 \in \mathbb{F}_q^\times$ is another cube (assuming $x \neq 1$), so this x is a neighbour of 1. We see that the subgroup C_0 generated by these neighbours contains $\mathbb{F}_q^\times$, so that its order is divisible by $q-1$. We now show that any element $x \in \mathbb{F}_{q^2}$ satisfying $x^m = 1$, where $m = (q+1)/3$, is also a neighbour of 1 (it is a cube since $x^{(q^2-1)/3} = x^{(q-1)m} = 1$). Clearly this will suffice to show that $C_0 = C$.

Let x be such an element. Cubing, we see that $x^{q+1} = 1$ so that $x^q = x^{-1}$. To check that $1+x$ is a cube, we show that $(1+x)^{(q^2-1)/3} = 1$ and for this we compute:

$$(1+x)^{(q-1)m} = \frac{(1+x)^{qm}}{(1+x)^m} = \left(\frac{1+x^q}{1+x}\right)^m = \left(\frac{1+x^{-1}}{1+x}\right)^m = \frac{1}{x^m} = 1\,.$$

(2) Since the elements of $\mathbb{F}_q$ are cubes, the subgroup generated by C is really an $\mathbb{F}_q$-linear subspace, so that its order is 1, q or q^2 by linear algebra. The cardinality of C is greater than q, so the result follows. □

The second, quite technical lemma is a variation on Lemma 2.10 about Frobenius actions. Indeed, the proof is an elaboration of an argument due to Wiscons which served to prove Lemma 2.10 (see [GLS22]). Note that, when the hypothesis $|T_0| > 1$ is not satisfied, then the action is Frobenius.

Lemma 3.5. *Let $G = N \rtimes T$ be a semi-direct product. Let K be a normal subgroup of G with $K \subset N$, and let $A = N \smallsetminus K$. We assume that the action of T on A by conjugation is free, and that the action of T on $K \smallsetminus \{1\}$ factors as a free action of a quotient T/T_0. Also, to avoid degenerate cases, we assume $|N : K| > 1$ and $|T_0| > 1$.*

Finally, we assume that the action of G on the set of cosets of T is binary. Then $T_0 = T$. Moreover, if $|N : K| > 2$, then $|T| \leq 1 + 2|K|$.

Proof. If $|N : K| = 2$, and there is a prime p dividing the order of T/T_0, we notice that p divides $|A|$, while $|K| = 1 \bmod p$. This is absurd, as $|A| = |K|$ in this case, so we conclude that $T_0 = T$. We continue the argument under the assumption $|N : K| > 2$.

The set of cosets of T in G may be identified with N, in such a way that the action of the subgroup N is by right multiplication, and the action of T is by conjugation. The stabilizer of 1 is $G_1 = T$ and the stabilizer of $x \in N$ is $G_x = T^x$.

First we note that $T \cap T^a = \{1\}$ for $a \in A$. Indeed, $T \cap T^a$ is the stabilizer of a for the action of the subgroup T, and this is assumed to be free. By the same token, for $k \in K \smallsetminus \{1\}$, we have $T \cap T^k = T_0$.

Pick $a, b \in A$ with $a \neq b$. We claim that $T^b \cap T^a = \{1\}$ when a and b are not in the same (right) coset of K in N, and $T^b \cap T^a = T_0^a = T_0^b$ otherwise. To see this, note $(T^b \cap T^a)^{b^{-1}} = T \cap T^{ab^{-1}}$ and by the previous paragraph, this intersection is trivial unless $k := ab^{-1} \in N \smallsetminus A = K$, so that $a = kb$; by the second point made in the previous paragraph, when $a = kb$, we have $T^b \cap T^a = T_0^b$. Also, elements of T_0 commute with elements of K by assumption, so $T_0^k = T_0$ and it follows that $T_0^a = T_0^b$.

