Almost simple groups of Lie type and symmetric designs with λ prime

Seyed Hassan Alavi* Mohsen Bayat Ashraf Daneshkhah

Department of Mathematics
Faculty of Science
Bu-Ali Sina Unoversity
Hamedan, Iran

alavi.s.hassan@basu.ac.ir
m.bayat@sci.basu.ac.ir
adanesh@basu.ac.ir

Submitted: Feb 13, 2020; Accepted: Mar 22, 2021; Published: Apr 23, 2021

Abstract

In this article, we investigate symmetric (v, k, λ) designs $\mathcal{D}$ with λ prime admitting flag-transitive and point-primitive automorphism groups G. We prove that if G is an almost simple group with socle a finite simple group of Lie type, then $\mathcal{D}$ is either the point-hyperplane design of a projective space $\mathrm{PG}_{n-1}(q)$, or it is of parameters $(7, 4, 2)$, $(11, 5, 2)$, $(11, 6, 3)$ or $(45, 12, 3)$.

Mathematics Subject Classifications: 05B05, 05B25, 20B25

1 Introduction

A *symmetric* (v, k, λ) *design* is an incidence structure $\mathcal{D} = (\mathcal{P}, \mathcal{B})$ consisting of a set $\mathcal{P}$ of v *points* and a set $\mathcal{B}$ of v *blocks* such that every point is incident with exactly k blocks, and every pair of blocks is incident with exactly λ points. If $2 < k < v - 1$, then $\mathcal{D}$ is called a *nontrivial* symmetric design. A *flag* of $\mathcal{D}$ is an incident pair (α, B), where α and B are a point and a block of $\mathcal{D}$, respectively. An *automorphism* of a symmetric design $\mathcal{D}$ is a permutation of the points permuting the blocks and preserving the incidence relation. An automorphism group G of $\mathcal{D}$ is called *flag-transitive* if it is transitive on the set of flags of $\mathcal{D}$. If G acts primitively on the point set $\mathcal{P}$, then G is said to be *point-primitive*. A group G is said to be *almost simple* with socle X if $X \trianglelefteq G \leqslant \mathrm{Aut}(X)$, where X is a nonabelian simple group. Further definitions and notation can be found in Section 1.2 below.

*Corresponding author, Alternative email address: alavi.s.hassan@gmail.com

 https://doi.org/10.37236/9366

The main aim of this paper is to study symmetric designs with λ prime admitting a flag-transitive and point-primitive almost simple automorphism group with socle being a finite simple groups of Lie type. Recently, Z. Zhang, Y. Zhang and S. Zhou in [37] proved that if $\mathcal{D}$ is a nontrivial symmetric (v, k, λ) designs with λ prime and G is a flag-transitive and point-primitive automorphism group of $\mathcal{D}$, then G must be of affine or almost simple type. We have studied nontrivial symmetric (v, k, λ) design with k prime admitting flag-transitive almost simple automorphism groups [2], and proved that such a design is either a projective space, or it has a parameters set $(11, 5, 2)$. We are now interested in possible classification of symmetric (v, k, λ) designs $\mathcal{D}$ with λ prime admitting a flag-transitive and point-primitive almost simple automorphism group G. We have already shown in [6] that almost simple exceptional groups of Lie type give rise to no possible symmetric designs with λ prime. In the present paper, we focus on the case where G is an almost simple group with socle X being a finite simple classical group of Lie type, and prove that $\mathcal{D}$ is either the point-hyperplane design of a projective space $\mathrm{PG}_{n-1}(q)$, or it is of parameters $(7, 4, 2)$, $(11, 5, 2)$, $(11, 6, 3)$ or $(45, 12, 3)$, and we give detailed information of these designs in Section 2.

Theorem 1. *Let $\mathcal{D}$ be a nontrivial symmetric (v, k, λ) design with λ prime, and let α be a point of $\mathcal{D}$. If G is a flag-transitive and point-primitive automorphism group of $\mathcal{D}$ of almost simple group of Lie type with socle X. Then $\mathcal{D}$ is the point-hyperplane design of $\mathrm{PG}_{n-1}(q)$ with $\lambda = (q^{n-2} - 1)/(q - 1)$ prime and $X = \mathrm{PSL}_n(q)$, or $\mathcal{D}$ and G are as in* Table 1.

Despite of the case where k is prime, even in symmetric designs with λ prime, flag-transitivity does not necessarily imply point-primitivity. One of these examples arose from studying flag-transitive biplanes (symmetric designs with $\lambda = 2$). It is known that there are only three non-isomorphic symmetric designs with parameters $(16, 6, 2)$, two of which admit flag-transitive and point-imprimitive design and one is not flag-transitive. The next interesting examples are the symmetric designs with parameters $(45, 12, 3)$. Indeed, Praeger [33] proves that there are only two examples of flag-transitive designs with parameters $(45, 12, 3)$. One is point-primitive and related to unitary geometry, while the other is point-imprimitive and constructed from a 1-dimensional affine space for which we also give an explicit base block in Section 2 below. In general, Praeger and Zhou [34] study symmetric (v, k, λ) designs admitting flag-transitive and point-imprimitive designs, and running through the potential parameters, we can only exclude one possibility, and so Corollary 2 below is an immediate consequence of their result [34, Theorem 1.1]. To our knowledge, at this stage, any possible classification of flag-transitive and point-imprimitive designs with λ prime seems to be out of reach.

Corollary 2. *Suppose that $\mathcal{D}$ is a symmetric (v, k, λ) design with λ prime admitting flag-transitive and point-imprimitive automorphism group G. If G leaves invariant a non-trivial partition $\mathcal{C}$ of $\mathcal{P}$ with d classes of size c, then there is a constant l such that, for each $B \in \mathcal{B}$ and $\Delta \in \mathcal{C}$, $|B \cap \Delta| \in \{0, l\}$, and one of the following holds:*

(a) $k \leqslant \lambda(\lambda - 3)/2$*;*

Table 1: Parameters in Theorem 1

Line	v	k	λ	X	G	G_α	Designs	References*
1	7	4	2	$\mathrm{PSL}_2(7)$	$\mathrm{PSL}_2(7)$	Sym_4	Complement of Fano plane	[3, 13]
2	11	5	2	$\mathrm{PSL}_2(11)$	$\mathrm{PSL}_2(11)$	Alt_5	Hadamard	[3, 13]
3	11	6	3	$\mathrm{PSL}_2(11)$	$\mathrm{PSL}_2(11)$	Alt_5	Complement of line 2	[3, 13]
4	45	12	3	$\mathrm{PSU}_4(2)$	$\mathrm{PSU}_4(2)$	$2{\cdot}(\mathrm{Alt}_4{\times}\mathrm{Alt}_4){\cdot}2$	-	[11, 16, 33]
5	45	12	3	$\mathrm{PSU}_4(2)$	$\mathrm{PSU}_4(2){:}2$	$2{\cdot}(\mathrm{Alt}_4{\times}\mathrm{Alt}_4).2{:}2$	-	[11, 16, 33]

Note: The last column addresses to references in which a design with the parameters in the line has been constructed.

(b) $(v,k,\lambda) = (\lambda^2(\lambda+2), \lambda(\lambda+1), \lambda)$ *with* $(c,d,l) = (\lambda^2, \lambda+2, \lambda)$ *or* $(\lambda+2, \lambda^2, 2)$*;*

(c) $(v,k,\lambda,c,d,l) = ((\lambda+6)(\lambda^2+4\lambda-1)/4, \lambda(\lambda+5)/2, \lambda, \lambda+6, (\lambda^2+4\lambda-1)/4, 3)$*, where* $\lambda \equiv 1$ *or* $3 \pmod 6$.

1.1 Outline of proofs

In order to prove Theorem 1 in Section 4, as noted above, by [6, Corollary 1.2], we only need to consider the case where the socle X of G is a finite simple classical group. In particular, by [1, 3, 5, 7, 15], in the case where X is a linear or unitary group, we can assume that the dimension of the underlying vector space is at least 5. Moreover, we include all possible symmetric (v,k,λ) designs for $\lambda = 2,3$ obtained in [18, 30, 32] and therein references, and so we can also assume that $\lambda \geqslant 5$. If λ is coprime to k, then the possible designs can be read off from [9, Corollary 1.2]. Since $\lambda(v-1) = k(k-1)$, we need to focus on the case where λ divides k. Since also G is point-primitive, a point-stabiliser $H = G_\alpha$ is maximal in G. Note that $v = |G : H|$ is odd as λ is odd prime and $\lambda(v-1) = k(k-1)$. Therefore, as a key tool, we use a classification of primitive permutation groups of odd degree [27, Theorem] which gives the possible candidates for H. Another important and useful fact is that k divides the order of H, and so λ is a prime divisor of $|H|$. At some stage, the knowledge of subdegrees (length of suborbits) of the G-action on the right cosets of H in G is essential. We now analyse each possibilities of H. Considering the fact that k divides $\lambda(v-1)$ and if applicable k also divides λd with d a subdegree, we find a polynomial $f(q)$ of smallest possible degree for which k divides $\lambda f(q)$. As λ is a odd prime divisor of $|H|$, we find possible upper bounds u_λ. In most cases, we observe that $v < u_\lambda f(q)^2$ does not hold and this violates the fact that $\lambda v < k^2$. In some cases, the inequality $v < u_\lambda f(q)^2$ has some solutions, and these solutions suggest some parameters set that are needed to be argued as well. In the remaining cases, however, we need to use some other arguments and new techniques to settle down our claims. In this manner, Theorem 1 follows from Propositions 18-21. The proof of Corollary 2 is also given in Section 4, and the proof follows immediately from [34, Theorem 1.1] by ruling out one possible case. In this paper, we use the software GAP [19] for computational arguments.

1.2 Definitions and notation

All groups and incidence structures in this paper are finite. Symmetric and alternating groups on n letters are denoted by Sym_n and Alt_n, respectively. We write "n" for a group of order n. Also for a given positive integer n and a prime divisor p of n, we denote the p-part of n by n_p, that is to say, $n_p = p^t$ with $p^t \mid n$ but $p^{t+1} \nmid n$. For finite simple groups of Lie type, we adopt the standard notation as in [14], and in particular, we use the standard notation to denote the finite simple classical groups, that is to say, $\mathrm{PSL}_n(q)$, for $n \geqslant 2$ and $(n, q) \neq (2, 2), (2, 3)$, $\mathrm{PSU}_n(q)$, for $n \geqslant 3$ and $(n, q) \neq (3, 2)$, $\mathrm{PSp}_{2m}(q)$, for $n = 2m \geqslant 4$ and $(m, q) \neq (2, 2)$, $\Omega_{2m+1}(q) = \mathrm{P}\Omega_{2m+1}(q)$, for $n = 2m + 1 \geqslant 7$ and q odd, $\mathrm{P}\Omega^{\pm}_{2m}(q)$, for $n = 2m \geqslant 8$. In this manner, the only repetitions are

$$\begin{array}{lll} \mathrm{PSL}_2(4) \cong \mathrm{PSL}_2(5) \cong \mathrm{Alt}_5, & \mathrm{PSL}_2(7) \cong \mathrm{PSL}_3(2), & \mathrm{PSL}_2(9) \cong \mathrm{Alt}_6, \\ \mathrm{PSL}_4(2) \cong \mathrm{Alt}_8, & \mathrm{PSp}_4(3) \cong \mathrm{PSU}_4(2). & \end{array}$$

Recall that a symmetric design $\mathcal{D}$ with parameters (v, k, λ) is a pair $(\mathcal{P}, \mathcal{B})$, where $\mathcal{P}$ is a set of v points and $\mathcal{B}$ is a set of v blocks such that each block is a k-subset of $\mathcal{P}$ and each two distinct points are contained in λ blocks. We say that $\mathcal{D}$ is nontrivial if $2 < k < v - 1$. Further notation and definitions in both design theory and group theory are standard and can be found, for example in [10, 14, 17, 24, 26].

2 Examples and Comments

In this section, we provide some examples of symmetric designs with λ prime admitting a flag-transitive automorphism almost simple group with socle X. We remark here that the designs in Table 1 can be found in [3, 7], but the construction given here is obtained by GAP [19].

Example 3. The point-hyperplane of a projective space $\mathrm{PG}_{n-1}(q)$ with parameters $((q^n - 1)/(q - 1), (q^{n-1} - 1)/(q - 1), (q^{n-2} - 1)/(q - 1))$ for $n \geqslant 3$ is a well-known example of flag-transitive symmetric designs. Any group G with $\mathrm{PSL}_n(q) \leqslant G \leqslant \mathrm{P\Gamma L}_n(q)$ acts flag-transitively on $\mathrm{PG}_{n-1}(q)$. If $n = 3$, then we have the *Desarguesian plane* with parameters $(q^2 + q + 1, q + 1, 1)$ which is a projective plane. The design $\mathcal{D}$ with parameters $(7, 4, 2)$ in line 1 of Table 1 is the complement of the unique well-known symmetric design, namely, *Fano Plane* admitting flag-transitive and point-primitive automorphism group $\mathrm{PSL}_2(7) \cong \mathrm{PSU}_2(7)$ with point-stabiliser Sym_4.

Example 4. The symmetric $(11, 5, 2)$ design is a *Paley difference set* which is also a Hadamard design with the base block $\{1, 2, 3, 5, 11\}$, and its full automorphism group is $\mathrm{PSU}_2(11)$ acting flag-transitively and point-primitively. In this case, the point-stabiliser is isomorphic to Alt_5. The complement of this design is the unique symmetric $(11, 6, 3)$ design whose full automorphism group $\mathrm{PSU}_2(11)$ is also flag-transitive and point-primitive with Alt_5 as point-stabiliser.

Example 5. There are exactly three non-isomorphic symmetric $(16, 6, 2)$ design, two of which are flag-transitive. The first symmetric design admitting a flag-transitive automorphism group is constructed from a difference set in 2^4 whose automorphism group is $2^4\ \mathrm{Sym}_6 < 2^4\ \mathrm{GL}_4(2)$ with point-stabiliser Sym_6. The second example of symmetric $(16, 6, 2)$ design admitting a flag-transitive automorphism group arose from a difference set in 2×8, and the point-stabiliser of order 48 acts as the full group of symmetries of the cube, hence is a central extension $\mathrm{Sym}_4 \circ 2$ of the symmetric group Sym_4 by a group of order 2. These two designs admit point-imprimitive automorphism group. The last symmetric $(16, 6, 2)$ design can be constructed as a difference set in $Q_8 \times 2$. The full automorphism group of order $16 \cdot 24$ of this design is not flag-transitive.

Example 6. Mathon and Spence [29] have constructed $3,752$ pairwise non-isomorphic symmetric $(45, 12, 3)$ designs, and they have shown that at least $1,136$ of these designs have a trivial automorphism group. Cheryl E. Praeger in [33] constructs two flag-transitive symmetric $(45, 12, 3)$ designs, and proves that these designs are the only two examples. One of these symmetric designs is related to unitary geometry and admits point-primitive automorphism group $\mathrm{PSU}_4(2) \cdot 2$, while the other has point-imprimitive automorphism group $G \leqslant \mathrm{A\Gamma L}_1(81)$. The base block of the former design is $\{1, 2, 4, 5, 12, 15, 17, 21, 28, 34, 35, 38\}$, and more detailed information about this design can be found in [11, 13] and therein references. We here give an explicit base block for the point-imprimitive example. Let G be a permutation group on the set $\mathcal{P} := \{1, \dots, 45\}$ generated by the permutations $\sigma_1, \dots, \sigma_5$ below

$$\begin{aligned}
\sigma_1 :=\ & (1, 2, 4, 5, 3)(6, 16, 43, 13, 14)(7, 39, 33, 45, 26)(8, 21, 37, 32, 28)(9, 11, 25, 35, 10)\\
& (12, 44, 24, 40, 17)(15, 30, 38, 23, 19)(18, 34, 20, 31, 41)(22, 36, 27, 42, 29),\\
\sigma_2 :=\ & (1, 5, 2, 3, 4)(6, 10, 16, 9, 43, 11, 13, 25, 14, 35)(7, 40, 39, 17, 33, 12, 45, 44, 26, 24)\\
& (8, 23, 21, 19, 37, 15, 32, 30, 28, 38)(18, 22, 34, 36, 20, 27, 31, 42, 41, 29),\\
\sigma_3 :=\ & (2, 5, 3, 4)(6, 17, 32, 20, 11, 26, 23, 29)(7, 30, 42, 43, 12, 21, 34, 35)\\
& (8, 31, 10, 45, 15, 22, 13, 40)(9, 39, 19, 27, 14, 44, 28, 18)(16, 24, 37, 41, 25, 33, 38, 36),\\
\sigma_4 :=\ & (2, 3)(4, 5)(6, 32, 11, 23)(7, 42, 12, 34)(8, 10, 15, 13)(9, 19, 14, 28)(16, 37, 25, 38)\\
& (17, 20, 26, 29)(18, 39, 27, 44)(21, 35, 30, 43)(22, 40, 31, 45)(24, 41, 33, 36),\\
\sigma_5 :=\ & (1, 6, 11)(3, 40, 45)(4, 41, 36)(5, 13, 10)(8, 35, 39)(9, 42, 38)(14, 37, 34)(15, 44, 43)\\
& (17, 32, 29)(18, 30, 33)(20, 23, 26)(21, 27, 24).
\end{aligned}$$

Then $G \cong 3^4 : (5 : 8)$ is isomorphic to a subgroup of $\mathrm{A\Gamma L}_1(81)$. The group G has a subgroup $K \cong 3^2 : 8$ with an orbit of size 12, namely,

$$B = \{1, 2, 3, 4, 6, 11, 19, 28, 36, 40, 41, 45\}.$$

Let now $\mathcal{B}$ be the set of G-orbits B^G. Then $\mathcal{D} = (\mathcal{P}, \mathcal{B})$ forms a symmetric $(45, 12, 3)$ design with flag-transitive automorphism group G. Moreover, $C = \{1, 6, 11, 17, 20, 23, 26, 29, 32\}$ is a G-invariant partition on $\mathcal{P}$, and so G is point-imprimitive. Note that the full automorphism group of $\mathcal{D}$ is isomorphic to $3^4 : (\mathrm{SL}_2(5) : 2)$ which is also point-imprimitive.

