Hypermaps Over Non-Abelian Simple Groups and Strongly Symmetric Generating Sets

Andrea Lucchini[a] Pablo Spiga[b]

Submitted: Mar 5, 2021; Accepted: Mar 30, 2023; Published: Jul 28, 2023

Abstract

A generating pair x, y for a group G is said to be *symmetric* if there exists an automorphism $\varphi_{x,y}$ of G inverting both x and y, that is, $x^{\varphi_{x,y}} = x^{-1}$ and $y^{\varphi_{x,y}} = y^{-1}$. Similarly, a group G is said to be *strongly symmetric* if G can be generated with two elements and if all generating pairs of G are symmetric.

In this paper we classify the finite strongly symmetric non-abelian simple groups. Combinatorially, these are the finite non-abelian simple groups G such that every orientably regular hypermap with monodromy group G is reflexible.

Mathematics Subject Classifications: 05C10, 05C25, 20B25

1 Introduction

The aim of this note is to classify the finite strongly symmetric non-abelian simple groups.

Theorem 1. Let S be a finite non-abelian simple group. Then S is strongly symmetric if and only if $S \cong \mathrm{PSL}(2, q)$ for some prime power q.

Interest on strongly symmetric groups stems from maps and hypermaps, which (roughly speaking) are embeddings of graphs on surfaces, see [6]. We give a brief account on this connection, for more details see [4, 10].

A map on a surface is a decomposition of a closed connected surface into vertices, edges and faces. The vertices and edges of this decomposition form the underlying graph of the map. An automorphism of a map is an automorphism of the underlying graph which can be extended to a homeomorphism of the whole surface. For the definition of hypermaps, which bring us closer to strongly symmetric groups, we need to take a more combinatorial point of view.

Each map on a orientable surface can be described by two permutations, usually denoted by R and L, acting on the set of directed edges (that is, ordered pairs of adjacent

[a]Dipartimento di Matematica "Tullio Levi-Civita", University of Padova, Via Trieste 63, 35121 Padova, Italy (lucchini@math.unipd.it).
[b]Dipartimento di Matematica Pura e Applicata, University of Milano-Bicocca, Via Cozzi 55, 20126 Milano, Italy (pablo.spiga@unimib.it).

vertices) of the underlying graph. The permutation R permutes cyclically the directed edges starting from a given vertex and preserving a chosen orientation of the surface. The permutation L interchanges the end vertices of a given directed edge. The monodromy group of the surface is the group generated by R and L and the map is said to be regular if the monodromy group acts regularly, that is, the identity is the only permutation fixing some element.

Observe that in a map, we have $L^2 = 1$. A hypermap is simply given by the combinatorial data R and L, where L is not necessarily an involution. Inspired by the topological and geometrical counterpart for maps, a hypermap is said to be reflexible if the assigment $R \mapsto R^{-1}$ and $L \mapsto L^{-1}$ extends to a group automorphism of $\langle R, L\rangle$; otherwise the hypermap is said to be chiral.

It was shown in [4, Lemma 7], that a finite group G is strongly symmetric if and only if every orientably regular hypermap with monodromy group G is reflexible. In particular, Theorem 1 classify the finite non-abelian simple groups G with the property that every orientably regular hypermap with monodromy group G is reflexible.

In our opinion, Theorem 1 suggests a natural problem, which in principle should give a measure of how chirality is abundant among regular hypermaps. Let S be a non-abelian simple group and let $\delta(S)$ be the proportion of strongly symmetric generating sets of S, that is,

$$\delta(S) := \frac{|\{(x,y) \in S \times S \mid x, y \text{ symmetric generating set}\}|}{|\{(x,y) \in S \times S \mid S = \langle x, y\rangle\}|}.$$

The closer $\delta(S)$ is to 1, the more abundant reflexible hypermaps are among orientably regular hypermaps with monodromy group S. Indeed, Theorem 1 classifies the groups S attaining 1. We do not have any "running conjecture", but we wonder whether statistically it is frequent the case that $\delta(S) < 1/2$. Moreover, we wonder whether it is statistically significant the case that $\delta(S) \to 0$ as $|S| \to \infty$, as S runs through a certain family of non-abelian simple groups.[1]

2 Proof of Theorem 1

We start with a preliminary lemma.