Fix $a_0 \in A$. We are going to study the various sets $X_a = a_0 \cdot G_a \smallsetminus \{a_0\}$, where $a \in A$ and $a_0 \cdot G_a$ is the orbit of a_0 under G_a. Suppose that, for some a, b, we can find a_1 such that $a_1 \in (a_0 \cdot G_a \cap a_0 \cdot G_b) \setminus a_0 \cdot G_{ab}$. Set $I = (a_0, a, b)$ and $J = (a_1, a, b)$ and observe that $I \underset{2}{\sim} J$ but $I \underset{3}{\not\sim} J$. This contradicts the fact that the action of G on N is assumed to be binary. Hence we conclude that, for any $a, b \in A$ the intersection of $a_0 \cdot G_a$ and $a_0 \cdot G_b$ is $a_0 \cdot G_{ab}$.

So if a and b are not in the same coset of K, we have $X_a \cap X_b = \emptyset$. On the other hand, if $a = kb$ for some $k \in K \smallsetminus \{1\}$, then $X_a \cap X_b = a_0 \cdot T_0^a \smallsetminus \{a_0\}$, where $T_0^a = T_0^b$. We may put $Z_a = a_0 \cdot T_0^a \smallsetminus \{a_0\}$, and Z_a only depends on the coset of K containing a.

If we write Y_a for the union of all the sets X_{ka}, for $k \in K$, then Y_a is the disjoint union of Z_a and the various $X_{ka} \smallsetminus Z_a$. When a and b are not in the same coset of K, the sets Y_a and Y_b are disjoint.

Now when a does not lie in Ka_0, we have $|a_0 \cdot G_a| = |G_a| = |T|$, since $G_{a_0 a} = \{1\}$, so $|X_a| = |T| - 1$. Also $|a_0 \cdot T_0^a| = |T_0^a| = |T_0|$, so we have $|Z_a| = |T_0| - 1$.

Suppose now that A is the disjoint union of the cosets $Ka_0, Ka_1, \ldots, Ka_s$. The union of the sets Y_{a_i} for $1 \le i \le s$ is disjoint, and it forms a subset of A, so we have

$$s\Big[|T_0| - 1 + |K|(|T| - |T_0|)\Big] \le |N| - |K|\,. \tag{*}$$

Put $e = [N : K]$, so that $s = e - 2$, and put $d = [T : T_0]$. From (*) we have

$$1 - \frac{1}{|T_0|} + |K|(d-1) \le \frac{|N| - |K|}{|T_0|(e-2)}\,, \tag{**}$$

and then using that $|T_0| \ge 2$ and some simple rearrangement, we obtain

$$d < 1 + \frac{1}{2}\left(1 + \frac{1}{e-2}\right) \le 2\,.$$

We have proved that $d = 1$ and $T_0 = T$.

Going back to (*), we are left with

$$|T| \le 1 + \frac{|N|}{e}\left(1 + \frac{1}{e-2}\right) \le 1 + \frac{2|N|}{e} = 1 + 2|K|\,.$$

This concludes the proof. □

§4. The binary actions of $\mathrm{PSL}_2(q)$

This section is devoted to the proof of Theorem 1.2, which was stated in the introduction, and which is reproduced here:

Theorem. *Let $G = \mathrm{PSL}_2(q)$ act on Ω, the set of right cosets of a subgroup $H < G$ and suppose $q \neq 5$. The action is binary if and only if one of the following occurs:*

1. *$H = \{1\}$ and the action is regular;*
2. *$q = 2^a$ for some integer a and H is a Sylow 2-subgroup of G;*
3. *$q = 2^a$ for some odd integer a and $|H| = 3$.*

Since $G = \mathrm{PSL}_2(q)$ has a single conjugacy class of involutions, Theorem 1.1 implies that we need only deal with the case where H has odd order. We must prove that, under the supposition that the action of G on the cosets of H is binary, H is trivial, or else we are in case (3) of the theorem.

A quick look at the subgroup structure of G tells us that if H has odd order, then there are two possibilities:

1. H is cyclic of order dividing $q \pm 1$;
2. q is odd and H is a subgroup of a Borel subgroup of G.

We will make use of a result that follows from results in [Gar15].