3 Preliminaries

In this section, we state some useful facts in both design theory and group theory. Recall that a group G is called almost simple if $X \trianglelefteq G \leqslant \mathrm{Aut}(X)$, where X is a (nonabelian) simple group.

Lemma 7. [1, Lemma 2.2] *Let G be an almost simple group with socle X, and let H be maximal in G not containing X. Then $G = HX$ and $|H|$ divides $|\mathrm{Out}(X)| \cdot |X \cap H|$.*

Lemma 8. [3, Lemma 2.1] *Let $\mathcal{D}$ be a symmetric (v, k, λ) design, and let G be a flag-transitive automorphism group of $\mathcal{D}$. If α is a point of $\mathcal{D}$ and $H = G_\alpha$, then*

(a) $k(k-1) = \lambda(v-1)$*;*

(b) $k \mid |H|$ *and* $\lambda v < k^2$*;*

(c) $k \mid \lambda d$*, for all nontrivial subdegrees d of G.*

Lemma 9 (Tits' Lemma)**.** [36, 1.6] *If X is a group of Lie type in characteristic p, then any proper subgroup of index prime to p is contained in a proper parabolic subgroup of X.*

Lemma 10. [36, 1.6] *Suppose that $\mathcal{D}$ is a symmetric (v, k, λ) design admitting a flag-transitive and point-primitive almost simple automorphism group G with socle X of Lie type in odd characteristic p. Suppose also that the point-stabiliser G_α, not containing X, is not a parabolic subgroup of G. Then* $\gcd(p, v-1) = 1$.

If a group G acts on a set $\mathcal{P}$ and $\alpha \in \mathcal{P}$, the *subdegrees* of G are the size of orbits of the action of the point-stabiliser G_α on $\mathcal{P}$.

Lemma 11. [28] *If X is a group of Lie type in characteristic p, acting on the set of cosets of a maximal parabolic subgroup, and X is not $\mathrm{PSL}_n(q)$, $\mathrm{P}\Omega_n^+(q)$ (with $n/2$ odd) and $E_6(q)$, then there is a unique subdegree which is a power of p.*

For a point-stabiliser H of an automorphisms group G of a flag-transitive design $\mathcal{D}$, by Lemma 8(b), we conclude that $\lambda|G| \leqslant |H|^3$, and so we have that

Corollary 12. *Let $\mathcal{D}$ be a flag-transitive (v, k, λ) symmetric design with automorphism group G. Then $|G| \leqslant |H|^3$, where α is a point in $\mathcal{D}$, and so $|X| < |\mathrm{Out}(X)|^2 \cdot |H \cap X|^3$.*

Lemma 13. [2, Lemma 2.5] *Suppose that $\mathcal{D}$ is a (v, k, λ) symmetric design. Let G be a flag-transitive automorphism group of $\mathcal{D}$ with simple socle X of Lie type in characteristic p. If the point-stabiliser $H = G_\alpha$ contains a normal quasi-simple subgroup N of Lie type in characteristic p and p does not divide $|Z(N)|$, then either p divides k, or N_B is contained in a parabolic subgroup P of N and k is divisible by $|N{:}P|$.*

The following result gives a classification of primitive groups of odd degree of almost simple type with socle finite simple classical groups. This result is proved independently in [21] and [27]. Here we follow the description of this groups as in [27].

Lemma 14. [27, Theorem] *Let G be a primitive permutation group of odd degree v on the set Γ. Assume that the socle $X = X(q)$ of G is a simple classical group with a natural projective module $V = V_n(q)$, where $q = p^a$ and p prime, and let $H = G_\alpha$ be the stabilizer of a point $\alpha \in \Gamma$, then one of the following holds:*

(a) *if q is odd then one of $(i), (ii)$ below holds:*

  (i) *X is a classical group with natural projective module $V = V_n(q)$ and one of (1)-(7) below holds:*

   (1) *H is the stabilizer of a nonsingular subspace (any subspace for $X = \mathrm{PSL}_n(q)$);*

   (2) *$H \cap X$ is the stabilizer of an orthogonal decomposition $V = \oplus V_j$ with all V_j's isometric (any decomposition $V = \oplus V_j$ with $\dim(V_j)$ constant for $X = \mathrm{PSL}_n(q)$);*

   (3) *$X = \mathrm{PSL}_n(q)$, H is the stabilizer of a pair $\{U, W\}$ of subspaces of complementary dimensions with $U \leqslant W$ or $U \oplus W = V$, and G contains a graph automorphism;*

   (4) *$H \cap X$ is $\mathrm{SO}_7(2)$ or $\Omega_8^+(2)$ and X is $\Omega_7(q)$ or $\mathrm{P}\Omega_8^+(q)$, respectively, q is prime and $q \equiv \pm 3 \pmod 8$;*

   (5) *$X = \mathrm{P}\Omega_8^+(q)$, q is prime and $q \equiv \pm 3 \pmod 8$, G contains a triality automorphism of X and $H \cap X$ is $2^3 \cdot 2^6 \cdot \mathrm{PSL}_3(2)$;*

   (6) *$X = \mathrm{PSL}_2(q)$ and $H \cap X$ is dihedral, Alt_4, Sym_4, Alt_5 or $\mathrm{PGL}_2(q_0)$, where $q = q_0^2$;*

   (7) *$X = \mathrm{PSU}_3(5)$ and $H \cap X = M_{10}$.*

  (ii) *$H = N_G(X(q_0))$, where $q = q_0^t$ and t is an odd prime;*

(b) *if q is even then $H \cap X$ is a parabolic subgroup of X.*

We will use the following results in order to obtain suitable lower or upper bounds for parameters of possible designs. The proof of these results can be found in [4, 8]

Lemma 15. [8, Lemma 4.2 and Corollary 4.3]

(a) *If $n \geqslant 2$, then*

$$\begin{aligned} q^{n^2-2} &< |\mathrm{PSL}_n(q)| \leqslant |\mathrm{SL}_n(q)| < (1-q^{-2})q^{n^2-1}, \\ (1-q^{-1})q^{n^2-2} &< |\mathrm{PSU}_n(q)| \leqslant |\mathrm{SU}_n(q)| < (1-q^{-2})(1+q^{-3})q^{n^2-1}. \end{aligned}$$

(b) *If $n \geqslant 4$, then*

$$\begin{aligned} \frac{1}{4}q^{n(n-1)/2} &< |\Omega_n(q)| < |\mathrm{SO}_n(q)| \leqslant (1-q^{-2})(1-q^{-4})q^{n(n-1)/2}, \\ \frac{1}{2\beta}q^{n(n+1)/2} &< |\mathrm{PSp}_n(q)| \leqslant |\mathrm{Sp}_n(q)| \leqslant (1-q^{-2})(1-q^{-4})q^{n(n+1)/2} \end{aligned}$$

with $\beta = \gcd(2, q-1)$.

(c) *If $n \geqslant 6$, then*

$$\frac{1}{8}q^{n(n-1)/2} < |\mathrm{P\Omega}_n^{\pm}(q)| < |\mathrm{SO}_n^{\pm}(q)| \leqslant \delta(1-q^{-2})(1-q^{-4})(1+q^{-n/2})q^{n(n-1)/2}$$

with $\delta = \gcd(2, q)$.

Lemma 16. [8, Lemma 4.4] *Suppose that t is a positive integer. Then*

(a) *if $t \geqslant 5$, then $t! < 5^{(t^2-3t+1)/3}$;*

(b) *if $t \geqslant 4$, then $t! < 2^{4t(t-3)/3}$.*

Lemma 17. [4, Lemma 3.12] *Let q be a prime power and $n \geqslant 3$ be a positive integer number, then*

$$q^{\frac{n(n-1)}{2}} < \prod_{j=2}^{n}(q^j - 1) < \prod_{j=2}^{n}(q^j - (-1)^j) < q^{\frac{n^2+n-2}{2}}.$$

4 Proof of the main results

In this section, we prove Theorem 1 and Corollary 2. Suppose that $\mathcal{D}$ is a nontrivial symmetric design with λ prime, and that G is an automorphism group of $\mathcal{D}$ which is an almost simple group whose socle X is a finite nonabelian simple group of Lie type. Suppose now that G is flag-transitive and point-primitive. Let $H = G_\alpha$, where α is a point of $\mathcal{D}$. Then H is maximal in G (see [17, 7, Corollary 1.5A]), and so Lemma 7 implies that

$$v = \frac{|X|}{|H \cap X|}. \tag{1}$$

As mentioned in Section 1.1, we only need to focus on the case where X is a finite simple classical group. Moreover, the parameter v is odd and the possibilities for H can be read off from [27] which are also recorded in Lemma 14. Further, we can assume that $\lambda \geqslant 5$ is an odd prime and in the case where X is $\mathrm{PSL}_n(q)$ or $\mathrm{PSU}_n(q)$, we can also assume that $n \geqslant 5$. In Propositions 18-21 below, we discuss possible cases for the pairs (X, H), and finally prove Theorem 1. In what follows, we denote by $\hat{}H$ the preimage of the group H in the corresponding group.

Proposition 18. *Let $\mathcal{D}$ be a nontrivial symmetric (v, k, λ) design with $\lambda \geqslant 5$ prime. Suppose that G is an automorphism group of $\mathcal{D}$ of almost simple type with socle $X = \mathrm{PSL}_n(q)$ for $n \geqslant 5$. If G is flag-transitive, point-primitive and $H = G_\alpha$ with α a point of $\mathcal{D}$, then $\mathcal{D}$ is the point-hyperplane design of $\mathrm{PG}_{n-1}(q)$ with $\lambda = (q^{n-2}-1)/(q-1)$ prime and $H \cap X \cong \hat{}[q^{n-1}]{:}\mathrm{SL}_{n-1}(q){\cdot}(q-1)$.*

Proof. Let $H_0 = H \cap X$, where $H = G_\alpha$ with α a point of $\mathcal{D}$. It follows from Lemma 8(a) that v is odd. Then by Lemma 14, we have one of the following possibilities:

(1) H_0 is a parabolic subgroup of X;

(2) H is the stabilizer of a pair $\{U, W\}$ of subspaces of complementary dimensions with $U \leqslant W$ and G contains a graph automorphism.

(3) q is odd, and H is the stabilizer of a pair $\{U, W\}$ of subspaces of complementary dimensions with $U \oplus W = V$, and G contains a graph automorphism.

(4) q is odd, and H_0 is the stabilizer of a partition $V = V_1 \oplus \cdots \oplus V_t$ with $\dim(V_j) = i$;

(5) $q = q_0^t$ is odd with t odd prime, and $H = N_G(X(q_0))$;

In what follows, we analyse each of these possible cases separately.

(1) Let H_0 be a parabolic subgroup of X. In this case, $H = P_i$, where $i \leqslant \lfloor n/2 \rfloor$, and by [23, Proposition 4.1.17], the subgroup H_0 is isomorphic to

$$\hat{}q^{i(n-i)} : \mathrm{SL}_i(q) \times \mathrm{SL}_{n-i}(q) \cdot (q-1).$$

Suppose first that $H = P_1$. Then G is 2-transitive, and this case has already been studied by Kantor [20]. Therefore, $\mathcal{D}$ is the point-hyperplane design of $\mathrm{PG}_{n-1}(q)$ with parameters set $((q^n-1)/(q-1), (q^{n-1}-1)/(q-1), (q^{n-2}-1)/(q-1))$ and $\lambda = (q^{n-2}-1)/(q-1)$ prime, as desired.

Suppose now that $H = P_i$ with $i \geqslant 2$. It follows from (1) and [31, p. 534] that

$$v = \frac{(q^n-1)(q^{n-1}-1)\cdots(q^{n-i+1}-1)}{(q^i-1)\cdots(q^2-1)(q-1)} > q^{i(n-i)}. \tag{2}$$

Then by Lemmas 7 and 8(b), the parameter k divides $|\mathrm{Out}(X)| \cdot |H_0|$, where $|H_0| = q^{n(n-1)/2}\gcd(n, q-1)^{-1} \cdot \prod_{j=2}^{n-i}(q^j-1) \cdot \prod_{j=1}^{i}(q^j-1)$ and $|\mathrm{Out}(X)| = 2a \cdot \gcd(n, q-1)$. Note that λ is an odd prime divisor of k. Then λ must divide a, p, $q-1$ or $(q^j-1)/(q-1)$, for some $j \in \{2, \ldots, n-i\}$, and so

$$\lambda \leqslant (q^{n-i}-1)/(q-1). \tag{3}$$

Here by Lemma 8(c) and [25, Corollary 2], the parameter k divides $\lambda d_{i,j}(q)$, where

$$d_{i,j}(q) = q^{j^2} \cdot \prod_{l=i-j+1}^{i}(q^l-1) \cdot \prod_{l=n-j-i+1}^{n-i}(q^l-1) \cdot \prod_{l=1}^{j}(q^l-1)^{-2}, \tag{4}$$

for $l = 1, 2, \ldots, i$. Therefore, k divides $\lambda d_{i,1}(q)$, where $d_{i,1}(q) = q(q^i-1)(q^{n-i}-1)(q-1)^{-2}$. Then by (2) and Lemma 8(b), we have that

$$\lambda q^{i(n-i)} < \lambda v < k^2 \leqslant \lambda^2 q^2 (q^i-1)^2 (q^{n-i}-1)^2 (q-1)^{-4}.$$

Thus $q^{i(n-i)} \cdot (q-1)^4 < \lambda q^2 (q^i-1)^2 (q^{n-i}-1)^2$, and so (3) implies that $q^{i(n-i)}(q-1)^5 < q^2(q^i-1)^2(q^{n-i}-1)^3 < q^{3n-i+2}$. Thus

$$q^{i(n-i)}(q-1)^5 < q^{3n-i+2}, \tag{5}$$

and hence $n(i-3) < i^2 - i + 2$. Note that $2i \leqslant n$. Thus $2i(i-3) \leqslant n(i-3) < i^2 - i - 1$, and so $i^2 < 5i + 2$. Hence $i = 2, 3, 4, 5$.

If $i = 5$, then by (5), we have that $q^{2n-22}(q-1)^5 < 1$. Since $n \geqslant 2i = 10$, the last inequality holds only for $(n, q) = (10, 2)$, in which case by (2), $v = 109221651$. Moreover, by Lemmas 7 and 8(b), k divides $|\mathrm{Out}(X)| \cdot |H_0|$. Thus k is a divisor of 6710027434028590694400. It is easy to check that for possible k, the fraction $k(k-1)/(v-1)$ is not a prime number.

If $i = 4$, then (5) implies that $q^{n-14}(q-1)^5 < 1$, and so $n \in \{8, 9, 10, 11, 12, 13, 14\}$ as $n \geqslant 2i = 8$. Note by (2) that q is even as v is odd. Then $\gcd(v-1, q^2+1) = 1$. Recall by Lemma 8 that k divides $\lambda \gcd(v-1, d_{4,1})$. Then $v < \lambda \cdot [d_{4,1}/(q^2+1)]^2$, where $\lambda \leqslant (q^{n-4}-1)/(q-1)$, and hence

$$v < (q-1)^{-1}(q^{n-4}-1) \cdot [d_{4,1}/(q^2+1)]^2. \tag{6}$$

For each possible n, by straightforward calculation, we observe that (6) does not hold.

If $i = 2$, then G is a rank 3 primitive group, see [22]. The symmetric designs admitting primitive rank 3 automorphism groups have been classified by Dempwolff [16]. Running through all these possible cases, we can not find any such symmetric design with $\lambda \geqslant 5$ prime.

If $i = 3$, then (2) implies that

$$v = \frac{(q^n-1)(q^{n-1}-1)(q^{n-2}-1)}{(q^3-1)(q^2-1)(q-1)} > q^{3n-9}.$$

We now consider the following cases:

(1.1) Let q be odd. If n is even, then v is also even, which is impossible. Therefore, n is odd. Note by (4), [35, p. 338] and Lemma 8(c) that k divides $\lambda \gcd(d_{3,1}(q), d_{3,2}(q))$, where $d_{3,1}(q) = q(q^2+q+1)(q^{n-3}-1)(q-1)^{-1}$ and $d_{3,2}(q) = q^4(q^2+q+1)(q^{n-4}-1)(q^{n-3}-1)(q-1)^{-1}(q^2-1)^{-1}$. Therefore,

$$k \text{ divides } \lambda f(q), \tag{7}$$

where $f(q) = q(q^2+q+1)(q^{n-3}-1)(q^2-1)^{-1}$. Then by Lemma 8(b), we have that $\lambda q^{3n-9} < \lambda v < k^2 \leqslant \lambda^2 q^2 (q^2+q+1)^2 (q^{n-3}-1)^2 (q^2-1)^{-2}$. Thus

$$q^{3n-9}(q^2-1)^2 < \lambda q^2 (q^2+q+1)^2 (q^{n-3}-1)^2. \tag{8}$$

Since λ is an odd prime divisor of k, Lemmas 7 and 8(b) imply that λ divides a, p, $q-1$ or $(q^j-1)(q-1)^{-1}$, for some $j \in \{2, 3, \ldots, n-3\}$.