Lemma 1. *Let n be an integer with $n \geqslant 3$, let q be a prime power with $(n,q) \neq (3,4)$, let $g \in \mathrm{GL}(n,q)$ be a Singer cycle of order $q^n - 1$, let $x := g^{\gcd(n,q-1)}$ and let $a \in \Gamma\mathrm{L}(n,q)$ such that $x^a = zx^{\varepsilon}$, for some $z \in \mathbf{Z}(\mathrm{GL}(n,q))$ and $\varepsilon \in \{-1,1\}$. Then $z = 1$, $\varepsilon = 1$ and $a \in \langle g\rangle$.*

Proof. Let $e_1, \ldots, e_n$ be the canonical basis of the n-dimensional vector space $\mathbb{F}_q^n$ of row vectors over the finite field of cardinality q. Set $v := e_1$ and let P_1 be the stabilizer in $\mathrm{GL}(n,q)$ of the vector v. As $\langle g\rangle$ acts transitively on the set of non-zero vectors of $\mathbb{F}_q^n$ and as P_1 is the stabilizer of the non-zero vector v, we deduce from the Frattini argument

[1] During the refereeing process of this paper, Theorem 1 has proved to be useful in [7, page 2 and 3] for the proof of Cherlin's conjecture on finite primitive binary permutation groups.

that $\mathrm{GL}(n,q) = \langle g\rangle P_1$. In particular, as $a \in \Gamma\mathrm{L}(n,q)$, we have $a = g^i bc$, where $i \in \mathbb{Z}$, $b \in P_1$ and c lies in the Galois group $\mathrm{Gal}(\mathbb{F}_q)$ of the field $\mathbb{F}_q$. Set $a' := bc$. Observe that $x^a = x^{a'}$ because g^i centralizes $x \in \langle g\rangle$. Moreover, $a \in \langle g\rangle$ if and only if $a' \in \langle g\rangle$. Therefore, replacing a with a' if necessary, in the rest of the argument we may suppose that $a = a' = bc$.

As $\mathbf{Z}(\mathrm{GL}(n,q))$ consists of scalar matrices, we may identify the matrix z with an element in the field $\mathbb{F}_q$. We show that, for every $\ell \in \mathbb{N}$, we have $(vx^\ell)^a = z^\ell v x^{\varepsilon\ell}$. When $\ell = 0$, $v^a = v^{bc} = v$, because b and c fix the vector $v = e_1$. When $\ell > 0$, we have

$$(vx^\ell)^a = v^a (x^\ell)^a = v(x^\ell)^a = v(x^a)^\ell = v(zx^\varepsilon)^\ell = v(z^\ell x^{\varepsilon\ell}) = z^\ell v x^{\varepsilon\ell}.$$

Observe that $v, vx, \dots, vx^{n-1}$ is a basis of $\mathbb{F}_q$ and hence there exists $a_0, a_1, \dots, a_{n-1} \in \mathbb{F}_q$ with

$$vx^n = a_0 v + a_1 vx + \cdots + a_{n-1} vx^{n-1}. \tag{2.1}$$

Now, by applying a on both sides of this equality and using the previous paragraph, we obtain

$$z^n v x^{\varepsilon n} = a_0^c v + a_1^c z v x^\varepsilon + \cdots + a_{n-1}^c z^{n-1} v x^{\varepsilon(n-1)}. \tag{2.2}$$