Proposition 4.1. *Let $\mathcal{C}$ be a conjugacy class in $\mathrm{PSL}_2(q)$ with $q \geq 3$. Then $\mathcal{C}^2$ contains $\mathcal{C}$.*

We start with the case where H is cyclic of order dividing $q \pm 1$. We make use of the fact that in this case H is a TI-subgroup of $\mathrm{PSL}_2(q)$.

Lemma 4.2. *Let H be a non-trivial cyclic subgroup of $G = \mathrm{PSL}_2(q)$ with $q > 2$ and $|H|$ dividing $q \pm 1$. Then there always exist H_1, H_2, H_3, distinct conjugates of H such that $H_3 \subset H_1.H_2$, unless $q = 2^a$ with a odd and $|H| = 3$ (in which case the H_i's cannot be found).*

In particular the action of G on the set of cosets of H is binary if and only if $q = 2^a$ with a odd and $|H| = 3$.

Proof. Write h for a generator of H. We use the fact that the only conjugates of h that lie in H are h and h^{-1}. Now, by Proposition 4.1, we know that there exist h_1, h_2 conjugate to h such that $h_1 h_2 = h$. If $\langle h_1\rangle \neq \langle h_2\rangle$, then we can take $H_1 = \langle h_1\rangle$, $H_2 = \langle h_2\rangle$ and $H_3 = \langle h\rangle$ and we have $H_3 \subset H_1.H_2$ as required.

Consider the case where $\langle h_1\rangle = \langle h_2\rangle$. In this case either $h_2 = h_1$ or $h_1 = h_1^{-1}$; the latter case is impossible because then $h_1 h_2 = 1 = h$. The former case has h_1^2 a conjugate of h_1 and so $h_1^2 = h_1^{-1}$ and we conclude that $|H| = 3$. The rest of the proof thus assumes that $s = 3$, and that q is not a power of 3.

Here are a few easy facts. An element of $g \in \mathrm{SL}_2(q)$ has order 3 if and only if its trace is -1, if and only if its characteristic polynomial is $X^2 + X + 1$, if and only if it is conjugate to

$$g_0 = \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix}.$$

Write $Z = Z(\mathrm{SL}_2(q))$. It follows that an element $h \in \mathrm{PSL}_2(q)$ has order 3 if and only if $h = gZ$ for g of trace ± 1, if and only if h is conjugate to $g_0 Z$. In particular, the elements of order 3 form just one conjugacy class in G.

We may as well choose $h_1 = g_1 Z$ where

$$g_1 = \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}.$$

Then put $h_2 = g_2 Z$ where

$$g_2 = \begin{pmatrix} x & y \\ z & t \end{pmatrix}$$

and we assume that $x + t = \pm 1$. Then observe that

$$g_1 g_2 = \begin{pmatrix} x - z & y - t \\ x & y \end{pmatrix}.$$

We want to know under what conditions we can choose $x, y, z, t \in \mathbb{F}_q$ such that

$$x + t = \pm 1 \text{ and } xt - yz = 1 \text{ and } x + y - z = \pm 1.$$

With some rearranging we obtain

$$y^2 + (x \pm 1)y + (x^2 \pm x + 1) = 0. \tag{$*$}$$

Note that the two instances of "$\pm$" can be taken independently so, for any value of x with q odd we obtain up to 4 distinct quadratic equations in y.

If q is even, then we need to solve

$$y^2 + (x + 1)y + (x^2 + x + 1) = 0.$$

We set $Y = y + 1$ and $X = x + 1$ and we obtain

$$Y^2 + YX + X^2 = 0\,,$$

which is homogeneous. Hence, either $X = 0$ or else $\lambda^2 + \lambda + 1 = 0$ where $\lambda = Y/X$. The former solution corresponds to $x = 1$ and we obtain $g_1 = g_2$ and so $h_1 = h_2$ and thus H_1 and H_2 are not distinct. The latter equation, $\lambda^2 + \lambda + 1 = 0$, has a solution if and only if a is even, exactly as announced in the statement of the lemma.