Suppose first that λ divides a, p or $q-1$. Then by (8), we have that $q^{3n-9}(q^2-1)^2 < q^3(q^2+q+1)^2(q^{n-3}-1)^2$, and so $q^{3n-9}(q^2-1)^2 < q^{2n-3}(q^2+q+1)^2$. Hence $q^{n-6}(q^2-1)^2 < (q^2+q+1)^2$. Since $(q^2+q+1)^2 < q(q^2-1)^2$, we conclude that $q^{n-6} < q$, which is impossible as $n \geqslant 2i = 6$ is odd.

Suppose now that

$$\lambda \quad \text{divides} \quad (q^j-1)(q-1)^{-1}, \tag{9}$$

for some $j \in \{2, 3, \dots, n-3\}$. Since $q^{n-3}-1 < q^{n-3}$ and $q^j-1 < q^j$, it follows from (8) that $q^{3n-9}(q-1)(q^2-1)^2 < q^{2n+j-4}(q^2+q+1)^2$, and so $q^{n-j-5} < (q^2+q+1)^2/[(q-1)(q^2-1)^2]$. As $(q^2+q+1)^2 < q(q-1)(q^2-1)^2$, we conclude that $q^{n-j-6} < 1$, and so $j > n-6$. Since $j \leqslant n-3$, we have that $j \in \{n-5, n-4, n-3\}$, where n is odd. We now consider the following two subcases.

(1.1.1) Let $j = n-3$ or $n-5$. Note that j is even and λ divides q^j-1 by (9). Since λ is prime, it follows that $\lambda \leqslant q^{(n-3)/2}+1$, and so (8) yields $q^{n-9} < (q^2+q+1)^4(q^2-1)^{-4}$. Since $(q^2+q+1)^4 < q^2(q^2-1)^4$, we have that $q^{n-9} < q^2$, or equivalently, $q^{n-11} < 1$. Since also $n > 6$ is odd, we conclude that $n = 7, 9, 11$. Then by (2), we can obtain v. Note for these parameters v that $\gcd(v-1, q^2+q+1) = 1$. Since by Lemma 8, the parameter k divides $\lambda \gcd(v-1, d_{3,1})$, we conclude by (9) that $v < (q-1)^{-1}(q^{n-3}-1) \cdot [d_{3,1}/(q^2+q+1)]^2$, but for each possible n, this inequality does not hold for $q \geqslant 3$.

(1.1.2) Let $j = n-4$. Then by (9), the parameter λ divides $(q^{n-4}-1)(q-1)^{-1}$. Let u be a positive integer such that $\lambda u = (q^{n-4}-1)(q-1)^{-1}$. Note that $(q^{n-4}-1)(q-1)^{-1}$ is odd, and so u is an odd number. Here by (8) and (9), $uq^{3n-9}(q-1)(q^2-1) < q^2(q^2+q+1)^2(q^{n-3}-1)^2(q^{n-4}-1) < (q^2+q+1)^2 q^{3n-8}$, and so $u\cdot(q-1)(q^2-1)^2 < q(q^2+q+1)^2$. This inequality holds only for $u = 1$ or $(u, q) = (3, 3)$. In the latter case, since $\lambda u = (q^{n-4}-1)(q-1)^{-1}$, it follows that $u = 3$ divides $q^{n-5} + q^{n-6} + \ldots + q + 1$, where $q = 3$, which is impossible. Therefore, $u = 1$, and hence $\lambda = q^{n-5} + q^{n-6} + \ldots + q + 1$. Thus by (7), the parameter k divides $\lambda f(q)$, where $f(q) = q(q^2+q+1)(q^{n-3}-1)(q^2-1)^{-1}$. Let now m be a positive integer such that $mk = \lambda f(q)$. Then by Lemma 8(a), we have that $k = 1+m\cdot(v-1)/f(q)$. Note by (2) that $v-1 = g(q)\cdot q(q^{n-3}-1)(q^3-1)^{-1}(q^2-1)^{-1}(q-1)^{-1}$, where $g(q) = q^{2n-1} + q^{n+2} - q^{n+1} - q^n - q^{n-1} + q^5 - q^4 - q^3 + q + 1$. Therefore, $k = 1 + [m\cdot g(q)/(q^3-1)^2] > mq^{2n-7}$. Since k divides $q(q^2+q+1)(q^{n-4}-1)(q^{n-3}-1)(q^2-1)^{-1}(q-1)^{-1}$, we conclude that

$$m \cdot q^{2n-7} < q(q^2+q+1)(q^{n-4}-1)(q^{n-3}-1)(q^2-1)^{-1}(q-1)^{-1},$$

and so $m \cdot (q-1)(q^2-1) < q(q^2+q+1)$. This inequality holds only for $m = 1, 2$. Let now $r(q) = (q+1)(q^3-1)^2$ and $h(q) = q^{n+3} + q^7 + q^6 - q^5 - q^4 - q^3$. Then

$$(q^3-1)^2 \cdot k = m \cdot g(q) + (q^3-1)^2 = m \cdot h(q)(q^{n-4}-1) + m \cdot r(q) + (q^3-1)^2. \quad (10)$$

Since $\lambda = (q^{n-4}-1)/(q-1)$ is an odd prime divisor of $k = [m \cdot g(q) + (q^3-1)^2]/(q^3-1)^2$, it follows from (10) that $q^{n-4}-1$ divides $m \cdot r(q) + (q^3-1)^2 = [m \cdot (q+1) + 1](q^3-1)^2$. Recall that $m \leqslant 2$. Therefore, $q^{n-4}-1 \leqslant [m \cdot (q+1)+1](q^3-1)^2 \leqslant (2q+3)(q^3-1)^2$. Since q is odd, we conclude that $2q+3 \leqslant q^2$, and so $q^{n-4}-1 \leqslant q^8$. This inequality holds only for $n = 7, 9, 11$. By the same manner as in the previous cases, we observe that $v-1$ is coprime to q^2+q+1, and since $\lambda \leqslant (q-1)^{-1}(q^{n-4}-1)$, it follows that $v < (q-1)^{-1}(q^{n-4}-1) \cdot [d_{3,1}/(q^2+q+1)]^2$ for $n \in \{7, 9, 11\}$. But for each possible n, this inequality does not hold for any $q \geqslant 3$.

(1.2) Let q be even. Then (4) and Lemma 8(c) imply that

$$k \text{ divides } \lambda f(q), \quad (11)$$

where $f(q) := d_{3,1} = q(q^2+q+1)(q^{n-3}-1)/(q-1)$. Note that λ is an odd prime divisor of a or q^j-1 with $j \in \{1,\ldots,n-3\}$.

Suppose first that λ divides a or $q-1$. Then by Lemma 8(b), we have that $\lambda v < k^2 \leqslant \lambda^2 q^2(q^2+q+1)^2(q^{n-3}-1)^2/(q-1)^2$. Thus $q^{3n-9}(q-1)^2 < \lambda q^2(q^2+q+1)^2(q^{n-3}-1)^2 < q^3(q^2+q+1)^2(q^{n-3}-1)^2$, and so $q^{3n-9}(q-1)^2 < q^{2n-3}(q^2+q+1)^2$. Hence $q^{n-6}(q-1)^2 < (q^2+q+1)^2$. Since $(q^2+q+1)^2 < q^6(q-1)^2$, we conclude that $q^{n-6} < q^6$, and so $n = 6, 7, 8, 9, 10$. Define

$$d_n(q) = \begin{cases} f(q)/(q^2+q+1)^2, & \text{if } n = 6, 9; \\ f(q)/(q^2+q+1), & \text{if } n = 7, 8, 10. \end{cases}$$

Note that $\lambda \leqslant q-1$. Then by the same manner as before, we must have $v < (q-1)\cdot d_n(q)^2$. By solving this inequality for $n \in \{6,\ldots,10\}$, we conclude that $q = 2$ when $n \in \{7,8,10\}$. In these cases, however, $\lambda \leqslant \max\{a, q-1\} = 1$, which is a contradiction.

Suppose now that λ divides q^j-1, for some $j \in \{2,\ldots,n-3\}$. Therefore, $\lambda \leqslant q^j-1$. By (11) and Lemma 8(b), we have that $\lambda v < k^2 \leqslant \lambda^2 q^2(q^2+q+1)^2(q^{n-3}-1)^2/(q-1)^2$. Thus

$$q^{3n-9}(q-1)^2 < \lambda q^2(q^2+q+1)^2(q^{n-3}-1)^2. \tag{12}$$

Recall that $\lambda \leqslant q^j-1$. Hence $q^{3n-9}(q-1)^2 < (q^2+q+1)^2 q^{2n+j-4}$. Since $(q^2+q+1)^2 < q^6(q-1)^2$, we conclude that $q^{3n-9} < q^{2n+j+2}$, and so $j > n-11$. Since $j \leqslant n-3$, we have that $j \in \{n-10, n-9, \ldots, n-3\}$. Recall that λ divides q^j-1. Let u be a positive integer such that

$$\lambda = \frac{q^j-1}{u}. \tag{13}$$

Let now m be a positive integer such that $mk = \lambda f_n(q)$, where

$$f_n(q) = q(q^2+q+1)(q^{n-3}-1)/(q-1).$$

Then by Lemma 8(a), we have that $k = 1 + m(v-1)/f_n(q)$. Note that $v-1 = q(q^{n-3}-1)g_n(q)(q^3-1)^{-1}(q^2-1)^{-1}(q-1)^{-1}$, where $g_n(q) = q^{2n-1}+q^{n+2}-q^{n+1}-q^n-q^{n-1}+q^5-q^4-q^3+q+1$. Therefore,

$$k = 1 + \frac{m\cdot g_n(q)}{(q+1)(q^3-1)^2} > m\cdot q^{2n-9}. \tag{14}$$

Since $k \leqslant \lambda f_n(q)$ and $\lambda = (q^j-1)/u$, we conclude that $mq^{2n-9} < k \leqslant q(q^2+q+1)(q^j-1)(q^{n-3}-1)/[u\cdot(q-1)]$, and so $mu\cdot q^{n-j-7}(q-1) < (q^2+q+1)$. Hence,

$$mu < q^{j-n+7}. \tag{15}$$

Since $mu \geqslant 1$, it follows that $q^{j-n+7} > 1$, and so $j-n+7 > 0$. Therefore,

$$j = n-t \text{ with } t \in \{3,\ldots,6\}. \tag{16}$$

Table 2: The polynomials $h(q)$ and $r(q)$ as in Case 1.2 of Proposition 18.

j	$h_j(q)$	$r_j(q)$
$n-3$	$q^{n+2}+2q^5-q^4-q^3-q^2$	$3q^5-2q^4-2q^3-q^2+q+1$
$n-4$	$q^{n+3}+q^7+q^6-q^5-q^4-q^3$	$q^7+q^6-2q^4-2q^3+q+1$
$n-5$	$q^{n+4}+q^9+q^7-q^6-q^5-q^4$	$q^9+q^7-q^6-2q^4-q^3+q+1$
$n-6$	$q^{n+5}+q^{11}+q^8-q^7-q^6-q^5+q^2$	$q^8-q^7-q^6-q^4-q^3+q^2+q+1$

Let $h_j(q)$ and $r_j(q)$ be as in the second and third columns of Table 2. Then $g_n(q) = h_j(q) \cdot (q^j - 1) + r_j(q)$, and so

$$\begin{aligned}(q+1)(q^3-1)^2 \cdot k &= m \cdot g_n(q) + (q+1)(q^3-1)^2 \\ &= m \cdot h(q)(q^j-1) + m \cdot r(q) + (q+1)(q^3-1)^2. \end{aligned} \tag{17}$$

For j as in (16), we observe that $|m \cdot r_j(q) + (q^3-1)^2(q+1)| > 0$. Since $\lambda = (q^j-1)/u$ is a divisor of k, it follows from (17) that $(q^j-1)/u$ divides $|m \cdot r_j(q) + (q+1)(q^3-1)^2|$, where $mu < q^{j-n+7}$ and $r_j(q)$ is as in Table 2. Since $|r_j(q) + (q+1)(q^3-1)^2| < q^{10}$, we have that $q^j - 1 < muq^{10}$, and so by (15), we have that $q^{n-17} < 1$. This inequality holds only for $n = 6, \ldots, 16$. Define

$$d_n(q) = \begin{cases} 9 \cdot f_n(q)/(q^2+q+1)^2, & \text{if } n = 6, 9, 12, 15; \\ 3 \cdot f_n(q)/(q^2+q+1), & \text{if } n = 7, 8, 10, 11, 13, 14, 16. \end{cases}$$

Note that $\lambda \leqslant q^{n-3} - 1$. Since k divides $\lambda \cdot \gcd(v-1, f_n(q))$ which is a divisor of $\lambda d_n(q)$, the inequality $\lambda v < k^2$ implies that $v < (q^{n-3}-1) \cdot d_n(q)^2$, and considering each possible n, we conclude that $q \in \{2, 4, 8\}$. For each q, we obtain the parameter v by (2), and considering all divisors k of $|\mathrm{Out}(X)| \cdot |H_0|$, we observe that $k(k-1)/(v-1)$ is not prime, which is a contradiction.

(2) Let H be the stabilizer of a pair $\{U, W\}$ of subspaces of dimension i and $n-i$ with $2i < n$ and $U \leqslant W$. Then by [23, Proposition 4.1.22], the subgroup H_0 is isomorphic to $\hat{}[q^{2in-3i^2}] \cdot \mathrm{SL}_i(q)^2 \times \mathrm{SL}_{n-2i}(q) \cdot (q-1)^2$. It follows from (1) and Lemma 15 that $v > q^{i(2n-3i)}$. We note here that Lemma 11 is still true in this case. Then there is a subdegree which is a power of p. On the other hand, if p is odd, then the p-part $(v-1)_p$ of $v-1$ is q. Then by Lemma 8(c), k divides λq. Hence Lemma 8(b) implies that $\lambda q^{i(2n-3i)} < \lambda v < k^2 \leqslant \lambda^2 q^2$, and so

$$q^{i(2n-3i)} < \lambda q^2. \tag{18}$$

Note that λ is an odd prime divisor of $2a \cdot \gcd(n, q-1) \cdot |H_0|$. It follows from Lemmas 7 and 8(b) that λ divides a, p or $q^j - 1$, where $j \leqslant n-2$. Then $\lambda \leqslant q^{n-2} - 1$, and so (18) implies that $q^{i(2n-3i)} < q^2(q^{n-2}-1)$. Thus $n(2i-1) < 3i^2$. Since $n > 2i$, we have that $i^2 < 2i$. This inequality holds only for $i = 1$, in which case by (18), we conclude that $q^{2n-3i} < \lambda q^2$, where $\lambda \leqslant q^{n-2} - 1$. Then $q^{2n-3} < q^n$, and so $n < 3$, which is a contradiction.

(3) Let H be the stabilizer of a pair $\{U, W\}$ of subspaces of dimension i and $n-i$ with $2i < n$ and $V = U \oplus W$. Then by [23, Proposition 4.1.4], the subgroup H_0 is isomorphic to $\hat{}\mathrm{SL}_i(q) \times \mathrm{SL}_{n-i}(q) \cdot (q-1)$. We first show that $i \neq 1$. If $i = 1$, then by (1), we have that $v = q^{n-1}(q^n-1)/(q-1)$. Note by [35, p. 339] that k divides $\lambda q^{n-2}(q^{n-1}-1)/(q-1)$. On the other hand, by Lemmas 8(a) and 10, the parameter k divides $\lambda(v-1)$ and $v-1$ is coprime to q. Thus

$$k \text{ divides } \lambda(q^{n-1}-1)/(q-1). \tag{19}$$

We now apply Lemma 8(b) and conclude that $q^{n-1}(q^n-1) < \lambda(q^{n-1}-1)^2/(q-1)$. Note that λ is an odd prime divisor of $2a \cdot \gcd(n, q-1) \cdot |H_0|$. Then Lemmas 7 and 8(b) imply that λ divides a, p or $q^j - 1$, with $j \leqslant n-1$. If λ divides a, p or $q-1$, then the inequality $q^{n-1}(q^n-1) < \lambda(q^{n-1}-1)^2/(q-1)$ yields $q^{n-1}(q^n-1)(q-1) < q(q^{n-1}-1)^2$, which is impossible. Therefore,

$$\lambda \text{ divides } (q^j-1)/(q-1), \tag{20}$$

for some $j \in \{2, \ldots, n-1\}$. By (19), k divides $\lambda(q^{n-1}-1)/(q-1)$. Let u be a positive integer such that $uk = \lambda f_n(q)$, where $f_n(q) = (q^{n-1}-1)/(q-1)$. Since $v - 1 = (q^{n-1}-1)(q^n+q-1)/(q-1)$, by Lemma 8(a), we have that

$$k = u \cdot (q^n+q-1) + 1 \text{ and } \lambda = u^2 q(q-1) + \frac{u^2(2q-1)+u}{f_n(q)}. \tag{21}$$

Recall that k divides $\lambda f_n(q)$. So (21) implies that $u \cdot (q^n+q-1)+1$ divides $(q^j-1)(q^{n-1}-1)/(q-1)^2$. By Euclid's algorithm, we have that $u \cdot (q^n+q-1)+1$ divides $u \cdot (q^{n-1}+2q^j-q^{j-1}-1)+q^{j-1}$. Thus $u \cdot (q^n+q-1)+1 \leqslant u \cdot (q^{n-1}+2q^j-q^{j-1}-1)+q^{j-1}$, and so $q^n+q \leqslant q^{n-1}+2q^j$. Note that $j \leqslant n-1$. Then $q^n+q \leqslant 3q^{n-1}$, which is impossible. Therefore, $i \geqslant 2$. In this case, by [35, p. 340], we have that $v > q^{2i(n-i)}$. It follows from [35, p. 339-340] that k divides $\lambda(q^i-1)(q^{n-i}-1)$. Hence by Lemma 8(b), we have that $\lambda q^{2i(n-i)} < \lambda v < k^2 \leqslant \lambda^2(q^i-1)^2(q^{n-i}-1)^2$, and so

$$q^{2i(n-i)} < \lambda q^{2n}. \tag{22}$$

Note that λ is an odd prime divisor of k dividing $2a \cdot \gcd(n, q-1) \cdot |H_0|$. Then Lemmas 7 and 8(b) imply that λ is a divisor of a, p or $q^j - 1$, for some $j \leqslant n-i$. Thus

$$\lambda \leqslant (q^{n-i}-1)/(q-1), \tag{23}$$

and by (22), we have that $q^{2i(n-i)}(q-1) < q^{2n}(q^{n-i}-1)$. Therefore, $2i(n-i) < 3n-i$, and hence $n(2i-3) < 2i^2 - i$. This implies that $(n, i) = (5, 2)$, in which case $v = q^6(q^5-1)(q^2+1)/(q-1)$ and k divides $\lambda(q^2-1)(q^3-1)$. Then by Lemma 8(a), the parameter k divides $\lambda \gcd(v-1, (q^2-1)(q^3-1))$. Since $\gcd(v-1, q+1) = 1$, we conclude that k divides $\lambda(q-1)^2(q^2+q+1)$. Then the inequality $\lambda v < k^2$ and (23) yields $q^6(q^5-1)(q^2+1) < (q-1)^2(q^3-1)^3$, which is impossible.