We let $f(T) := T^n - a_{n-1}T^{n-1} - a_{n-2}T^{n-2} - \cdots - a_1 T - a_0 \in \mathbb{F}_q[T]$ be the characteristic polynomial of the matrix x. Observe that $f(T)$ is irreducible in $\mathbb{F}_q[T]$ because $x = g^{\gcd(n,q-1)}$ acts irreducibly on $\mathbb{F}_q^n$. Let $\lambda \in \mathbb{F}_{q^n}$ be a root of $f(T)$ and observe that λ generates the field extension $\mathbb{F}_{q^n}/\mathbb{F}_q$. Observe that λ has order $(q^n-1)/\gcd(n,q-1)$ in the multiplicative group $\mathbb{F}_q^*$, because so does x. Now, let $f^c(T) = T^n - a_{n-1}^c T^{n-1} - a_{n-2}^c T^{n-2} - \cdots - a_1^c T - a_0^c \in \mathbb{F}_q[T]$ be the image of the polynomial $f(T) \in \mathbb{F}_q[T]$ under the Galois automorphism $c \in \mathrm{Gal}(\mathbb{F}_q)$. Clearly, the roots of $f(T)$ are

$$\lambda, \lambda^q, \dots, \lambda^{q^{n-1}}$$

and the roots of $f^c(T)$ are

$$\lambda^c, \lambda^{cq}, \dots, \lambda^{cq^{n-1}}.$$

Moreover, let $\kappa \in \mathbb{N}$ with $q = p^\kappa$, for some prime number p, and let $j \in \{0, \dots, \kappa-1\}$ with $\omega^c = \omega^{p^j}$, $\forall \omega \in \mathbb{F}_q$.

We now distinguish the cases, depending on whether $\varepsilon = 1$ or $\varepsilon = -1$. Assume $\varepsilon = 1$. Using (2.1) and (2.2) and using the fact that $f(\lambda) = 0$, we get $f^c(z\lambda) = 0$. Therefore, we deduce $z\lambda$ is a root of $f^c(T)$ and hence, there exists $i \in \{0, \dots, n-1\}$, with $\lambda^{cq^i} = z\lambda$. This gives $\lambda^{cq^i - 1} = z \in \mathbb{F}_q^*$ and hence $\lambda^{(cq^i-1)(q-1)} = 1$. Since λ has order $(q^n-1)/\gcd(n,q-1)$, this implies

$$\frac{q^n-1}{\gcd(n,q-1)} \text{ divides } (p^j q^i - 1)(q-1). \tag{2.3}$$

If $p^j q^i - 1 = 0$, then $j = 0$ and $i = 0$. This implies $c = 1$ and $z = 1$ and the lemma follows in this case. Suppose $p^j q^i - 1 \neq 0$. Assume further that $(\kappa n, p) \neq (6,2)$. Then Zsigmondy's theorem guarantees the existence of a primitive prime divisor r of $p^{\kappa n} - 1$. Clearly r does not divide $p^j q^i - 1 = p^{j+\kappa i} - 1$ and hence we contradict (2.3). Finally, assume $(n\kappa, p) = (6, 2)$. Since we are excluding the case $(n, q) = (3, 4)$ in the statement of this lemma, we have $(n, q) = (6, 2)$. In particular, have $\kappa = 1$ and hence $z = 1$ and the proof follows again.

Assume $\varepsilon = -1$. Using (2.1) and (2.2) and using the fact that $f(\lambda) = 0$, we obtain that $z\lambda^{-1}$ is a root of $f^c(T)$ and hence, there exists $i \in \{0, \ldots, n-1\}$, with $\lambda^{cq^i} = z\lambda^{-1}$. This gives $\lambda^{cq^i+1} = z \in \mathbb{F}_q^*$ and hence $\lambda^{(p^jq^i+1)(q-1)} = 1$. Since λ has order $(q^n-1)/\gcd(n, q-1)$, this implies

$$\frac{q^n-1}{\gcd(n, q-1)} \text{ divides } (p^jq^i+1)(q-1). \tag{2.4}$$

An argument similar to the one above shows that (2.4) is never possible. $\square$

Proof of Theorem 1. Macbeath has proved in [11] that, for every prime power q, $\mathrm{PSL}(2, q)$ is strongly symmetric; see also [4, Proposition 8]. In particular, for the rest of the proof, we let S be a finite strongly symmetric non-abelian simple group and our task is to show that $S \cong \mathrm{PSL}(2, q)$, for some prime power q.