It remains to see that when q is odd and not a power of 3, we can find a solution to $(*)$ for some choice of signs, which is different from the solution $x = 1, y = -1$ (so $z = 1, t = 0$) which gives $g_1 = g_2$, and also different from the "opposite" solution which gives $g_1 = -g_2$ (in either case we would have $h_1 = h_2$). We choose to show that there is always a solution to $(*)$ with two "plus" signs, which of course implies that $(x, y) \neq (1, -1)$ and $(x, y) \neq (-1, 1)$.

First we try to find a solution with $x = 0$, which requires us to pick y with $y^2 + y + 1 = 0$. The discriminant of this equation is -3, and so y can be found when -3 is a square in $\mathbb{F}_q$. To finish the proof, we now suppose that -3 is not a square in $\mathbb{F}_q$, and we introduce the quadratic form

$$Q(X, Y, Z) = Y^2 + (X + Z)Y + X^2 + XZ + Z^2\,.$$

Any quadratic form in at least 3 variables over a finite field has a non-zero solution, as is classical (this is a consequence of the Chevalley-Warning Theorem). Let $(x, y, z) \neq (0, 0, 0)$ be such that $Q(x, y, z) = 0$. We claim that $z \neq 0$. Indeed, we have

$$Q(x, y, 0) = y^2 + xy + x^2\,,$$

so that $Q(x, y, 0) = 0$ implies

$$\left(x + \frac{1}{2}y\right)^2 + \frac{3}{4}y^2 = 0\,,$$

so that

$$-3 = \frac{2^2(x + \frac{1}{2}y)^2}{y^2} \in \mathbb{F}_q^{*2}\,.$$

This is at odds with our current assumption on the field $\mathbb{F}_q$, so $z \neq 0$. Now write

$$0 = \frac{1}{z^2}Q(x, y, z) = y_1^2 + (x_1 + 1)y_1 + x_1^2 + x_1 + 1$$

with $x_1 = \frac{x}{z}$ and $y_1 = \frac{y}{z}$. We are done.

The "in particular" now follows from Lemma 2.3. $\square$

We are left with the case where p is odd and H is a non-trivial odd-order subgroup of a Borel subgroup of G. We may assume that H is not cyclic of order dividing $q \pm 1$, hence we assume that $U_0 = O_p(H)$ is non-trivial. Then, by the structure of Borel subgroups of G, either $H = U_0$ (i.e. H is a p-group) or $H = U_0 \rtimes T_0$ where T_0 is cyclic of odd order dividing $q - 1$.

This case is dealt with in four lemmas. We emphasise that we assume that p is odd for the rest of this section. Since we are assuming that H is non-trivial, we must show that the action of G is not binary.

Lemma 4.3. *If $H \neq O_p(H)$, then the action of G on the set of cosets of H is not binary.*

Proof. In this case $H = U_0 \rtimes T_0$ where $U_0 = O_p(H)$ and T_0 is a non-trivial cyclic group of order at least 3 and dividing $q - 1$. Note that T_0 acts fixed-point-freely on U_0.

Let U be the unique Sylow p-subgroup containing U_0. Note that $N_G(T_0)$ is dihedral of order $q - 1$; what is more $N_G(T_0)$ has an index 2 subgroup T that is cyclic of order $\frac{q-1}{2}$, that contains T_0 and that satisfies $N_G(U) = U \rtimes T$.

Now let $h \in N_G(T_0) \backslash T$ and observe that $H \cap H^h$ contains T_0. On the other hand, since Sylow p-subgroups of G are TI-subgroups, $U \cap U^h = \{1\}$ and so $U_0 \cap U_0^h = \{1\}$. We conclude that $H \cap H^g = T_0$.