(4) Here $V = V_1 \oplus \cdots \oplus V_t$ with $\dim(V_j) = i$ and $n = it$. By [23, Proposition 4.2.9], the subgroup H_0 is isomorphic to $\hat{\ }\mathrm{SL}_i(q)^t \cdot (q-1)^{t-1} \cdot \mathrm{Sym}_t$. It follows from [2, p.12] that $v > q^{n(n-i)}/(t!)$. Let $i = 1$. By [35, p. 340], we have that k divides $2\lambda n(n-1)(q-1)$. Then Lemma 8(b) implies that $\lambda q^{n(n-1)}/(n!) < \lambda v < k^2 \leqslant \lambda^2 4n^2(n-1)^2(q-1)^2$. Therefore,

$$q^{n(n-1)} < 4\lambda \cdot (n!) \cdot n^2(n-1)^2(q-1)^2. \tag{24}$$

Since λ is an odd prime divisor of k, by Lemmas 7 and 8(b), λ must divide a, $n!$ or $q-1$. Then $\lambda \leqslant \max\{a, n, q-1\}$, and so $\lambda < n \cdot (q-1)$. Thus by (24), we conclude that

$$q^{n(n-1)} < 4n^3 \cdot (n!) \cdot (n-2)^2(q-1)^3. \tag{25}$$

It follows from Lemma 16 that $q^{n(n-1)} < 2^{[4n(n-3)+6]/3} \cdot n^5(q-1)^3$. Since $n^5 < 2^{3n}$, we conclude that $q^{3n^2-3n-9} < 2^{4n^2-3n+6}$, and so $3n^2-3n-9 \leqslant (3n^2-3n-9)\cdot \log_p q \leqslant (4n^2-3n+6)\cdot\log_p 2 \leqslant (4n^2-3n+6)\cdot \log_3 2 < (4n^2-3n+6)\times 0.7$. Hence $2n^2-9n < 132$. This inequality holds only for $n = 6, 7, 8, 9, 10$. However, for each such value of n, the inequality (25) does not hold, which is a contradiction. Therefore, $i \geqslant 2$, in which case by [35, p. 340], k must divide $\lambda t(t-1)(q^i-1)^2(q-1)^{-1}$. Then Lemma 8(b) implies that $\lambda q^{n(n-i)}/(t!) < \lambda v < k^2 \leqslant \lambda^2 t^2(t-1)^2(q^i-1)^4(q-1)^{-2}$. Therefore,

$$q^{n(n-i)} \cdot (q-1)^2 < \lambda \cdot (t!) \cdot t^2 \cdot (t-1)^2(q^i-1)^4. \tag{26}$$

Since λ is an odd prime divisor of k, by Lemmas 7 and 8(b), λ must divide a, p, $t!$ or q^j-1 for some $j \leqslant i$, and so $\lambda \leqslant \max\{a, p, t, (q^i-1)(q-1)^{-1}\}$, consequently

$$\lambda < t \cdot (q^i-1)(q-1)^{-1}. \tag{27}$$

Then (26) implies that $q^{n(n-i)} \cdot (q-1)^3 < t^5 \cdot (t!) \cdot (q^i-1)^5$. If $t \geqslant 4$, then by Lemma 16(b), we have that $t! < 2^{4t(t-3)/3}$, and hence $q^{3n(n-i)} \cdot (q-1)^9 < 2^{4t(t-3)} \cdot t^{15} \cdot (q^i-1)^{15}$. Since $t^{15} < 2^{9t}$ and $q^i - 1 < q^i$, it follows that

$$q^{3n^2-3i(n+5)+3} < 2^{4t^2-3t}, \tag{28}$$

where $n = it$. Therefore, $t^2(3i^2-4)+3 < 3t(i^2-1)+15i < 3ti(i+5)$, and so $t(3i^2-4) < 3i(i+5)$. This inequality holds only for $(i,t) = (2,4)$ or $(2,5)$. For these pairs of (i,t), we can easily observe that the inequality (28) does not hold, which is a contradiction. Hence $t = 2, 3$. If $t = 2$, then (26) and (27) imply that $q^{2i^2} \cdot (q-1)^3 < 16 \cdot (q^i-1)^5$. As $(q-1)^3 \geqslant 8$, we conclude that $q^{2i^2-5i-1} < 1$, and so $i = 2$ for which $n = 2i = 4$, which is impossible. If $t = 3$, then by (26) and (27), we have that $q^{6i^2} \cdot (q-1)^3 < 2^3 \cdot 3^4 \cdot (q^i-1)^5$, and so $q^{6i^2} < q^{5i+4}$, which is impossible.

(5) Let $H = N_G(X(q_0))$ with $q = q_0^t$ odd and t odd prime. Then by [23, Proposition 4.5.3], the subgroup H_0 is isomorphic to

$$\hat{\ }\mathrm{SL}_n(q_0) \cdot \gcd((q-1)(q_0-1)^{-1}, n)$$

with $q = q_0^t$. Note that $|\mathrm{Out}(X)| = 2a \cdot \gcd(n, q-1)$. Since $|X| < |\mathrm{Out}(X)|^2 \cdot |H_0|^3$ by Corollary 12, it follows from Lemma 15 that $q_0^{t(n^2-2)} < 4a^2 \cdot q_0^{3n^2}(q_0^t-1)^3$. As $a^2 < 2q$, we have that $q_0^{n^2(t-3)-6t} < 8$. Since also q_0 is odd, it follows that $3^{n^2(t-3)-6t} \leqslant q_0^{n^2(t-3)-6t} < 8 < 3^2$, and so $3^{n^2(t-3)-6t} < 3^2$. Therefore, $t(n^2-6) < 3n^2+2$. If $t \geqslant 5$, then $5(n^2-6) \leqslant t(n^2-6) < 3n^2+2$, and so $n^2 < 16$, which is impossible as $n \geqslant 5$. Therefore, $t = 3$. In this case by (1) and Lemma 15, we conclude that $v > q_0^{2n^2-9}$. It follows from Lemma 8(a)-(c) that k divides $\lambda \gcd(v-1, |\mathrm{Out}(X)| \cdot |H_0|)$. By Tits' Lemma 10 $v-1$ is coprime to q_0, and so k must divide $2\lambda a \cdot g(q_0)$, where $g(q_0) = (q_0^n-1)\cdots(q_0^2-1)\cdot \gcd(q_0^2+q_0+1, n)$. Then by Lemma 8(b), we have that $\lambda q_0^{2n^2-9} < \lambda v < k^2 \leqslant 4a^2\lambda^2(q_0^n-1)^2 \cdots (q_0^2-1)^2 \cdot (q_0^2+q_0+1)^2$. Note that $(q_0^2+q_0+1)^2 < q_0^5$. So

$$q_0^{n^2-n-12} < 4\lambda a^2. \tag{29}$$

Note by Lemmas 7 and 8(b) that λ is an odd prime divisor of a, p, q_0-1 or $(q_0^j-1)/(q_0-1)$ with $j \in \{2, 3, \ldots, n\}$, and so $\lambda \leqslant (q_0^n-1)/(q_0-1)$. Then by the inequality (29), we conclude that $q_0^{n^2-2n-12}(q_0-1) < 4a^2$. Recall that $a = ts = 3s$. Then $q_0^{n^2-2n-12}(q_0-1) < 36s^2$. Since $n \geqslant 5$, we have that $q_0^3(q_0-1) \leqslant q_0^{n^2-2n-12}(q_0-1) < 36 \cdot s^2$, and hence $q_0^3(q_0-1) < 36 \cdot s^2$, which is impossible. □

Proposition 19. *Let $\mathcal{D}$ be a nontrivial symmetric (v, k, λ) design with $\lambda \geqslant 5$ prime. Suppose that G is an automorphism group of $\mathcal{D}$ of almost simple type with socle X. If G is flag-transitive and point-primitive, then the socle X cannot be* $\mathrm{PSU}_n(q)$ *with $n \geqslant 5$.*

Proof. Let $H_0 = H \cap X$, where $H = G_\alpha$ with α a point of $\mathcal{D}$. Then by Lemma 8(a), the parameter v is odd, and so by Lemma 14, one of the following holds:

(1) q is even, and H_0 is a parabolic subgroup of X;

(2) q is odd, and H is the stabilizer of a nonsingular subspace;

(3) q is odd, and H_0 is the stabilizer of an orthogonal decomposition $V = \oplus V_j$ with all V_j's isometric;

(4) $q = q_0^t$ is odd with t odd prime, and $H = N_G(X(q_0))$.

We analyse each of these possible cases separately and arrive at a contradiction in each case.

(1) Let H_0 be a parabolic subgroup of X. Note in this case that $q = 2^a$ is even. By [23, Proposition 4.1.18], the subgroup H_0 is isomorphic to $\hat{}q^{i(2n-3i)} : \mathrm{SL}_i(q^2) \cdot \mathrm{SU}_{n-2i}(q) \cdot (q^2-1)$, for $i \leqslant \lfloor n/2 \rfloor$. It follows from (1) and [35] that $v > q^{i(2n-3i)}$. By Lemma 11, there is a unique subdegree $d = 2^c$. Note that

$$(v-1)_2 = \begin{cases} q, & \text{if } n \text{ is even and } i = n/2; \\ q^3, & \text{if } n \text{ is odd and } i = (n-1)/2; \\ q^2, & \text{otherwise,} \end{cases}$$

where $(v-1)_2$ is the 2-part of $v-1$. Since k divides $\lambda \gcd(v-1, d)$, it follows that k divides λq^t, where $t = 1, 2, 3$. Note that λ is an odd prime divisor of k. It follows from

Lemma 8(b) that λ must divide a, $q^{2j}-1$, for some $j \in \{1, 2, \dots, i\}$ or $q^j - 1$, for some $j \in \{2, \dots, n-2i\}$. Since $\max\{q^{n-2i}+1, q^i+1\} < q^{n-2}+1$, we conclude that

$$\lambda < q^{n-2}+1, \tag{30}$$

where $2i \leqslant n$. Then by Lemma 8(b), we have that $\lambda q^{i(2n-3i)} < \lambda v < k^2 \leqslant \lambda^2 q^6$, and so

$$q^{i(2n-3i)} < \lambda q^6. \tag{31}$$

It follows from (30) that $q^{i(2n-3i)} < q^6(q^{n-2}+1)$. Since $q^6(q^{n-2}+1) < q^{n+5}$, we have that $q^{i(2n-3i)} < q^{n+5}$, and so

$$n \cdot (2i-1) < 3i^2 + 5. \tag{32}$$

As $n \geqslant 2i$, it follows that $i^2 < 2i+5$. This inequality holds only for $i = 1, 2, 3$. If $i = 1$, then k divides λq^2. Let u be a positive integer such that $uk = \lambda q^2$. Since $\lambda < k$, we have that $u < q^2$. By [6, Lemma 3.7(a)], u is coprime to k, and so $u = 1$ or $u = q^2$. In the later case, we would have $k = \lambda$, which is a contradiction. Therefore, $u = 1$ and $k = \lambda q^2$. Note for $n \geqslant 4$ that $v - 1 = s(q) + q^2$, where $s(q)$ is a polynomial divisible by q^4. Since $k(k-1) = \lambda(v-1)$ and $k = \lambda q^2$, we have that $k = 1 + [s(q) + q^2]/q^2 = [s(q) + 2q^2]/q^2$. Therefore, $\lambda = [s(q) + 2q^2]/q^4$. Since q^4 divides $s(q)$, it follows that q^4 divides $2q^2$, which is impossible. If $i \in \{2, 3\}$, by the same argument as in the case where $i = 1$, we conclude that $n = 5$ and $k = \lambda q^3$ if $i = 2$, and $n = 6$ and $k = \lambda q$ if $i = 3$. Thus

$$\lambda = \begin{cases} \dfrac{q^5+q^2+2}{q^3}, & \text{if } i = 2; \\ \dfrac{q^8+q^7+q^5+q^4+q^3+q^2+2}{q}, & \text{if } i = 3. \end{cases}$$

Since λ has to be integer, it follows that $q = 2$ when $(n, i) = (6, 3)$ in which case $(v, k, \lambda) = (891, 446, 223)$, but by [11], we have no symmetric design with this parameters set.

(2) Let H be the stabilizer of a nonsingular subspace, and let q be odd. Here by [23, Proposition 4.1.4], H_0 is isomorphic to

$$\hat{}\mathrm{SU}_i(q) \times \mathrm{SU}_{n-i}(q) \cdot (q+1),$$

where $2i < n$. Then by (1) and Lemma 15, we have that $v > q^{2i(n-i)-6}$. It follows from [35, p. 336] that k divides $\lambda d_i(q)$, where $d_i(q) = (q^i - (-1)^i)(q^{n-i} - (-1)^{n-i})$. Then Lemma 8(b) implies that $\lambda q^{2i(n-i)-6} < \lambda v < k^2 \leqslant \lambda^2 (q^i - (-1)^i)^2 (q^{n-i} - (-1)^{n-i})^2$. Since $q^i - (-1)^i < 2q^i$ and $q^{n-i} - (-1)^{n-i} < 2q^{n-i}$, we have that

$$q^{2i(n-i)-6} < 16\lambda q^{2n}. \tag{33}$$

Since λ is an odd prime divisor of k, it follows from Lemmas 7 and 8(b) that λ divides a, p, $q \pm 1$, or $(q^j - (-1)^j)(q - (-1)^j)^{-1}$ with $j \in \{3, \dots, n-i\}$. Thus $\lambda \leqslant \lambda_i(q)$, where

$$\lambda_i(q) = \begin{cases} (q^{n-i}+1)(q+1)^{-1}, & \text{if } \quad n-i \quad \text{is odd;} \\ (q^{n-i-1}+1)(q+1)^{-1}. & \text{if } \quad n-i \quad \text{is even.} \end{cases} \tag{34}$$

Then by (33) and (34), we have that $q^{2i(n-i)-6} \cdot (q+1) < 32q^{3n-i}$, and so $n(2i-3)+i < 2i^2+8$. Since $n > 2i$, we conclude that $4i^2-5i < n(2i-3)+i < 2i^2+8$, and so $2i^2 < 5i+8$. This inequality holds only for $i = 1, 2, 3$.

Let $i = 1$. In this case by (1), we have that $v = q^{n-1}(q^n - (-1)^n)(q+1)^{-1}$. If n is even, then as q is odd, v is even, which is a contradiction. Therefore, n is odd, and hence $v = q^{n-1}(q^n+1)(q+1)^{-1}$. Recall that k divides $\lambda d_1(q)$, where $d_1(q) = (q+1)(q^{n-1}-1)$. Since $\gcd(v-1, (q+1)(q^{n-1}-1)) = (q^{n-1}-1)(q+1)^{-1}$, it follows that k divides $\lambda f(q)$, where $f(q) = (q^{n-1}-1)(q+1)^{-1}$. Let u be a positive integer such that $uk = \lambda f(q)$. Then by Lemma 8(a), we have that

$$k = u \cdot (q^n + q + 1) + 1 \quad \text{and} \quad \lambda = u^2 q(q+1) + \frac{u^2(2q+1)+u}{f(q)}. \tag{35}$$

Recall that $uk = \lambda f(q)$, where $f(q) = (q^{n-1}-1)(q+1)^{-1}$. Then by (34) and (35), we have that $u^2(q^n+q+1)+u < (q^{n-2}+1)(q^{n-1}-1)(q+1)^{-2}$. Therefore, $u^2q^n(q+1)^2 < (q^{n-2}+1)(q^{n-1}-1) < q^n(q^{n-3}+1)$. Note that $(q^{n-3}+1)(q+1)^{-2} < q^{n-5}$. Thus

$$u^2 < q^{n-5}. \tag{36}$$

Since λ is integer, by (35), we conclude that $f(q)$ divides $u^2(2q+1)+u$. Thus $q^n - 1 \leqslant [u^2(2q+1)+u](q+1)$. As $[u^2(2q+1)+u](q+1) < 6u^2q^2$, it follows that $q^n - 1 < 6u^2q^2$, and so by (36), we conclude that $q^n - 1 < 6q^{n-3}$. Therefore, $q^2 \leqslant 6$, which is impossible as q is odd.