Observe that, if $S = \langle s_1, s_2 \rangle$ and $\alpha \in \mathrm{Aut}(S)$ inverts both s_1 and s_2, then

$$\alpha^2 \in \mathbf{C}_{\mathrm{Aut}(S)}(s_1) \cap \mathbf{C}_{\mathrm{Aut}(S)}(s_2) = \mathbf{C}_{\mathrm{Aut}(S)}(\langle s_1, s_2 \rangle) = \mathbf{C}_{\mathrm{Aut}(S)}(S) = 1.$$

If α is the identity automorphism, then s_1, s_2 are involutions and hence $S = \langle s_1, s_2 \rangle$ is a dihedral group, contradicting the fact that S is a non-abelian simple group. Therefore α has order 2, that is, α is an involution of $\mathrm{Aut}(S)$.

In [10, Theorem 1.1], Leemans and Liebeck have proved that, if T is a finite non-abelian simple group that is not isomorphic to $\mathrm{Alt}(7)$, to $\mathrm{PSL}(2, q)$, to $\mathrm{PSL}(3, q)$ or to $\mathrm{PSU}(3, q)$, then there exist $x, s \in S$ such that the following hold:

(i) $T = \langle x, s \rangle$;

(ii) s is an involution;

(iii) there is no involution $\alpha \in \mathrm{Aut}(T)$ such that $x^\alpha = x^{-1}$, $s^\alpha = s$.

In particular, if S is not isomorphic to $\mathrm{Alt}(7)$, to $\mathrm{PSL}(2, q)$, to $\mathrm{PSL}(3, q)$ or to $\mathrm{PSU}(3, q)$, then S is not strongly symmetric. In the rest of this proof, we deal with each of these cases separately.

Assume $S = \mathrm{Alt}(7)$; in particular, $\mathrm{Aut}(S) = \mathrm{Sym}(7)$. Let $s_1 := (1, 2, 3, 4, 5, 6, 7)$ and $s_2 := (1, 2, 3, 4, 6, 7, 5)$ and, for $i \in \{1, 2\}$, let $\Delta_i := \{\alpha \in \mathrm{Sym}(7) \mid s_i^\alpha = s_i^{-1}\}$. It can be easily checked that $S = \langle s_1, s_2 \rangle$ and

$$\begin{aligned}\Delta_1 = \{&(2,7)(3,6)(2,4), (1,7)(2,6)(3,5), (1,6)(2,5)(3,4), (1,5)(2,4)(6,7),\\ &(1,4)(2,3)(5,7), (1,3)(4,7)(5,6), (1,2)(3,7)(4,6)\},\end{aligned}$$

$$\begin{aligned}\Delta_2 = \{&(2,5)(3,7)(4,6), (1,5)(2,7)(3,6), (1,7)(2,6)(3,4), (1,6)(2,4)(5,7),\\ &(1,4)(2,3)(5,6), (1,3)(4,5)(6,7), (1,2)(3,5)(4,7)\}.\end{aligned}$$

Since $\Delta_1 \cap \Delta_2 = \varnothing$, the generating pair s_1, s_2 of $\mathrm{Alt}(7)$ witnesses that $\mathrm{Alt}(7)$ is not strongly symmetric.

Assume $S = \mathrm{PSL}(3,q)$. Since $\mathrm{PSL}(3,2) = \mathrm{PSL}(2,7)$, we may assume $q > 2$. Moreover, we have verified with a computer that $\mathrm{PSL}(3,4)$ is not strongly symmetric.

Let $A := \mathrm{Aut}(S)$, let $d := \gcd(3, q-1)$ and let ι be the graph automorphism of $\mathrm{PSL}(3,q)$ defined via the inverse-transpose mapping $x \mapsto x^\iota = (x^{-1})^T$, for every $x \in \mathrm{PSL}(3,q)$, where x^T denotes the transpose of the element x of $\mathrm{PSL}(3,q)$. Since $x \in \mathrm{PSL}(3,q)$ is not a single matrix, but a coset of the center $\mathbf{Z}(\mathrm{SL}(3,q))$ in $\mathrm{SL}(3,q)$, there is a slight abuse of notation when we talk about the transpose of the coset x. However, since $\mathbf{Z}(\mathrm{SL}(3,q))$ consists of diagonal matrices, this should cause no confusion.