This implies, in particular, that H acts as a Frobenius group on the suborbit corresponding to H^g and T_0 is the corresponding Frobenius complement. Thus Lemma 2.10 implies that, since $|T_0| > 2$, this action of H is not binary and now Lemma 2.9 yields the result we seek. □

Lemma 4.4. *Let q be an odd prime power. Define*

$$C := \{x \in \mathbb{F}_q \mid x \text{ and } x+1 \text{ are nonzero squares}\}.$$

Then

$$|C| = \begin{cases} \frac{q-5}{4}, & \text{if } q \equiv 1 \pmod 4; \\ \frac{q-3}{4}, & \text{if } q \equiv 3 \pmod 4. \end{cases}$$

Proof. Suppose first that -1 is not a square in $\mathbb{F}_q$, that is, suppose $q \equiv 3 \bmod 4$. The map

$$f \colon \mathbb{F}_q \setminus \{0, 1, -1\} \longrightarrow C$$

defined by $f(x) = \left(\frac{x - x^{-1}}{2}\right)^2$ is well-defined, as follows from the observation that

$$\left(\frac{x - x^{-1}}{2}\right)^2 + 1 = \left(\frac{x + x^{-1}}{2}\right)^2,$$

and our assumption on q guarantees that $x + x^{-1} \neq 0$. However, f is also onto: if $b^2 \in C$, we have $b^2 + 1 = a^2$ for some a, so that putting $x = a + b$ yields $x^{-1} = a - b$, and thus $b^2 = f(x)$.

Fix y such that $y - y^{-1} \neq 0$, and let us count the number of x such that $x - x^{-1} = y - y^{-1}$. Considering the discriminant, we conclude that there are two possible values of x when $y^2 \neq -1$, and of course this is always the case given our current assumptions. As a result, the equation $f(x) = f(y)$ has always four solutions, as it amounts to $x - x^{-1} = \pm(y - y^{-1})$, and the size of C is $\frac{q-3}{4}$.

When $q \equiv 1 \bmod 4$ on the other hand, writing i for an element of $\mathbb{F}_q$ with $i^2 = -1$, we use the map f defined on $\mathbb{F}_q \setminus \{0, \pm 1, \pm i\}$ by the same formula as above, and argue similarly. □

Lemma 4.5. *Let U be a Sylow p-subgroup of G, let g be a non-trivial element of U and let $\mathcal{C}$ be the conjugacy class of g in G. If $q \neq 9$, then the component group of g in $\Gamma(\mathcal{C})$ is equal to U.*

Note that if $q = 9$, the the component group of g in $\Gamma(\mathcal{C})$ is equal to $\langle g \rangle$.

Proof. Recall that there are two conjugacy classes of p-elements in G and that $|\mathcal{C} \cap U| = \frac{q-1}{2}$. Consider $\Gamma_{\mathcal{C},U}$, the subgraph induced on $U \cap \mathcal{C}$ in $\Gamma(\mathcal{C})$.

It is easy to see that $\Gamma_{\mathcal{C},U}$ is isomorphic to the graph Δ whose vertices are nonzero squares in $\mathbb{F}_q$, with two vertices, x and y, connected if and only if $x - y$ or $y - x$ is a square in $\mathbb{F}_q$.

If $q \equiv 3 \pmod 4$, then -1 is not a square in $\mathbb{F}_q$ and, for all $x, y \in \mathbb{F}_q$, exactly one of $x - y$ and $y - x$ is a square in $\mathbb{F}_q$. We conclude that $\Gamma_{C,U}$ is connected and so the component group of g contains $\frac{q-1}{2}$ elements. We conclude that the component group of g is U.

If $q \equiv 1 \pmod 4$, then we use Lemma 4.4. We claim that each vertex in $\Gamma_{\mathcal{C},U}$ has valency $v = \frac{q-5}{4}$. To see this, write $x_1, \dots, x_v$ for the set of elements x in $\mathbb{F}_q$ with the property that x and $x+1$ are squares. Now, let y be a square in $\mathbb{F}_q$ and observe that y is connected to $y+yx_1, \dots, y+yx_v$ in $\Gamma_{\mathcal{C},U}$. This implies that a connected component of $\Gamma_{\mathcal{C},U}$ contains at least $\frac{q-1}{4}$ elements. Since all connected components contain the same number of elements, we either have that $\Gamma_{\mathcal{C},U}$ is connected (and we are done, as per the previous paragraph) or else $\Gamma_{\mathcal{C},U}$ has two connected components. Assume the latter. Also, let U' be the component group of g, and assume that $U' \neq U$; we must show that $q = 9$.