Let $i = 2$ or 3. Then

$$v = \frac{q^{i(n-i)} \cdot w_i(n,q)}{(q^i - (-1)^i)\cdots(q+1)},$$

where $w_i(n,q) = (q^n - (-1)^n)\cdots(q^{n-i+1} - (-1)^{n-i+1})$. Since k divides $\lambda d_i(q) = \lambda(q^i - (-1)^i)(q^{n-i} - (-1)^{n-i})$, it follows from Lemma 8(b) and (34) that $w_i(n,q) < q^{n-5}(q^3-1)^2$ when $i = 2$, and $w_i(n,q) < 32q^6(q^3+1)(q^2-1)$ when $i = 3$. If $i = 2$, then $w_2(n,q) \geqslant q^n(q^{n-1}-1)$, and so $q^5(q^{n-1}-1) < (q^3-1)^2$, which is impossible as $n > 2i = 4$. If $i = 3$, then since $n > 2i = 6$, $w_3(n,q) \geqslant (q^7+1)(q^6-1)(q^5+1)$, and so $(q^7+1)(q^6-1)(q^5+1) < 32q^6(q^3+1)(q^2-1)$, which is impossible.

(3) Let H_0 be the stabilizer of an orthogonal decomposition $V = \oplus V_j$ with all V_j's isometric, and let q be odd. In this case, by [23, Proposition 4.2.9], H_0 is isomorphic to

$$\hat{}\mathrm{SU}_i(q)^t \cdot (q+1)^{t-1} \cdot \mathrm{Sym}_t$$

It follows from [2, Proposition 3.5] that $v > q^{i^2t(t-1)/2}/(t!)$. Suppose first that $i \geqslant 2$. Since λ is an odd prime divisor of k, the parameter λ must divide $2a \cdot (t!) \cdot q^{it(i-1)/2)}(q^i - (-1)^i)^t \cdots (q^2-1)^t(q+1)^{t-1}$. Since $\max\{p, t, (q^i - (-1)^i)/2\} < t \cdot (q^i - (-1)^i)/2$, it follows that

$$\lambda < t \cdot (q^i - (-1)^i)/2. \tag{37}$$

By [35, p.336], the parameter k divides $\lambda t(t-1)(q^i-(-1)^i)^2$. Then by Lemma 8(b), we have that $\lambda q^{i^2t(t-1)/2}/(t!) < \lambda v < k^2 \leqslant t^2(t-1)^2\lambda^2(q^i-(-1)^i)^4$, and so

$$q^{i^2t(t-1)/2} < \lambda \cdot (t!) \cdot t^2(t-1)^2(q^i-(-1)^i)^4. \tag{38}$$

Then by (37), we have that $2q^{i^2t(t-1)/2} < (t!)\cdot t^3(t-1)^2(q^i-(-1)^i)^5$. Since $q^i-(-1)^i < 2q^i$, it follows that $q^{i^2(t^2-t)/2} < 16(t!)\cdot t^3(t-1)^2q^{5i}$. If $t \geqslant 4$, then by Lemma 16(b), we have that $t! < 2^{4t(t-3)/3}$, and so $q^{i^2(t^2-t)/2} < 2^{[4t(t-3)+12]/3}\cdot t^5q^{5i}$. Note that $t^5 \leqslant 2^{3t}$. Thus, $q^{i^2(t^2-t)/2} < 2^{[4t^2-3t+12]/3}\cdot q^{5i}$, and so $q^{3i^2(t^2-t)-30i} < 2^{8t^2-6t+24}$. Therefore,

$$t^2(3i^2-8) < 3i^2t+30i-6t+24. \tag{39}$$

Since $t \geqslant 4$, we have that $t^2(3i^2-8) < 3i^2t+30i-6t+24 < (3i^2+30i)t$, and so $t(3i^2-8) < 3i^2+30i$. Thus $12i^2-32 \leqslant t(3i^2-8) < 3i^2+30i$, and so $9i^2-30i < 32$. Then $i = 2, 3, 4$.

Suppose that $i = 2$. Then by (39), we conclude that $4t^2 < 6t+84$ implying that $t = 4, 5$. If $(i,t) = (2,4)$, then by (38) and (37), we have that $q^{24} < 4^4\cdot 3^3(q^2-1)^5$, which is impossible. If $(i,t) = (2,5)$, then by (38) and (37), we conclude that $q^{40} < 5^4\cdot 4^3\cdot 3(q^2-1)^5$, which is impossible. The case where $i = 3, 4$, can be ruled out by the same manner as above.

Suppose now that $i = 1$. Then H_0 is isomorphic to $\hat{}(q+1)^{n-1}\cdot \mathrm{Sym}_n$, and so by (1), we have that

$$v = \frac{q^{n(n-1)/2}(q^n-(-1)^n)\cdots(q^2-1)}{(q+1)^{n-1}\cdot n!}. \tag{40}$$

Note that λ is an odd prime divisor of k. Then λ divides $2a(n!)(q+1)^{n-1}$. Therefore, λ must divide a, $n!$ or $q+1$, and so $\lambda \leqslant \max\{a, n, (q+1)/2\}$. In conclusion, $\lambda < n(q+1)/2$. We now consider the following subcases:

(3.1) Let $q \geqslant 5$. Here by [35, p.337], we have that k divides $\lambda n(n-1)(q+1)^2/2$. Then Lemma 8(b) implies that $4q^{n(n-1)/2}(q^n-(-1)^n)\cdots(q^2-1) < \lambda(n!)\cdot n^2(n-1)^2(q+1)^{n+3}$. Recall that $\lambda < n(q+1)/2$. Therefore,

$$8q^{n(n-1)/2}(q^n-(-1)^n)\cdots(q^2-1) < (n!)\cdot n^3(n-1)^2(q+1)^{n+4}. \tag{41}$$

Note that $q+1 < 2q$. Then (41) and Lemma 17 imply that $q^{n^2-2n-4} < 2^{n+1}(n!)\cdot n^3(n-1)^2 < 2^{n+1}(n!)\cdot n^5$. As $n \geqslant 5$, we conclude that $n^5 \leqslant 2^{3n}$. Then by [8, Lemma 4.4], we have that $q^{3n^2-6n-12} < 2^{4n^2+3}$. Since $q \geqslant 5$, it follows that $2^{6n^2-12n-24} < q^{3n^2-6n-12} < 2^{4n^2+3}$. Thus $2n^2 < 12n+27$, and so $n = 5, 6, 7$. Let now $h_n(q) = 8q^{(n^2-3n-8)/2}(q^n-(-1)^n)\cdots(q^2-1)$. Then since $q+1 < 2q$, we conclude by (41) that $h_n(5) \leqslant h_n(q) < 2^{n+4}\cdot n^3(n-1)^2(n!)$, for $n \in \{5, 6, 7\}$. Define

$$u_n = \begin{cases} 2^{16}\cdot 3\cdot 5^4, & \text{if } n = 5; \\ 2^{17}\cdot 3^5\cdot 5^3, & \text{if } n = 6; \\ 2^{17}\cdot 3^4\cdot 5\cdot 7^4, & \text{if } n = 7. \end{cases}$$

Then $h_n(q) < u_n$ for $n \in \{5, 6, 7\}$, and hence $h_n(5) < u_n$, which is impossible.

(3.2) Let $q = 3$. Here by [35, p.337], we have that k divides $\lambda n(n-1)(n-2)(q+1)^3/6$. Then Lemma 8(b) implies that $6q^{n(n-1)/2}(q^n - (-1)^n) \cdots (q^2-1) < \lambda(n!) \cdot n^2(n-1)^2(n-2)^2(q+1)^{n+5}$. Recall that $\lambda < n$. Therefore,

$$3q^{n(n-1)/2}(q^n - (-1)^n) \cdots (q^2-1) < 2^{2n+9}n^3(n-1)^2(n-2)^2 \cdot (n!). \tag{42}$$

Since $q^{n(n-1)/2} \leqslant (q^n-(-1)^n) \cdots (q^2-1)$, replacing q by 3, we have that $3^{n^2-n} < 2^{2n+9}(n!) \cdot n^3(n-1)^2(n-2)^2 < 2^{2n+9}(n!) \cdot n^7$. As $n \geqslant 5$, we conclude that $n^7 \leqslant 2^{4n}$, and so [8, Lemma 4.4] implies that $3^{3n^2-3n} < 2^{4n^2+6n+27}$. Therefore, $3n^2 - 3n < (4n^2+6n+27) \cdot \log_3 2 < (4n^2+6n+27) \times 0.7$, and so $2n^2 < 72n + 189$, and hence $n \in \{5, \ldots, 38\}$. Let $h_n(q) = 3q^{(n^2-n)/2}(q^n - (-1)^n) \cdots (q^2-1)$. Then $h_n(3) < u_n$, where $u_n = 2^{2n+9}n^3(n-1)^2(n-2)^2 \cdot (n!)$. However, it is easy to check that this inequality does not hold for $n \in \{5, \ldots, 38\}$.

(4) Let $H = N_G(X(q_0))$ with $q = q_0^t$ odd and t odd prime. By [23, Proposition 4.5.3], the subgroup H_0 is isomorphic to

$$\hat{}\mathrm{SU}_n(q_0) \cdot \gcd((q+1)/(q_0+1), n).$$

Since $|\mathrm{Out}(X)| = 2a \cdot \gcd(n, q+1)$, by Lemma 15 and the inequality $|X| < |\mathrm{Out}(X)|^2 \cdot |H_0|^3$, we have that $q_0^{t(n^2-2)} < 8a^2 \cdot q_0^{3n^2}(1+q_0^{-1})^3(1+q_0^{-3})^3(q_0^t+1)^3$. As $a^2 < 2q$, $q_0^t + 1 < 2q_0^t$ and $(1+q_0^{-1})^3(1+q_0^{-3})^3 < 2$, we have that $q_0^{n^2(t-3)-6t} < 256$. Note that q_0 is odd. So $3^{n^2(t-3)-6t} < 256$. If $t \geqslant 5$, then $3^{2n^2-30} < 256 < 3^6$, and so $2n^2 - 30 < 6$, which contradicts the fact that $n \geqslant 5$. Therefore, $t = 3$. In this case, by (1) and Lemma 15, we have that $v > q_0^{2n^2-10}$. By Lemmas 7 and 8(b), the parameter k divides $2a \cdot q_0^{n(n-1)/2}(q_0^n - (-1)^n) \cdots (q_0^2-1) \cdot \gcd(q_0^2 - q_0 + 1, n)$. It follows from Lemma 8(a) and (c) that k divides $\lambda \gcd(v-1, |\mathrm{Out}(X)| \cdot |H_0|)$. Since by Lemma 10, $v-1$ is coprime to q_0, we conclude that

$$k \text{ divides } 2a\lambda \cdot |H_0|_{p'}. \tag{43}$$

Then by (43) and Lemma 8(b), we have that

$$\lambda q_0^{2n^2-10} < \lambda v < k^2 \leqslant 4a^2\lambda^2(q_0^n - (-1)^n)^2 \cdots (q_0^2-1)^2 \cdot (q_0^2 - q_0 + 1)^2.$$

Since $(q_0^2 - q_0 + 1)^2 < q_0^4$, we conclude that $q_0^{n^2-n-12} < 4a^2\lambda$. Since also λ is an odd prime divisor of $|H|$, it must divide a, p, $q \pm 1$ or $(q_0^j - (-1)^j)/(q_0 - (-1)^j)$, for some $j \in \{2, 3, \ldots, n\}$. Then $\lambda \leqslant (q_0^n - 1)/(q_0 - 1)$, and so the inequality $q_0^{n^2-n-12} < 4a^2\lambda$ implies that $q_0^{n^2-2n-12}(q_0-1) < 4a^2$. As $a = 3s$ and $n \geqslant 5$, it follows that $q_0^3(q_0-1) \leqslant q_0^{n^2-2n-12}(q_0-1) < 36s^2$. Therefore, $q_0^3(q_0-1) < 36s^2$, which is impossible. □

Proposition 20. *Let $\mathcal{D}$ be a nontrivial symmetric (v, k, λ) design with λ prime. Suppose that G is an automorphism group of $\mathcal{D}$ of almost simple type with socle X. If G is flag-transitive and point-primitive, then the socle X cannot* $\mathrm{PSp}_{2m}(q)$ *with* $(m, q) \neq (2, 2), (2, 3)$.

Proof. Let $H_0 = H \cap X$, where $H = G_\alpha$ with α a point of $\mathcal{D}$. Then by Lemma 8(a), v is odd, and so by Lemma 14 one of the following holds:

(1) q is even, and H_0 is a parabolic subgroup of X;

(2) q is odd, and H is the stabilizer of a nonsingular subspace;

(3) q is odd, and H_0 is the stabilizer of an orthogonal decomposition $V = \oplus V_j$ with all V_j's isometric;

(4) $q = q_0^t$ is odd with t odd prime, and $H = N_G(X(q_0))$.

We now analyse each of these possible cases separately.

(1) Let H_0 be a parabolic subgroup of X, and let $q = 2^a$ be even. Then [23, Proposition 4.1.19] implies that H_0 is isomorphic to

$$[q^h] \cdot (\mathrm{GL}_i(q) \times \mathrm{PSp}_{2m-2i}(q)),$$

where $h = 2mi + (i - 3i^2)/2$ and $i \leqslant m$. It follows from (1) and Lemma 15 that $v > q^{i(4m-3i)}$. By Lemma 11, there is a unique subdegree $d = 2^c$. The 2-power $(v-1)_2$ is q. Since k divides $\lambda \gcd(v-1, d)$, it follows that k divides λq. By the fact that λ is an odd prime divisor of k, Lemma 8(b) implies that λ must divide a, $q^j - 1$ with $j \in \{1, \dots, i\}$ or $q^{2j} - 1$ with $j \in \{1, \dots, m-i\}$. Thus

$$\lambda \leqslant (q^m - 1)/(q-1). \tag{44}$$

It follows from Lemma 8(b) that $\lambda q^{i(4m-3i)} < \lambda v < k^2 \leqslant \lambda^2 q^2$, and so $q^{i(4m-3i)} < \lambda q^2$. Then by (44), we have that

$$q^{i(4m-3i)}(q-1) < q^2(q^m - 1). \tag{45}$$

Therefore, $i(4m - 3i) < m + 2$, and so $m(4i - 1) < 3i^2 + 2$. Since $i \leqslant m$, it follows that $i(4i - 1) \leqslant m(4i - 1) < 3i^2 + 2$. Thus $i^2 < i + 2$, and hence $i = 1$. By (45), we have that $q^{4m-3}(q-1) < q^2(q^m - 1)$, and so $q^{4m-3} < q^{m+2}$, which is impossible.

(2) Let H be the stabilizer of a nonsingular subspace, and let q be odd. Here by [23, Proposition 4.1.3], the subgroup H_0 is isomorphic to

$$\mathrm{PSp}_{2i}(q) \times \mathrm{PSp}_{2m-2i}(q) \cdot 2,$$

where $2i < m$. In this case, $v > q^{4i(m-i)}$, and so Lemma 8(c) implies that k divides $\lambda d_i(q)$, where $d_i(q) = (q^{2i}-1)(q^{2m-2i})(q^2-1)^{-2}$. Again by Lemma 8(b), we conclude that $\lambda q^{4i(m-i)} < \lambda v < k^2 \leqslant \lambda^2(q^{2i} - 1)^2(q^{2m-2i} - 1)^2(q^2 - 1)^{-4}$. Therefore,

$$q^{4i(m-i)}(q^2 - 1)^4 < \lambda(q^{2i} - 1)^2(q^{2m-2i} - 1)^2 \tag{46}$$

Since λ is an odd prime divisor of k, Lemmas 7 and 8(b) imply that λ must divide a, p or $q^{2j} - 1$, for some $j \in \{1, \dots, m-i\}$, and so

$$\lambda \leqslant q^{m-i} + 1. \tag{47}$$

Then by (46), we have that $q^{4i(m-i)+6} < q^{5m-i}$. Thus $4i(m-i)+6 < 5m-i$, and so $m(4i-5) < 4i^2-i-6$. As $m > 2i$, the last inequality holds only for $i=1$, in which case by (1), we have that $v = q^{2m-2}(q^{2m}-1)(q^2-1)^{-1}$ and

$$k \text{ divides } \lambda d_1(q), \tag{48}$$

where $d_1(q) = (q^{2m-2}-1)(q^2-1)^{-1}$. Let u be a positive integer such that $uk = \lambda d_1(q)$. Since $v-1 = (q^{2m-2}-1)(q^{2m}+q^2-1)(q^2-1)^{-1}$, by Lemma 8(a), we have that

$$k = u\cdot(q^{2m}+q^2-1)+1 \quad \text{and} \quad \lambda = u^2q^2(q^2-1)+\frac{u^2(2q^2-1)+u}{d_1(q)}. \tag{49}$$

It follows from (49) and (48) that $u\cdot(q^{2m}+q^2-1)+1 \leqslant (q^{m-1}+1)(q^{2m-2}-1)(q^2-1)^{-1}$, and so $uq^{2m}(q^2-1) < (q^{m-1}+1)(q^{2m-2}-1)$. Since $(q^{m-1}+1)(q^{2m-2}-1) < q^{2m-2}(q^{m+1}+1)$, we have that $u \leqslant 2q^{m-4}$. Since λ is a positive integer, we conclude by (49) that $d_1(q)$ must divide $u^2(2q^2-1)+u$. Since also $u \leqslant 2q^{m-4}$, we have that $q^{2m-2}-1 \leqslant (u^2(2q^2-1)+u)(q^2-1) \leqslant 2u^2q^2(q^2-1) < 8q^{2(m-4)+2}(q^2-1)$, and so $q^{2m-2}-1 < 8q^{2m-6}(q^2-1)$. Thus $q^{2m-2}-1 < 8q^{2m-4}$, and hence $q^2 \leqslant 8$, which is impossible as q is odd.