Next, let Ω_1 be the set of cyclic subgroups of S generated by a Singer cycle of order $(q^2+q+1)/d$ and, for any $K \in \Omega_1$, let

$$\Delta_K := \{\alpha \in A \mid \alpha^2 = 1,\, k^\alpha = k^{-1}\ \forall k \in K\}.$$

Observe that the set Ω_1 consists of a single S-conjugacy class.

Let $K \in \Omega_1$, let $k \in K$ be a generator of K and let $\alpha, \beta \in \Delta_K$. Then $k^\alpha = k^{-1} = k^\beta$ and hence $\beta^{-1}\alpha \in \mathbf{C}_{\mathrm{Aut}(S)}(k)$. This shows that $\Delta_K \subseteq \mathbf{C}_{\mathrm{Aut}(S)}(k)\alpha$ and that Δ_K consists of the involutions in $\mathbf{C}_{\mathrm{Aut}(S)}(k)\alpha$.

From [2, Theorem 8], we see that there exists a symmetric matrix $g \in \mathrm{GL}(3,q)$ having order q^3-1. Let $\bar{g}$ be the projection of g in $\mathrm{PGL}(3,q)$. The element $h := \bar{g}^d$ generates a subgroup $H \in \Omega_1$. Since g is symmetric, $g = g^T$ and hence $h^\iota = h^{-1}$, that is, $\iota \in \Delta_H$ and Δ_H consists of the involutions contained in $\mathbf{C}_{\mathrm{Aut}(S)}(h)\iota$. From Lemma 1, we deduce that, if $a \in \mathrm{P\Gamma L}(3,q)$ and $h^a = h^\varepsilon$ with $\varepsilon \in \{1,-1\}$, then $\varepsilon = 1$ and $a \in \langle \bar{g} \rangle$. As $\bar{g}^\iota = \bar{g}^{-1}$, we deduce $\mathbf{C}_{\mathrm{Aut}(S)}(h) = \langle \bar{g} \rangle$ and that $\langle \bar{g}, \iota \rangle$ is a dihedral group of order $2(q^2+q+1)$. Thus

$$|\Delta_H| = q^2+q+1. \tag{2.5}$$

Let Ω_2 be the set of the conjugates of ι in A. Given $y \in \Omega_2$, we want to determine the number δ_y of subgroups $K \in \Omega_1$ with the property that $y \in \Delta_K$. Consider the bipartite graph having vertex set $\Omega_1 \cup \Omega_2$ and having edge set consisting of the pairs $\{K, y\}$ with $K \in \Omega_1, y \in \Omega_2$ and $y \in \Delta_K$. Since Ω_1 and Ω_2 both consist of a single A-conjugacy class, the group A acts as a group of automorphisms on our bipartite graph with orbits Ω_1 and Ω_2. Thus, the number of edges of the bipartite graph is $|\Omega_1||\Delta_H| = |\Omega_2|\delta_y$. Therefore, for every $y \in \Omega_1$, we have

$$\delta_y = \frac{|\Omega_1||\Delta_H|}{|\Omega_2|}. \tag{2.6}$$

Let ω_H be the number of $K \in \Omega_1$ with $\Delta_H \cap \Delta_K \neq \varnothing$. Clearly

$$\omega_H \leqslant \delta_y |\Delta_H|. \tag{2.7}$$

We claim that there exists $K \in \Omega_1$ with $\Delta_H \cap \Delta_K = \varnothing$. From (2.5), (2.6) and (2.7), it suffices to show that

$$|\Omega_1| > \delta_y|\Delta_H| = \frac{|\Omega_1||\Delta_H|^2}{|\Omega_2|} \geqslant \omega_H$$

or, equivalently, that

$$|A : \mathbf{C}_A(\iota)| = |\Omega_2| > |\Delta_H|^2 = (q^2 + q + 1)^2.$$

Let $G = \mathrm{InnDiag}(S) = \mathrm{PGL}(3, q)$. From [8, Chapter 4] or [5, Proposition 3.2.11], we have $\mathbf{C}_G(\iota) = \mathrm{Sp}(2, q)$ when q is even and $\mathbf{C}_G(\iota) = \mathrm{PGO}(2, q)$ when q is odd. Thus, in both cases, we have

$$|A : \mathbf{C}_A(\iota)| \geqslant |G : \mathbf{C}_G(\iota)| = \frac{(q^3 - 1)(q^2 - 1)q^3}{(q^2 - 1)q} = (q^3 - 1)q^2.$$

As $q > 2$, it follows $|A : \mathbf{C}_A(\iota)| > (q^2 + q + 1)^2$ and our claim is now proved.