Suppose first that $q \leq 15$. Since q is an odd prime power, which is not prime (as this would imply $U' = U$), we deduce that $q = 9$. So we may as well suppose that $q > 15$ and look for a contradiction. Under this assumption however, we have $\frac{q-1}{4} + 1 > \frac{q}{5}$, so we see that the index of U' in U is 3, and that q is a power of 3.

The situation is as follows: $\Gamma_{\mathcal{C},U}$ has two connected components, each containing $\frac{q-1}{4}$ vertices and, since the valency of each vertex is $\frac{q-5}{4}$, each is isomorphic to a complete graph. Write X_1 and X_2 for each component and note that $\langle X_1 \rangle$ and $\langle X_2 \rangle$ are both index 3 subgroups of U. We see also that $\langle X_1 \rangle$ and $\langle X_2 \rangle$ together comprise at least $\frac{q-1}{2}$ elements and, since this exceeds $\frac{q}{3}$, these two subgroups generate U. Finally note that, since the difference of any two vertices in X_1 (resp. X_2) is a square, $\langle X_1 \rangle \cup \langle X_2 \rangle \subseteq X_1 \cup X_2 \cup \{0\}$, the set of squares in $\mathbb{F}_q$. But now

$$\frac{q}{3} + \frac{q}{3} - \frac{q}{9} = |\langle X_1 \rangle \cup \langle X_2 \rangle| \leq X_1 \cup X_2 \cup \{0\} = \frac{q+1}{2}$$

and we obtain that $q \leq 9$, a contradiction which finishes the proof. □

Lemma 4.6. *If $H = O_p(H)$, then the action of G on the set of cosets of H is not binary.*

Proof. In this case, H is a non-trivial p-group. Let g be a p-element of maximal fixity. Lemma 4.5 and Theorem 2.5 imply that either $q = 9$ and $|H| = 3$ or else H is equal to a Sylow p-subgroup of G. If $q = 9$, then $G = A_6$ and the lemma follows from [GG] (or can be checked directly using GAP). Thus we assume that H is a Sylow p-subgroup of G.

We observe that

$$\begin{pmatrix} -3 & 1 \\ -4 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -4 & 1 \end{pmatrix}. \tag{4.1}$$

We let h_1 (resp h_2, h_3) be the projective image in G of the first (resp. second, third) matrix of (4.1).

Note that all matrices in (4.1) have trace equal to ± 2, hence h_1, h_2 and h_3 are all p-elements. Note, too, that h_1 is the image of an upper-triangular matrix, h_2 is the image of a lower-triangular matrix and h_3 is the image of a matrix that is neither upper nor lower-triangular. Thus h_1, h_2, h_3 lie in distinct Sylow p-subgroups of G which we denote H_1, H_2 and H_3, respectively. Now, since $h_1 \in H_1 \cap H_2 \cdot H_3$, Lemma 2.3 gives the result. □

We remark that it is easy to use a similar strategy to classify the transitive binary actions of the Suzuki groups.

Theorem 4.7. *Let $G = {}^2B_2(2^{2a+1})$, with $a \geq 1$, act on Ω, the set of right cosets of a subgroup $H < G$. The action is binary if and only if one of the following occurs:*

1. *$H = \{1\}$ and the action is regular;*
2. *H is the centre of a Sylow 2-subgroup of G.*

Proof. The group G has a unique class of involutions hence, when $|H|$ is even, the result follows from Theorem 1.1. Assume, then, that $|H| > 1$ is odd. Consulting [Suz62] we see that in this case $|H|$ is cyclic of order dividing $q-1$, $q-r+1$ or $q+r+1$ where $q = 2^{2a+1}$ and $r = 2^{a+1}$. What is more H is a TI-subgroup.

Let h be a generator of H and let $N = N_G(H)$. Consider the action of N on the set of non-trivial elements of H. Again referring to [Suz62] it is easy to see that the orbits in this action are of size at most 4, hence h is conjugate in G to at most 4 of its powers (including itself).