(3) Let H_0 be the stabilizer of an orthogonal decomposition $V = \oplus V_j$ with all V_j's isometric, and let q be odd. In this case, by [23, Proposition 4.2.10], the subgroup H_0 is isomorphic to $\hat{\ }\mathrm{Sp}_{2i}(q)\wr\mathrm{Sym}_t$ with $it = m$. Here by [2, p.16], we have that $v > q^{2i^2t(t-1)}/(t!)$. The parameter λ divides k. Then it divides $2a\cdot(t!)\cdot q^{i^2t}(q^{2i}-1)^t\cdots(q^2-1)^t$ by Lemmas 7 and 8(b). Therefore, λ divides a, p, $t!$ or $q^{2j}-1$, for some $j \in \{1,\dots,i\}$, and since $\lambda \leqslant \max\{a,p,t,(q^i+1)/2\}$, it follows that

$$\lambda < t\cdot(q^i+1)/2. \tag{50}$$

Note also by [35, p.328] that

$$k \quad \text{divides} \quad \lambda t(t-1)(q^{2i}-1)^2(q-1)^{-1}/2. \tag{51}$$

Then Lemma 8(b) implies that $\lambda v < k^2 \leqslant \lambda^2t^2(t-1)^2(q^{2i}-1)^4(q-1)^{-2}/4$, and so

$$4q^{2i^2t(t-1)}(q-1)^2 < \lambda\cdot t^2(t-1)^2(t!)(q^{2i}-1)^4. \tag{52}$$

It follows from (50) and (52) that

$$8q^{2i^2t(t-1)}(q-1)^2 < t^3(t-1)^2(t!)(q^{2i}-1)^4(q^i+1). \tag{53}$$

We now consider the following subcases:

(3.1) Assume first that $t \geqslant 4$. Note by Lemma 16(b) that $t! < 2^{4t(t-3)/3}$. Then $4^3q^{6i^2t(t-1)}\cdot(q-1)^6 < 2^{4t(t-3)}\cdot t^{15}(q^{2i}-1)^{12}q^{3i}$, and so $q^{6i^2t^2-6i^2t-27i+3} < 2^{4t^2-3t-6}$. Thus $2t^2(3i^2-2) < 3t(2i^2-1)+27i-9 < 3ti(2i+9)$. Therefore,

$$2t(3i^2-2) < 3i(2i+9). \tag{54}$$

As $t \geqslant 4$, it follows that $8(3i^2-2) \leqslant 2t(3i^2-2) < 3i(2i+9)$, and so $8(3i^2-2) < 3i(2i+9)$. Then $i = 1, 2$. If $i = 2$, then by (54), we conclude that $20t = 2t(3i^2-2) < 3i(2i+9) = 78$, and so $t < 4$, which is a contradiction. Therefore, $i = 1$. By (53), we have that $8q^{2t(t-1)}(q-1)^2 < t^3(t-1)^2(t!)(q^2-1)^4(q+1)$. As $t \geqslant 4$, by Lemma 16(b), we conclude that $4q^{2t(t-1)-8} < 2^{4t(t-3)/3}{\cdot}t^5$. Since $t^5 < 2^{3t}$, we have that $q^{6t(t-1)-24} < 2^{4t^2-3t-6}$. Thus $6t(t-1)-24 \leqslant [6t(t-1)-24]{\cdot}\log_p q < (4t^2-3t-6)\cdot\log_p 2 < (4t^2-3t-6)\times 0.7$. Therefore, $32t^2-39t < 198$, which is impossible for any $t \geqslant 4$.

(3.2) Assume now that $t = 3$. It follows from (53) that $q^{12i^2}{\cdot}(q-1)^2 < 3^4{\cdot}(q^{2i}-1)^4(q^i+1)$. Since $q^{2i}-1 < q^{2i}$ and $q^i+1 < 2q^i$, we conclude that $q^{12i^2}{\cdot}(q-1)^2 < 3^4{\cdot}(q^{2i}-1)^4(q^i+1) < 2\cdot 3^4 q^{9i}$, and so $q^{12i^2} < q^{9i+4}$. Thus $i = 1$. Again, we apply (53) and conclude that $q^{12}{\cdot}(q-1)^2 < 3^4{\cdot}(q^2-1)^4(q+1)$, which is impossible.

(3.3) Assume finally that $t = 2$. The inequality (53) implies that $q^{4i^2}{\cdot}(q-1)^2 < 2(q^{2i}-1)^4(q^i+1)$. Since $q^i+1 < 2q^i$, we have that $q^{4i^2}{\cdot}(q-1)^2 < 2q^{9i}$. This inequality holds only for $i \in \{1, 2\}$. If $i = 2$, then $m = 4$, and so by (1), we have that $v = q^8(q^4+q^2+1)(q^4+1)/2$. By (51) and Lemma 8(a), the parameter k must divide $\lambda(q^2+1)^2$. Then by Lemma 8(b), we conclude that $\lambda q^8(q^4+q^2+1)(q^4+1)/2 < k^2 \leqslant \lambda^2(q^2+1)^4$, and so $q^8(q^4+q^2+1)(q^4+1) < 2\lambda(q^2+1)^4$. Then (50) implies that $q^8(q^4+q^2+1)(q^4+1) < (q^2+1)^5$, which is impossible. Therefore, $i = 1$, and hence (1) implies that

$$v = \frac{q^2(q^2+1)}{2}. \tag{55}$$

Since $\gcd(v-1, q+1)$ divides $\gcd(3, q+1)$, it follows from (51) and Lemma 8(a) that

$$k \text{ divides } c_1\lambda f(q),$$

$f(q) = q^2-1$ and $c_1 = \gcd(3, q+1)$. Let now u be a positive integer such that $uk = c_1\lambda f(q)$. Then Lemma 8 implies that

$$2c_1k = u\cdot(q^2+2) + 2c_1 \quad \text{and} \quad 2c_1^2\lambda = u^2 + \frac{3u^2+2c_1u}{q^2-1}. \tag{56}$$

Recall that k divides $\lambda\cdot c_1 f(q)$. Then (56) implies that $u(q^2+2)+2c_1 \leqslant 2\lambda\cdot c_1^2 f(q)$, and so

$$u < 2c_1^2\lambda. \tag{57}$$

Note that λ is an odd prime divisor of k. Then Lemmas 7 and 8(b) implies that λ divides $4aq^2(q^2-1)^2$. Therefore, λ divides a, p, $(q-1)/2$ or $(q+1)/2$. We now analyse each of these possibilities.

(3.3.1) Let λ divides a. By (57), we have that $u < 2a\cdot c_1^2$. Note that λ is an integer number. Then (56) implies that q^2-1 must divide $3u^2+2c_1u$, where $u < 2a\cdot c_1^2$. Thus $q^2-1 \leqslant 3u^2+2c_1u \leqslant 12a^2\cdot c_1^4 + 4a\cdot c_1^3$, and so $q^2 < 16a^2\cdot c_1^4$, where $c_1 = \gcd(3, q+1)$, and this holds only for the pairs $(p, a) \in \{(3, 1), (5, 1)\}$, and so λ divides $a = 1$, which is impossible.

(3.3.2) Let λ divides p. Since $\lambda > 1$, we have that $\lambda = p$, and so by (57), we have that $u < 2p \cdot c_1^2$. As λ is a positive integer, it follows from (56) that $q^2 - 1$ divides $3u^2 + 2c_1 u$, where $u < 2p \cdot c_1^2$. Thus $q^2 - 1 \leqslant 3u^2 + 2c_1 u \leqslant 12p^2 \cdot c_1^4 + 4p \cdot c_1^3$, and so $q^2 < 16p^2 \cdot c_1^4$, where $c_1 = \gcd(3, q + 1)$. Thus either $(p, a) = (3, 2)$, or $a = 1$. If $(p, a) = (3, 2)$, then by (55), we have that $v = 3321$ and that k divides $\lambda \cdot c_1 f(p^2) = 3f(9) = 240$. Since $\lambda = 3$, we conclude that $3(v - 1) = k(k - 1)$, for some divisor k of 240, which is a contradiction. Thus $a = 1$, and so $q = p$. Since λ is an odd prime divisor of k, it follows from (56) that $q = p$ must divide $u + c_1$. Let now u_1 be a positive integer such that $u = u_1 p - c_1$. Then by (57), $u_1 p - c_1 < 2p \cdot c_1^2$, and since $p \geqslant 3 \geqslant c_1 = \gcd(3, p + 1)$, we have that $u_1 p < 2p \cdot c_1^2 + c_1 \leqslant 2p \cdot c_1^2 + p$, and so

$$u_1 < 2c_1^2 + 1. \tag{58}$$

If $c_1 = 1$, then $u_1 = 1$ or 2. Clearly, we have that $p^2 - 1 \nmid 3u_1^2 p^2 - 4u_1 p + 1$. If $c_1 = 3$, then $u_1 = 1, 2, \ldots, 18$. For each value of u_1, by Euclid's algorithm, it is easy to know that $p^2 - 1 \nmid 3u_1^2 p^2 - 12u_1 p + 9$ except for the case where

$$(p, u_1) \in \{(5, 1), (5, 3), (5, 5), (11, 1), (11, 3), (17, 1)\}.$$

Note here that $p = q = \lambda$. Then for each such pair by (55), we can obtain v, and this is a contradiction as for each v and p, the equation $p(v - 1) = k(k - 1)$ has no positive integer solutions.

(3.3.3) Let λ divides $(q - \epsilon 1)/2$, where $\epsilon \in \{+, -\}$. Then $\gcd(\lambda, p) = 1$. On the other hand by Lemma 10, we know that $\gcd(v - 1, p) = 1$, and so Lemma 8(a) implies that $\gcd(k, p) = 1$. It follows from Lemmas 7 and 8(a) that k divides $|\mathrm{Out}(X)| \cdot |H \cap X|_{p'} = 4a(q^2 - 1)^2$. Then (56) implies that

$$u \cdot (q^2 + 2) + 2c_1 \text{ divides } 8a \cdot c_1(q^2 - 1)^2. \tag{59}$$

Note that $8ac_1 u \cdot (q^2 - 1)^2 = 8ac_1 h(q)[u \cdot (q^2 + 2) + 2c_1] + G(u, q)$, where $h(q) = q^2 - 4$ and $G(u, q) = 8ac_1[9u - 2c_1 h(q)]$. Then $G(u, q) = 0$ or we conclude by (59) that

$$u \cdot (q^2 + 2) + 2 \cdot c_1 \text{ divides } |G(u, q)|. \tag{60}$$

Suppose that $G(u, q) = 0$. Then $9u = 2c_1 h(q)$. Then $u = 2c_1 h(q)/9 = 2c_1(q^2 - 4)/9$. Then (56) implies that $\lambda = 2(q^2 - 1)(q^2 - 4)/81$, which is impossible.

Suppose now that $G(u, q) > 0$. Then $u > 2(q^2 - 4)/9$ and by (60), $u \cdot (q^2 + 2) + 2 \cdot c_1 < |G(u, q)| = 72ac_1 u - 16ac_1^2 h(q) \leqslant 72ac_1 u$, and so $q^2 + 2 < 72ac_1$. Since $r(q) = 9$, it follows that $q^2 + 2 < 72a \cdot c_1$. This inequality holds when $q = 3, 5, 7, 9, 11$. Note by (57) that $u < c_1^2(q + 1)$ as λ divides $(q - \epsilon 1)/2$. Thus for $q \in \{3, 5, 7, 9, 11\}$, as $2(q^2 - 4)/9 < u < c_1^2(q + 1)$, we have that $(q, u) \in \{(3, 2), (3, 3), (5, 5), (5, 6), \ldots, (5, 17), (11, 27), (11, 28), \ldots, (11, 35)\}$. We can now check (56) for these pairs (q, u), and observe that for no such pairs, λ is prime.

Suppose finally that $G(u, q) < 0$. Then (60) implies that $u \cdot (q^2 + 2) + 2c_1 < |G(u, q)| = 16ac_1^2 h(q) - 72ac_1 u < 16ac_1 h(q) = 16ac_1 \cdot (q^2 - 4)$, and so $u < 16ac_1$. Note by (56) that

Table 3: Some parameters for Case 3.3.3 in Proposition 20

p	3	5	7	11, 13, …89
$a \leqslant$	4	3	2	1
$u <$	82	378	50	270

q^2-1 divides $3u^2+2c_1u$. Then $q^2-1 \leqslant 3u^2+2c_1u < 3\cdot 16^2a^2c_1^2 + 2\cdot 16ac_1^2$, and so $q^2-1 < 2^{10}a^2c_1^2$, and this holds only for $q=p^a$ as in Table 3. For each q, we can find an upper bound for u listed in the same table, and it is easy to check by (56) that these possible pairs (q,u) give rise to no possible parameters with λ prime.

(4) Let $H = N_G(X(q_0))$ with $q=q_0^t$ odd and t odd prime. Then by [23, Proposition 4.5.4], the subgroup H_0 is isomorphic to $\mathrm{PSp}_{2m}(q_0)$ with $q=q_0^t$. As $|\mathrm{Out}(X)|$ divides $2a$, by Lemma 15 and Corollary 12, we have that $q_0^{tm(2m-1)} < 16a^2\cdot q_0^{3m(2m+1)}$. Since $a^2<2q$, it follows that

$$q_0^{t(2m^2-m-1)} < 32\cdot q_0^{6m^2+3m}. \tag{61}$$

As q_0 is odd, $q_0^{t(2m^2-m-1)} < q_0^{6m^2+3m+4}$. Thus $t(2m^2-m-1) < 6m^2+3m+4$. If $t \geqslant 9$, then $9(2m^2-m-1) \leqslant t(2m^2-m-1) < 6m^2+3m+4$, and so $12m^2 < 12m+13$, which is impossible. Therefore, $t=3,5,7$. If $t=7$, then by (61), we have that $q_0^{8m^2-10m-7} < 32$. As $m \geqslant 2$ and q_0 is odd, $3^5 \leqslant q_0^{8m^2-10m-7} < 32$, and so $3^5<32$, which is impossible. If $t=5$, then (61) implies that $q_0^{4m^2-8m-5} < 32$, and this inequality holds only for $m=2$. If $(m,t)=(2,5)$, then by (1), we have that

$$v = \frac{q_0^{16}(q_0^{20}-1)(q_0^{10}-1)}{(q_0^4-1)(q_0^2-1)} > q_0^{35}.$$

By Lemmas 7 and 8(b), the parameter k divides $2a\cdot q_0^4(q_0^4-1)(q_0^2-1)$. It follows from Lemmas 8 and 10 that k divides $2\lambda a\cdot(q_0^4-1)(q_0^2-1)$. Then by Lemma 8(b), we conclude that $\lambda q_0^{35} < \lambda v < k^2 \leqslant 4\lambda^2a^2\cdot(q_0^4-1)^2(q_0^2-1)^2 < 4\lambda^2a^2\cdot q_0^{12}$. Hence, $q_0^{23} < 4\lambda a^2$. Since k divides $2a\cdot q_0^4(q_0^4-1)(q_0^2-1)$ and λ is an odd prime divisor of k, we conclude that $\lambda \leqslant q_0^2+1$. Then the inequality $q_0^{23} < 4a^2\lambda$ implies that $q_0^{21} < 8a^2$, and since $a=ts=5s$, it follows that $q_0^{21} < 200\cdot s^2$, which is impossible. Hence $t=3$. In this case by (1) and Lemma 15, we have that $v > q_0^{4m^2-4m-2}$. It follows from Lemmas 7 and 8 and Tits' Lemma 10 that k divides $2a\lambda\cdot g(q_0)$, where $g(q_0)=(q_0^{2m}-1)\cdots(q_0^2-1)$. By Lemma 8(b), we conclude that $\lambda q_0^{4m^2-4m-2} < \lambda v < k^2 \leqslant 4\lambda^2a^2\cdot(q_0^{2m}-1)^2\cdots(q_0^2-1)^2$. Thus

$$q_0^{2m^2-6m-2} < 4a^2\lambda. \tag{62}$$

Note that λ is an odd prime divisor of k and k divides $|H|$. Then λ must divide a, p or $(q_0^{2j}-1)$, for some $j \in \{1,\ldots,m\}$, and so

$$\lambda \leqslant q_0^m+1. \tag{63}$$

Therefore, by the inequality (62), we have that $q_0^{2m^2-6m-2} < 4a^2 \cdot (q_0^m + 1)$. As $a = ts = 3s$ and $q_0^m + 1 < 2q_0^m$, we conclude that $q_0^{2m^2-7m-2} < 72s^2$ implying that $m = 2, 3, 4$. If $m = 2$, then by (1), we have that $v = q_0^8(q_0^8 + q_0^4 + 1)(q_0^4 + q_0^2 + 1) > q_0^{20}$. Here by Lemma 8(a)-(c), k divides $2\lambda a \cdot \gcd(v-1, |H \cap X|)$. Then by Lemma 10 and the fact that $\gcd(v-1, q_0^2+1) = 2$, we conclude that $k \leqslant 4\lambda a \cdot (q_0^2 - 1)^2$. So Lemma 8(b) implies that $\lambda q_0^{20} < \lambda v < k^2 \leqslant 16\lambda^2 a^2 (q_0^2-1)^4$. Thus, $q_0^{12} < 16\lambda a^2$. So by (63), we have that $q_0^{12} < 16a^2 \cdot (q_0^2 + 1)$. Recall that $a = 3s$ and $q_0^2 + 1 < 2q_0^2$. Then $q_0^{12} < 2^5 \cdot 3^2 \cdot s^2$, which is impossible. By the same manner as above, the remaining cases where $m = 3, 4$ can be ruled out. $\square$

Proposition 21. *Let $\mathcal{D}$ be a nontrivial symmetric (v, k, λ) design with λ prime. Suppose that G is an automorphism group of $\mathcal{D}$ of almost simple type with socle X. If G is flag-transitive and point-primitive, then the socle X cannot be $\mathrm{P\Omega}_n^{\epsilon}(q)$ with $\epsilon \in \{\circ, -, +\}$.*

Proof. Let $H_0 = H \cap X$, where $H = G_\alpha$ with α a point of $\mathcal{D}$. Note by Lemma 8(a) that v is odd, and so by Lemma 14, we have one of the following possibilities:

(1) q is even, and H_0 is a parabolic subgroup of X;

(2) q is odd, and H is the stabilizer of a nonsingular subspace;

(3) q is odd, and H_0 is the stabilizer of an orthogonal decomposition $V = \oplus V_j$ with all V_j's isometric;

(4) H_0 is $\mathrm{SO}_7(2)$ or $\Omega_8^+(2)$ and X is $\Omega_7(q)$ or $\mathrm{P\Omega}_8^+(q)$, respectively, $q = p \equiv \pm 3 \pmod 8$;

(5) $X = \mathrm{P\Omega}_8^+(q)$, $q = p \equiv \pm 3 \pmod 8$, G contains a triality automorphism of X and H_0 is $2^3 \cdot 2^6 \cdot \mathrm{PSL}_3(2)$;

(6) $q = q_0^t$ is odd with t odd prime, and $H = N_G(X(q_0))$.