Now choose $K = \langle y \rangle \in \Omega_1$ such that $\Delta_H \cap \Delta_K = \varnothing$. We use the list of the maximal subgroups of $S = \mathrm{PSL}(3, q)$, see [3, Table 8.3]. When $q \neq 4$, $\mathbf{N}_S(H)$ is a maximal subgroup of S isomorphic to $H : 3$ and hence $\langle h, y \rangle = S$. In particular, h, y is a generating pair of S witnessing that S is not strongly symmetric. When $q = 4$, we have used the computer algebra system `magma` [1] to show that $\mathrm{PSL}(3, 4)$ is not strongly symmetric.

Let $S = \mathrm{PSU}(3, q)$ and $A = \mathrm{Aut}(S)$. Since $\mathrm{PSU}(3, 2)$ is solvable, $q > 2$. Let $A := \mathrm{Aut}(S)$, let $d := \gcd(3, q + 1)$ and let Ω_1 be the set of cyclic subgroups of S generated by a Singer cycle of order $(q^2 - q + 1)/d$ and, for any $K \in \Omega_1$, let

$$\Delta_K := \{\alpha \in A \mid \alpha^2 = 1,\ k^\alpha = k^{-1}\ \forall k \in K\}.$$

Observe that the set Ω_1 consists of a single S-conjugacy class.

Let ϕ be the automorphism of S induced by the Frobenius automorphism $x \mapsto x^q$ of the underlying finite field $\mathbb{F}_{q^2}$ of order q^2. We recall now some main facts about Singer cycles. Let $\mathbb{F}_{q^6}$ be the field with q^6 elements and let $a \in \mathbb{F}_{q^6}$ with $a \neq 0$. Consider the multiplication $\pi_a : \mathbb{F}_{q^6} \to \mathbb{F}_{q^6}$ defined by $\pi_a(x) = ax$, for all $x \in \mathbb{F}_{q^6}$. For every divisor d of 6, the set $V = \mathbb{F}_{q^6}$ can be interpreted as a vector space of dimension $6/d$ over the field $\mathbb{F}_{q^d}$ and the map π_a is a $\mathbb{F}_{q^d}$-linear transformation of V. Thus, once a base is fixed, π_a induces a matrix belonging to $\mathrm{GL}(6/d, q^d)$. Now, let a be a generator of the multiplicative field of $\mathbb{F}_{q^6}$. Then, by [9, Theorem 5.2], the multiplication π_{q^3-1} seen as a $\mathbb{F}_{q^2}$-linear transformation of $\mathbb{F}_{q^6}$ induces a Singer cycle g for $\mathrm{GU}(3, q)$ having order $q^3 + 1$. Moreover,

$$g^\phi = \pi^\phi_{a^{3}-1} = \pi_{a^{(q^3-1)q^3}} = \pi_{a^{q^6-q^3}} = \pi_{a^{1-q^3}} = \pi_{a^{-(q^3-1)}} = g^{-1}.$$

Let $\bar{g}$ be the projection of g in $\mathrm{PGU}(3, q)$ and let $h := \bar{g}^d$. Thus $H := \langle h \rangle \in \Omega_1$ and $\phi \in \Delta_H$. Since $\mathbf{C}_{\mathrm{PGU}(3,q)}(\langle \bar{g} \rangle) = \langle \bar{g} \rangle$ and since no field automorphism centralizes H, we deduce that Δ_H is the set of the $q^2 - q + 1$ involutions in the dihedral group $\langle \bar{g}, \phi \rangle$ of order $2(q^2 - q + 1)$ (we are omitting some details here, but these are similar to the arguments in the case of $\mathrm{PSL}(3, q)$). In particular, $|\Delta_H| = q^2 - q + 1$.