Let $\mathcal{C}$ be the conjugacy class of G containing h and recall the standard formula (see, for instance, [Isa94, p. 45]):

$$|\{(x,y) \in \mathcal{C} \mid xy = h\}| = \frac{|\mathcal{C}|^2}{|G|} \sum_{\chi \in \mathrm{Irr}(G)} \frac{\chi(h)^2 \overline{\chi(h)}}{\chi(1)}.$$

Using the character table given in [Suz62, §17], together with this formula, it is easy to check that, for any fixed H of odd order, the value of the expression on the right-hand side of the formula is strictly greater than 4. Thus we can find $x, y \in \mathcal{C}$ with $x, y \notin H$ such that $xy = H$. Now set $H_1 = \langle h \rangle = H$, $H_2 = \langle x \rangle$ and $H_3 = \langle y \rangle$ and observe that these are distinct conjugates of H. By construction $h \in H_1 \cap H_2 \cdot H_3$ and so Lemma 2.3 implies the result. □

References

[Asc73] Michael Aschbacher, *A condition for the existence of a strongly embedded subgroup*, Proc. Am. Math. Soc. **38** (1973), 509–511 (English).

[Ben71] Helmut Bender, *Transitive Gruppen gerader Ordnung, in denen jede Involution genau einen Punkt fest läßt*, J. Algebra **17** (1971), 527–554.

[BHR13] John N. Bray, Derek F. Holt, and Colva M. Roney-Dougal, *The maximal subgroups of the low-dimensional finite classical groups*, London Mathematical Society Lecture Note Series, vol. 407, Cambridge University Press, Cambridge, 2013.

[CCN+85] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, and R. A. Wilson, *Atlas of finite groups*, Oxford University Press, 1985. MR 827219

[Che16] Gregory Cherlin, *On the relational complexity of a finite permutation group*, J. Alg. Combin. **43** (2016), no. 2, 339–374. MR 3456493

[GAP16] The GAP Group, *GAP – Groups, Algorithms, and Programming, Version 4.8.4*, 2016.

[Gar15] Shelly Garion, *Expansion of conjugacy classes in* $\mathrm{PSL}_2(q)$., J. Group Theory **18** (2015), no. 6, 961–980.

[GG] Nick Gill and Pierre Guillot, *The binary actions of alternating groups*, arXiv 2303.06003.

[GGL] Nick Gill, Pierre Guillot, and Martin W. Liebeck, *The binary actions of simple groups of lie type of characteristic 2*, arXiv 2402.08357.

[GHS19] Nick Gill, Francis Hunt, and Pablo Spiga, *Cherlin's conjecture for almost simple groups of Lie rank 1*, Math. Proc. Camb. Philos. Soc. **167** (2019), no. 3, 417–435.

[Gla66] George Glauberman, *Central elements in core-free groups*, J. Algebra **4** (1966), 403–420.

[GLS98] Daniel Gorenstein, Richard Lyons, and Ronald Solomon, *The classification of the finite simple groups. Number 3. Part I. Chapter A*, Mathematical Surveys and Monographs, vol. 40, American Mathematical Society, Providence, RI, 1998.

[GLS22] Nick Gill, Martin W. Liebeck, and Pablo Spiga, *Cherlin's conjecture for finite primitive binary permutation groups*, Lect. Notes Math., vol. 2302, 2022.

[Isa94] I. Martin Isaacs, *Character theory of finite groups.*, corr. repr. of the 1976 orig. ed., New York, NY: Dover Publications, Inc., 1994 (English).

[KL90] P. Kleidman and M. Liebeck, *The subgroup structure of the finite classical groups*, London Mathematical Society Lecture Note Series, vol. 129, Cambridge University Press, Cambridge, 1990. MR 1057341 (91g:20001)

[Suz62] Michio Suzuki, *On a class of doubly transitive groups.*, Ann. Math. (2) **75** (1962), 105–145.

[Suz64] Michio Suzuki, *On a class of doubly transitive groups. II*, Ann. Math. (2) **79** (1964), 514–589.

[Wis16] Joshua Wiscons, *A reduction theorem for primitive binary permutation groups.*, Bull. Lond. Math. Soc. **48** (2016), no. 2, 291–299.