Note in the cases (1) and (6) for $X = \Omega_{2m+1}(q)$ that we argue exactly the same as in the symplectic groups. Therefore, we exclude these possibilities, and analyse the remaining cases.

(1) Let H_0 be a parabolic subgroup of X, and let q be even. As noted above, we only need to consider the case where $X = \mathrm{P\Omega}_{2m}^{\epsilon}(q)$ with $(m, \epsilon) \neq (2, +)$, $\epsilon = \pm$ and q even. We postpone the case where $(m, \epsilon) = (4, +)$ and G contains a triality automorphism till the end of this case. In this case by [23, Proposition 4.1.20], H_0 is isomorphic to $[q^h] \cdot \mathrm{GL}_i(q) \times \Omega_{2m-2i}^{\epsilon}(q)$, where $h = 2mi - (3i^2 + i)/2$.

Suppose first that H stabilises a totally singular i-space with $i \leqslant m-1$, and so $H = P_i$ excluding the case where $i = m-1$ and $\epsilon = +$, where $H = P_{m,m-1}$. It follows from (1) and Lemma 15 that $v > 2^{-5} q^{(4mi-3i^2-i-2)/2}$. Note that λ is an odd prime divisor of k and $|\mathrm{Out}(X)|$ divides $6a$. Then by Lemma 8(b), we have that

$$\lambda \leqslant q^{m-1} + 1. \tag{64}$$

In all cases, by Lemma 11 there is a unique subdegree d of X that is a power of p except for the case where $\epsilon = +$, m is odd and $H = P_m$ or P_{m-1}. Note that the p-part $(v-1)_p$ of $v-1$ is q^2 or 8. Since k divides $\lambda \gcd(v-1,d)$, it follows that k divides λq^3. It follows from Lemma 8(b) that $\lambda q^{(4mi-3i^2-i-2)/2} < 32\lambda v < 32k^2 \leqslant 32\lambda^2 q^6$. Therefore, $q^{(4mi-3i^2-i-2)/2} < 32\lambda q^6$, an so by (64), we have that

$$q^{(4mi-3i^2-i-2)/2} < 32q^6(q^{m-1}+1). \tag{65}$$

Then $q^{(4mi-3i^2-i-2)/2} < 2^5 \cdot q^6(q^{m-1}+1)$. Since $q^{m-1}+1 < 2q^{m-1}$, it follows that $q^{2m(2i-1)-3i^2-i-12} < 2^{12}$. Since also $m \geqslant i+1$, it follows that $2(i+1)(2i-1) \leqslant 2m(2i-1) < 3i^2+i+24$, and so $i^2+i < 26$, then $i \in \{1,2,3,4\}$. If $i=1$, then $2m = 2m(2i-1) < 3i^2+i+24 = 28$, and so $m = 4,\dots,13$. By (1), we have that $v = (q^m - \epsilon 1)(q^{m-1}+\epsilon 1)/(q-1)$. Recall that there is a unique subdegree d of X that is a power of p. Since k divide $\lambda \gcd(v-1,d)$, it follows that k divides λq. Thus Lemma 8(b) that $\lambda(q^{m-1}+\epsilon 1)(q^m-\epsilon 1)/(q-1) \leqslant \lambda v < k^2 \leqslant \lambda^2 q^2$, and so $(q^{m-1}+\epsilon 1)(q^m - \epsilon 1) < \lambda q^2(q-1)$. Then by (64), we have that $(q^m - \epsilon 1)(q^{m-1}+\epsilon 1) < q^2(q-1)(q^{m-1}+1)$. If $\epsilon = +$, then $(q^{m-1}+1)(q^m-1) < q^2(q-1)(q^{m-1}+1)$, and so $(q^m-1) < q^2(q-1)$, which does not hold for any $m \geqslant 4$, which is a contradiction. If $\epsilon = -$, then $(q^{m-1}-1)(q^m+1) < q^2(q-1)(q^{m-1}+1)$, and so $q^{2m-1} - q^m + q^{m-1} - 1 < q^{m+2} - q^{m+1} + q^3 - q^2$, and so $q^{2m-3} - q^{m-2} + q^{m-3} \leqslant q^m - q^{m-1} + q - 1$. Since $q^{m-3} > q-1$, $q^{m-2}(q^{m-1}-1) \leqslant q^{m-2}(q^2-q)$, and so $(q^{m-1}-1) \leqslant (q^2-q)$, which is impossible. For the remaining cases $i = 2,3,4$, we argue exactly as in the case where $i=1$.

Suppose finally that $H = P_m$ when $X = \mathrm{P}\Omega^+_{2m}(q)$. Note that here P_{m-1} and P_m are the stabilizers of totally singular m-spaces from the two different X-orbits. Here by (1), we have that

$$v = (q^{m-1}+1)(q^{m-2}+1)\cdots(q+1) > q^{m(m-1)/2}. \tag{66}$$

Note that λ is an odd prime divisor of k and $|\mathrm{Out}(X)|$ divides $6a$. Then by Lemma 8(b), λ must divide 3, a or q^j-1, for some $j \in \{1,\dots,m\}$. Thus

$$\lambda \leqslant (q^m-1)/(q-1). \tag{67}$$

Assume that m is even. Note by [35, p. 332] that there is a subdegree d which is a power of p. On the other hand, the p-part of $v-1$ is q. Since k divides $\lambda \gcd(v-1,d)$, we have that k divides λq, and so Lemma 8(b) implies that $\lambda q^{m(m-1)/2} < \lambda v < k^2 < \lambda^2 q^2$, and so $q^{m(m-1)/2} < \lambda q^2$. Thus by (67), we conclude that $q^{m(m-1)/2}(q-1) < (q^m-1)q^2$, and so $m(m-1) < 2m+4$, which is impossible for $m \geqslant 4$.

Assume that m is odd. Then [35, p. 332] implies that k divides $\lambda q(q^m-1)$, and so by Lemma 8(b), we have that $\lambda q^{m(m-1)/2} < \lambda v < k^2 < \lambda^2 q^2 (q^m-1)^2$. Thus $q^{m(m-1)/2} < \lambda q^2(q^m-1)^2$. Then (67) implies that $q^{m(m-1)/2}(q-1) < q^2(q^m-1)^3$, and so $m(m-1) < 6m+4$, then $m = 5,7$. If $m=5$, then action here is of rank three. The symmetric designs with a primitive rank 3 automorphism group have been classified by Dempwolff [16], we know that there is no such symmetric design with λ prime. If $m=7$, then since

k divides $\lambda q(q^7-1)$ and $\gcd(v-1, q^6+q^5+q^4+q^3+q^2+q+1)=1$, the parameter k must divide $\lambda q(q-1)$. It follows from Lemma 8(b), that $\lambda q^{21} < \lambda v < k^2 < \lambda^2 q^2(q-1)^2$, and so $q^{21} < \lambda q^2(q-1)^2$. Thus by (67), we conclude that $q^{21} < q^2(q-1)^2(q^7-1)$, which is impossible.

Let now $X = \mathrm{P}\Omega_8^+(q)$, and let G contain a triality automorphism. We use [12, Table 8.50], where the maximal subgroups are determined. By case (1), we only need to consider the case where $H \cap X$ is isomorphic to $[q^{11}]{:}(q-1)^2 \cdot \mathrm{GL}_2(q)$. By (1), we have that $v = (q^6-1)(q^4-1)^2/(q-1)^3 > q^{11}$. Since the p-part of $v-1$ is q and k divides $\lambda \gcd(v-1, d)$, it follows that k divides λq. Then Lemma 8(b) implies that $\lambda q^{11} < \lambda v < k^2 < \lambda^2 q^2$, and so $q^{11} < \lambda q^2$. Note that λ is and odd prime divisor of k dividing $|\mathrm{Out}(X)| \cdot |H \cap X|$. Then Note that λ is an odd prime divisor of k and $|\mathrm{Out}(X)|$ divides $6a$. Then λ must divide 3, a or q^j-1, for some $j \in \{1, 2\}$, and so $\lambda \leqslant \max\{3, q+1\} \leqslant q+1$. Recall that $q^{11} < \lambda q^2$. Therefore, $q^{11} < q^2(q+1)$, which is a impossible.

(2) Let H be the stabilizer of a nonsingular subspace, and let q be odd. Here, we need to discuss the odd and even dimension of the underlying orthogonal space separately.

(2.1) Let $X = \Omega_{2m+1}(q)$ with q odd and $m \geqslant 3$. In this case $H = N_i^{\epsilon}$ with $i \leqslant m$. If $i = 1$, then by [23, Proposition 4.1.6], H_0 is isomorphic to $\hat{}\Omega_{2m}^{\epsilon}(q){\cdot}2$ with $\epsilon \in \{+, -\}$. It follows from (1) that $v = q^m(q^m+\epsilon 1)/2$. Note here that if $\epsilon = -$, then m is odd as v must be odd.

According to [35, p.331-332], k must divide $\lambda d^{\epsilon}(q)$, where $d^{\epsilon}(q) = (q^m - \epsilon 1)/2$. Let u be a positive integer such that $uk = \lambda(q^m - \epsilon 1)/2$. Then by Lemma 8(a), we have that

$$k = u \cdot (q^m + \epsilon 2) + 1 \quad \text{and} \quad \lambda = 2u^2 + \frac{\epsilon 3u^2 + u}{d^{\epsilon}(q)}. \tag{68}$$

Since $uk = \lambda d^{\epsilon}(q) = \lambda(q^m - \epsilon 1)/2$, it follows from Lemma 8(b) that $\lambda v < k^2 \leqslant \lambda^2 d^{\epsilon}(q)^2/u^2$. Therefore,

$$2u^2 q^m(q^m + \epsilon 1) < \lambda(q^m - \epsilon 1)^2. \tag{69}$$

Note that here $|\mathrm{Out}(X)| = 2a$ and λ is an odd prime divisor of k. Then by Lemmas 7 and 8(b), λ must divide a, p, $q^m - \epsilon 1$ or $q^{2j}-1$, for some $j \in \{1, \ldots, m-1\}$. Considering all these possible cases, it is easy to see that $\lambda \leqslant (q^m - \epsilon 1)/(q - \epsilon 1)$. So by (69), we have that $2u^2 q^m(q^m + \epsilon 1) < \lambda(q^m - \epsilon 1)^2/(q - \epsilon 1) \leqslant (q^m - \epsilon 1)^3/(q - \epsilon 1)$. Therefore,

$$u^2 < \frac{(q^m - \epsilon 1)^3}{2q^m(q^m + \epsilon 1)(q - \epsilon 1)}. \tag{70}$$

Note that λ is an integer number. Then (68) implies that $d^{\epsilon}(q)$ must divide $|\epsilon 3u^2 + u|$, where $d^{\epsilon}(q) = (q^m - \epsilon 1)/2$.

Let now $\epsilon = +$. Then, by (70), we conclude that

$$\frac{q^m - 1}{2} = d^{+}(q) \leqslant 3u^2 + u \leqslant 4u^2 < \frac{2(q^m-1)^3}{q^m(q^m+1)(q-1)},$$

and so $q^m(q^m+1)(q-1) < 4(q^m-1)^2$. Therefore, $(q-1) < 4(q^m-1)^2/[q^m(q^m+1)] < 4$, and hence $q = 3$. In this case, G has rank 3 by [22, Theorem 1.1], and by [16], we know that there is no such symmetric design with λ prime.

Let now $\epsilon = -$. Then (70) yields

$$\frac{q^m+1}{2} = d^-(q) \leqslant 3u^2 - u < 3u^2 < \frac{3(q^m+1)^3}{2q^m(q^m-1)(q+1)},$$

and so $q^m(q^m-1)(q+1) < 3(q^m+1)^2$. Since $q \geqslant 3$, it follows that $4q^m(q^m-1) < 3(q^m+1)^2$, and so $q^{2m} < 10q^m + 3$, which is impossible as $m \geqslant 3$.

Therefore, $i \geqslant 2$. Here by [23, Proposition 4.1.6], $H \cap X$ is isomorphic to $\Omega_i^\epsilon(q) \times \Omega_{n-i}(q){\cdot}4$, where i is even and $\epsilon \in \{+,-\}$. It follows from [35, p.331], we have that $v > q^{i(n-i)}/4$ and $k \leqslant 2a\lambda q^m$, where $n = 2m+1$ and $m \geqslant 3$. Then by Lemma 8(b), we have that

$$q^{i(n-i)} < 16\lambda a^2 q^{n-1}. \tag{71}$$

Since λ is an odd prime divisor of k, Lemmas 7 and 8 imply that λ must divide a, p, $q^{j_1} - \epsilon$ or $q^{2j_2} - 1$, where $j_1 \leqslant \lfloor m/2 \rfloor$ and $j_2 \leqslant \lfloor (n-i-1)/2 \rfloor$. Note that $m > i$. Thus $\lambda \leqslant (q^{(n-i-1)/2} + 1)/2$, and so (71) implies that $q^{i(n-i)} < 16a^2 q^{(3n-i-3)/2}$. Therefore,

$$q^{n(2i-3)-2i^2+i+3} \leqslant 256a^4. \tag{72}$$

As $m > i$, we have that $n > 2i$, and so $q^{2i^2-5i+3} \leqslant 256a^4$. This inequality holds only for $i = 2$, in which case (72) implies that $q^{n-3} = q^{n(2i-3)-2i^2+i+3} \leqslant 256a^4$. This inequality holds only for $(n, q) = (7, 3)$, in which case by [12, Tables 8.39], $H \cap X$ is isomorphic to $\Omega_2^-(3) \times \Omega_5(3) \cdot 4$, and so (1) implies that $v = 22113$. By Lemmas 7 and 8, k is a divisor of 415720. For these values of (v, k), the fraction $k(k-1)/(v-1)$ is not prime, which is a contradiction.

(2.2) Let $X = \mathrm{P}\Omega_{2m}^\epsilon(q)$ with q odd, $m \geqslant 4$ and $\epsilon \in \{-,+\}$. Then $H = N_i$ with $i \leqslant m$. Set $n = 2m$.

If $i = 1$, then by [23, Proposition 4.1.6], $H \cap X$ is isomorphic to $\hat{}\Omega_{2m-1}(q){\cdot}4$. Here by (1), we have that $v = q^{m-1}(q^m - \epsilon 1)/2$. Note that $|\mathrm{Out}(X)|$ divides $6a{\cdot}\gcd(4, q^m-1)$ and λ is an odd prime divisor of k. Then by Lemmas 7 and 8(b), λ must divide a, 3, p or $q^{2j} - 1$, for some $j \in \{1, 2, \ldots, m-1\}$. Therefore,

$$\lambda \leqslant (q^{m-1} + 1)/2. \tag{73}$$

According to [35, p.332-333], the parameter k divides $\lambda(q^{m-1} + \epsilon 1)/2$ if $q \equiv 1 \pmod 4$, or $\lambda(q^{m-1} - \epsilon 1)/2$ if $q \equiv 3 \pmod 3$. Thus k divides $\lambda d^\epsilon(q)$, where $d^\epsilon(q) = (q^{m-1} \pm \epsilon 1)/2$. By Lemma 8(a), k divides $\lambda(v-1)$. Therefore, k must divide $\lambda \gcd(v-1, d^\epsilon(q))$. Note that $\gcd(v-1, d^\epsilon(q)) < q-1$. Therefore, $k < \lambda(q-1)$. Then by (73) and Lemma 8(b), we have that $\lambda q^{m-1}(q^m - \epsilon 1) \leqslant \lambda v < k^2 < \lambda^2(q-1)^2$, and so (73) implies that $q^{m-1}(q^m - \epsilon 1) < (q^{m-1} + 1)(q-1)^2$, which is impossible.

Table 4: Some large maximal subgroups of finite simple classical groups in Proposition 21.