Let Ω_2 be the set of the conjugates of ϕ in A. Given $y \in \Omega_2$, we want to determine the number δ_y of subgroups $K \in \Omega_1$ with $y \in \Delta_K$. Arguing as in the previous paragraph, we deduce that

$$\delta_y = \frac{|\Omega_1||\Delta_H|}{|\Omega_2|}.$$

Let ω_H be the number of $K \in \Omega_1$ with $\Delta_H \cap \Delta_K \neq \varnothing$. Clearly

$$\omega_H \leqslant \delta_y |\Delta_H|.$$

We claim that there exists $K \in \Omega_1$ with $\Delta_H \cap \Delta_K = \varnothing$. It suffices to show that

$$|\Omega_1| > \delta_y |\Delta(H)| = \frac{|\Omega_1||\Delta_H|^2}{|\Omega_2|} \geqslant \omega_H$$

or, equivalently, that

$$|A : \mathbf{C}_A(\phi)| = |\Omega_2| > |\Delta_H|^2 = (q^2 - q + 1)^2.$$

Let $G = \mathrm{InnDiag}(S) = \mathrm{PGU}(3, q)$. From [8, Chapter 4] or [5, Proposition 3.3.15], we have $\mathbf{C}_G(\phi) = \mathrm{Sp}(2, q)$ when q is even and $\mathbf{C}_G(\phi) = \mathrm{PGO}(2, q)$ when q is odd. In both cases, it follows

$$|A : \mathbf{C}_A(\phi)| \geqslant |G : \mathbf{C}_G(\phi)| = \frac{(q^3 + 1)(q^2 - 1)q^3}{(q^2 - 1)q} = (q^3 + 1)q^2.$$

It follows $|A : \mathbf{C}_A(\phi)| > (q^2 - q + 1)^2$ and our claim is now proved.

Now choose $K = \langle y \rangle \in \Omega_1$ such that $\Delta_H \cap \Delta_K = \varnothing$. We use the list of the maximal subgroups of $S = \mathrm{PSU}(3, q)$, see [3, Table 8.3]. When $q \notin \{3, 5\}$, $\mathbf{N}_S(H)$ is a maximal subgroup of S isomorphic to $H : 3$ and hence $\langle h, y \rangle = S$. In particular, h, y is a generating pair of S witnessing that S is not strongly symmetric. When $q \in \{3, 4\}$, we have used the computer algebra system `magma` [1] to show that $\mathrm{PSU}(3, 3)$ and $\mathrm{PSU}(3, 5)$ are not strongly symmetric. □

References

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

[2] J. V. Brawley, Similarity to symmetric matrices over finite fields, *Finite Fields and their applications* **4** (1998), 261–274.

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

[4] A. Breda D'Azevedo, G. Jones, R. Nedela and M. Škoviera, Chirality groups of maps and hypermaps, *J. Algebraic Combin.* **29** (2009), no. 3, 337–355.

[5] T. C. Burness, M. Giudici, *Derangements and Primes*, Australian Mathematical Society Lecture Series **25**, Cambridge University Press, 2016.

[6] H. S. M. Coxeter, W. O. J. Moser, *Generators and Relations for Discrete Groups*, 3rd edn. Springer, New York (1972).

[7] N. Gill, M. W. Liebeck, P. Spiga, *Cherlin's Conjecture for Finite Primitive Binary Permutation Groups*, Lecture notes in mathematics **2302**, Springer, 2022.

[8] D. Gorenstein, R. Lyons, R. Solomon, *The classification of the finite simple groups*, Number 3. Amer. Math. Soc. Surveys and Monographs **40**, 3 (1998).

[9] M. D. Hestenes, Singer groups, *Can. J. Math.* **XXII**, no 3 (1970), 492–513.

[10] D. Leemans, M. W. Liebeck, Chiral polyhedra and finite simple groups, *Bull. Lond. Math. Soc.* **49** (2017), no. 4, 581–592.

[11] A. M. Macbeath, On a theorem of Hurwitz, *Proc. Glasgow Math. Assoc.* **5** (1961), 90–96.