X	$H \cap X$	v	k divides
$\mathrm{P}\Omega_8^-(3)$	$\hat{}(\Omega_2^-(3) \times \Omega_6^+(3)){\cdot}2^2$	209223	388177920
$\mathrm{P}\Omega_8^-(5)$	$\hat{}(\Omega_2^-(5) \times \Omega_6^+(5)){\cdot}2^2$	102703125	1392768000000
$\mathrm{P}\Omega_8^-(7)$	$\hat{}(\Omega_2^-(7) \times \Omega_6^+(7)){\cdot}2^2$	6075747307	296651671142400
$\mathrm{P}\Omega_8^-(9)$	$\hat{}(\Omega_2^-(9) \times \Omega_6^+(9)){\cdot}2^2$	127287028233	32486299582464000
$\mathrm{P}\Omega_{10}^-(3)$	$\hat{}(\Omega_2^-(3) \times \Omega_8^+(3)){\cdot}2^2$	16409061	158469754060800
$\mathrm{P}\Omega_{10}^+(3)$	$\hat{}(\Omega_2^+(3) \times \Omega_8^+(3)){\cdot}2^2$	32549121	158469754060800

Therefore, we can assume that $1 < i \leqslant m$. Then by [2, p.19], $v > q^{i(2m-i)}/4$ and by [35, p. 333], $k \leqslant 4a\lambda{\cdot}q^m$. Then Lemma 8(b) implies that $\lambda v < \lambda q^{i(2m-i)} < 4k^2 < 64\lambda^2 a^2 q^{2m}$. Thus

$$q^{2m(i-1)-i^2} < 64\lambda a^2. \tag{74}$$

Note that λ is an odd prime divisor of k and by Lemma 8(b), k divides $|\mathrm{Out}(X)|{\cdot}|H \cap X|$, where $|\mathrm{Out}(X)|$ divides $6a{\cdot}\gcd(q^m - \epsilon 1)$. Here by [23, Proposition 4.1.6], $H \cap X$ divides $|\Omega_i^{\delta_1}(q) \times \Omega_{n-i}^{\delta_2}(q){\cdot}4|$, where $\delta_i \in \{\circ, -, +\}$ and $i \geqslant 2$. Then $\lambda \leqslant \lambda_i(q)$, where $n = 2m$ and

$$\lambda_i(q) = \begin{cases} 2^{-1}{\cdot}(q^{(n-i)/2}+1), & \text{if } (n-i)/2 \text{ is even and } \delta_2 = -; \\ 2^{-1}{\cdot}(q^{(n-i-1)/2}+1), & \text{if } i \text{ is odd;} \\ (q^{(n-i)/2} - (-1)^{\delta_2})(q - (-1)^{\delta_2})^{-1}, & \text{otherwise.} \end{cases} \tag{75}$$

Thus by (74) and (75), we have that $q^{2m(i-1)-i^2} < 32a^2{\cdot}(q^{(n-i)/2}+1)$. Since $q^{(n-i)/2}+1 < 2q^{(n-i)/2}$, it follows that

$$q^{m(2i-3)-i^2} < 64a^2. \tag{76}$$

Note that $i \leqslant m$. Thus $q^{i^2-3i} \leqslant q^{m(2i-3)-i^2} < 64a^2$, and so $q^{i^2-3i} < 64a^2$. This inequality holds only for $i = 2, 3$. If $i = 3$, then by (74) and (75), we have that $q^{4m-9} < 32a^2{\cdot}(q^{m-2}+1)$. Hence $q^{3m-7} < 64a^2$. As $m \geqslant 4$, it follows that $q^5 \leqslant q^{3m-7} < 64a^2$, and so $q^5 < 64a^2$, which is impossible. Therefore, $i = 2$. We now consider the following two subcases:

(2.2.1) Let m be even. If $\delta_2 = -$, then by (74) and (75), we have that $q^{2m-4}{\cdot}(q+1) < 32a^2{\cdot}(q^{m-1}+1)$. Hence $q^{m-3}{\cdot}(q+1) < 64a^2$. This inequality holds only for $(m, q) = (4, 3)$ in which case $v = 189540$, which is not odd. If $\delta_2 = +$, then by (74) and (75), we have that $q^{2m-4}{\cdot}(q-1) < 32a^2{\cdot}(q^{m-1}-1)$. Hence $q^{m-3}{\cdot}(q-1) < 32a^2$. This inequality holds only for $(m, q) \in \{(4, 3), (4, 5), (4, 7), (4, 9)\}$. We now apply [23, Proposition 4.1.6] and obtain $H \cap X$ as listed in Table 4, and considering the fact that v is odd, we have that $(m, q, \epsilon) \in \{(4, 3, -), (4, 5, -), (4, 7, -), (4, 9, -)\}$. Moreover, Lemma 8(b) says that k divides $|\mathrm{Out}(X)|{\cdot}|H \cap X|$, and so we can find the possible values of k as in the fourth column of Table 4. This is a contradiction as for each k and v as in Table 4, the fraction $k(k-1)/(v-1)$ is not prime.

Table 5: Some parameters for Case 3 in Proposition 21

Line	X	$H \cap X$	v	k divides
1	$\Omega_7(3)$	$2^6{\cdot}\mathrm{Alt}_7$	28431	645120
2	$\Omega_7(5)$	$2^6{\cdot}\mathrm{Alt}_7$	1416796875	645120
3	$\Omega_9(3)$	$2^8{\cdot}\mathrm{Alt}_9$	1416290265	185794560
4	$\Omega_{11}(3)$	$2^{10}{\cdot}\mathrm{Alt}_{11}$	3741072100580529	81749606400
5	$\Omega_{13}(3)$	$2^{12}{\cdot}\mathrm{Alt}_{13}$	564416277323644023433155	51011754393600
6	$\mathrm{P}\Omega_8^+(3)$	$2^6{\cdot}\mathrm{Alt}_8$	3838185	15482880
7	$\mathrm{P}\Omega_8^+(5)$	$2^6{\cdot}\mathrm{Alt}_8$	6906884765625	15482880
8	$\mathrm{P}\Omega_{12}^+(3)$	$2^{10}{\cdot}\mathrm{Alt}_{12}$	27575442453379079259	2942985830400
9	$\mathrm{P}\Omega_{10}^-(3)$	$2^8{\cdot}\mathrm{Alt}_{10}$	1399578039873	3715891200
6	$\mathrm{P}\Omega_{14}^-(3)$	$2^{12}{\cdot}\mathrm{Alt}_{14}$	32152618284915465959467883895	1428329123020800

(2.2.2) Let m be odd. If $\delta_2 = -$, then by (74) and (75), we have that $q^{2m-4} < 32a^2{\cdot}(q^{m-1}+1)$. Hence $q^{m-3} < 64a^2$. This inequality holds only for $m = 5$ and $q = 3, 5, 7, 9$. All these cases can be ruled out as v has to be odd. If $\delta_2 = +$, then by (75) and (74), we have that $q^{2m-4}{\cdot}(q-1) < 32a^2{\cdot}(q^{m-1}-1)$. Hence $q^{m-3}{\cdot}(q-1) < 32a^2$. This inequality holds only for $(m, q) = (5, 3)$ for $\epsilon = \pm$. By [23, Proposition 4.1.6], we can obtain $H \cap X$ as in Table 4, and for each such $H \cap X$, by (1), we find v as in the third column of Table 4. Note by Lemma 8(b) that k divides $|\mathrm{Out}(X)|{\cdot}|H \cap X|$, and so we can find the possible values of k as in the fourth column of Table 4. All these cases can be ruled out as the fraction $k(k-1)/(v-1)$ is not prime.

(3) Let H_0 be the stabilizer of an orthogonal decomposition $V = \oplus V_j$ with all V_j's isometric, and let q be odd. This case has to be treated separately for both odd and even dimension of V.

(3.1) Let $X = \Omega_{2m+1}(q)$ with q odd and $m \geqslant 3$. In this case H is the stabilizer of a subspace decomposition into isometric non-singular spaces of dimension i, where i is odd.

Let $i = 1$. Then by [23, Proposition 4.2.15], the subgroup $H \cap X$ is isomorphic to $2^{2m}{\cdot}\mathrm{Sym}_{2m+1}$ or $2^{2m}{\cdot}\mathrm{Alt}_{2m+1}$ if $q \equiv \pm 1 \pmod 8$ or $q \equiv \pm 3 \pmod 8$, respectively. The subgroups $H \cap X$ satisfying $|X| < |\mathrm{Out}(X)|^2{\cdot}|H \cap X|^3$ are listed in Table 5, and for each such $H \cap X$, by (1), we obtain the parameter v as in the fourth column of Table 5. Moreover, Lemma 8(b) says that k divides $|\mathrm{Out}(X)| \cdot |H \cap X|$, and so we can find the possible values of k as in the fifth column of Table 5. For each possible case, we observe that $k(k-1)/(v-1)$ is not prime, which is a contradiction.

Therefore, $i \geqslant 3$, and hence [23, Proposition 4.2.14] implies that $H \cap X$ is isomorphic to

$$(2^{t-1} \times \Omega_i(q)^t{\cdot}2^{t-1}){\cdot}\mathrm{Sym}_t,$$

where $it = 2m + 1$.

Let $i = 3$. Then $H \cap X$ is isomorphic to $(2^{t-1} \times \Omega_3(q)^t \cdot 2^{t-1}) \cdot \mathrm{Sym}_t$, and so by Lemma 15, we conclude that $q^{m^2} \prod_{j=1}^{m}(q^{2j}-1) < a^2 \cdot 2^3 \cdot 2^{6t-6} \cdot (t!)^3 \cdot q^{3t}(q^2-1)^{3t}/2^{-3t}$.

Since $a^2 < q$ and $q^{m^2} \leqslant \prod_{j=1}^{m}(q^{2j}-1)$, it follows that $q^{2m^2} < 2^{3t-3}\cdot(t!)^3\cdot q^{9t+1}$. Thus $q^{2m^2-9t-1} < 2^{3t-3}\cdot(t!)^3$. Since $2m+1=3t$, we conclude that

$$q^{9t^2-24t-1} < 2^{6t-6}\cdot(t!)^6. \tag{77}$$

If $t=3$, then $q^8 < 2^{18}\cdot 3^6$. This inequality holds for $q\in\{3,5,7,9\}$, and so in each case, we easily observe by (1) that v is even, which is a contradiction. Thus $t\geqslant 5$. Since by Lemma 16(a) we have that $t! < 5^{(t^2-3t+1)/3}$, it follows from (77) that $q^{9t^2-24t-1} < 2^{6t-6}\cdot(t!)^6 < 2^{6t-6}\cdot 5^{2t^2-6t+2}$. Thus $q^{9t^2-24t-1} < 2^{6t-6}\cdot 5^{2t^2-6t+2}$. Since $2^{6t-6}\cdot 5^{2t^2-6t+2} < 5^{2t^2}$, it follows that $q^{9t^2-24t-1} < 5^{2t^2}$. Then $\log_p q\cdot(9t^2-24t-1) < \log_p 5\cdot(2t^2) < 3t^2$, and so $9t^2-24t-1 < 3t^2$. Thus, $6t^2-24t-1<0$, this inequality does not hold for any $t\geqslant 5$, which is a contradiction.

Let $i\geqslant 5$. Then by Corollary 12 and Lemma 15, we have that $q^{m^2}\prod_{j=1}^{m}(q^{2j}-1) < a^2\cdot 2^3\cdot 2^{6t-6}\cdot(t!)^3\cdot q^{3it(i-1)/2}$. Since $a^2<q$ and $q^{m^2}\leqslant\prod_{j=1}^{m}(q^{2j}-1)$, it follows that $q^{2m^2} < 2^{6t-3}\cdot(t!)^3\cdot q^{[3it(i-1)+2]/2}$. Thus $q^{2m^2-[3it(i-1)+2]/2} < 2^{6t-3}\cdot(t!)^3$. Since $2m+1=it$, we conclude that

$$q^{(it-1)^2-3it(i-1)-2} < 2^{12t-6}\cdot(t!)^6. \tag{78}$$

If $t=3$, then $q^{3i-1} < 2^{36}\cdot 3^6$. Since $2^{36}\cdot 3^6 < 3^{29}$, it follows that $q^{3i-1} < 3^{29}$. This inequality holds only for $i\in\{5,7,9\}$. If $i=5$, then by (78), we conclude that $q^{14} < 2^{36}\cdot 3^6$. This inequality holds only for $q\in\{3,5,7,9\}$. Then by (1), we easily observe that v is not odd, which is a contradiction. By the same manner, we can rule out the remaining case where $i=7,9$. Therefore $t\geqslant 5$, and hence by Lemma 16(a), we have that $t! < 5^{(t^2-3t+1)/3}$, and so (78) implies that $q^{(it-1)^2-3it(i-1)-2} < 2^{12t-6}\cdot(t!)^6 < 2^{12t-6}\cdot 5^{2t^2-6t+2}$. Since $2^{12t-6}\cdot 5^{2t^2-6t+2} < 5^{2t^2}$, it follows that $q^{(it-1)^2-3it(i-1)-2} < 5^{2t^2-1}$. Then $[i^2t(t-3)+it-1]\cdot\log_p q < (2t^2-1)\cdot\log_p 5 < 3t^2$, and so

$$i^2t(t-3)+it-1 < 3t^2. \tag{79}$$

Note that $i\geqslant 5$. Then (79) implies that $25t^2-20t-1\leqslant i^2t(t-3)-5it-1<3t^2$, and so $23t^2-20t-1<0$, which is impossible.

(3.2) Let $X=\mathrm{P}\Omega_{2m}^{\epsilon}(q)$ with q odd, $m\geqslant 4$ and $\epsilon\in\{-,+\}$. In this case, H is an imprimitive subgroup of G stabilizing a decomposition $V=V_1\oplus\cdots\oplus V_t$ with the dimension of each V_j's equal to i, so $2m=it$.

(3.2.1) Let $i=1$. Then by Corollary 12 and [23, Proposition 4.2.15], we can obtain $H\cap X$ as listed in Table 5. For each such $H\cap X$, by (1), we can obtain v as in the third column of Table 5. Moreover, Lemma 8(b) says that k divides $|\mathrm{Out}(X)|\cdot|H\cap X|$, and so we can find the possible values of k as in the fourth column of Table 5. This is a contradiction as for each k and v as in Table 5, the fraction $k(k-1)/(v-1)$ is not prime. Hence $i\geqslant 2$.

(3.2.2) Let i be odd. Then by [23, Proposition 4.2.14], $H\cap X$ is isomorphic to $(2^{t-2}\times\Omega_i(q)^t.2^{t-1}).\mathrm{Sym}_t$ with t even and $\epsilon=(-1)^{m(q-1)/2}$.

If $i=3$, then $t\geqslant 4$ as $3t=it=2m\geqslant 8$. It follows from Corollary 12 and Lemma 15 that $q^{m(2m-1)} < |\mathrm{Out}(X)|^2\cdot 2^{6t-6}\cdot(t!)^3\cdot q^{3t}(q^2-1)^{3t}/2^{-3t}$. Since $|\mathrm{Out}(X)|$ divides $24a$

and $a^2 < q$, we conclude that $q^{2m^2-m} < 2^{3t} \cdot 3^2 \cdot (t!)^3 q^{9t+1}$. Thus $q^{2m^2-m-9t-4} < 2^{3t} \cdot (t!)^3$. Since $2m = 3t$, we have that

$$q^{9t^2-21t-8} < 2^{6t} \cdot (t!)^6. \tag{80}$$

Note by Lemma 16(b) that $t! < 2^{4t(t-3)/3}$. Thus (80) implies that $q^{9t^2-21t-8} < 2^{6t} \cdot (t!)^6 < 2^{6t} \cdot 2^{8t^2-24t}$, and so $q^{9t^2-21t-8} < 2^{8t^2-18t}$. Then $(9t^2-21t-8) \cdot \log_p q < (8t^2-18t) \cdot \log_p 2 < (8t^2-18t) \times 0.7$, and so $90t^2 - 210t - 80 < 56t^2 - 126t$. Therefore, $34t^2 - 84t - 80 < 0$, this inequality does not hold for any $t \geqslant 4$, which is a contradiction.

Therefore, $i \geqslant 5$. If $t = 2$, then $m = i$ as $2m = it$. Let u be a positive integer such that $i = 2u+1$. Then by (1), we have that

$$v = \frac{q^{3u^2+2u}(q^{2u+1} - \epsilon 1)(q^{4u}-1)(q^{4u-2}-1)\cdots(q^2-1)}{2(q^{2u}-1)^2(q^{2u-2}-1)^2\cdots(q^2-1)^2},$$

which is even, and this is a contradiction. If $t \geqslant 4$, then by Corollary 12 and Lemma 15, we have that $q^{m(2m-1)} < |\mathrm{Out}(X)|^2 \cdot 2^{6t-6} \cdot (t!)^3 \cdot q^{3it(i-1)/2}$. Thus, $q^{4m^2-2m} < |\mathrm{Out}(X)|^4 \cdot 2^{12t-12} \cdot (t!)^6 \cdot q^{3it(i-1)}$. Note that $|\mathrm{Out}(X)|$ divides $24a$ and $a^2 < q$. Thus, $q^{4m^2-2m} < 2^{12t} \cdot 3^4 \cdot (t!)^6 q^{3it(i-1)+2}$. Since $2m = it$, we conclude that

$$q^{i^2t^2-it-3it(i-1)-6} < 2^{12t} \cdot (t!)^6. \tag{81}$$

Since $t! < 2^{4t(t-3)/3}$ for $t \geqslant 4$ by Lemma 16(b), we conclude that $q^{i^2t^2-it-3it(i-1)-6} < 2^{12t} \cdot (t!)^6 < 2^{12t} \cdot 2^{8t^2-24t}$, and so $q^{i^2t^2-it-3it(i-1)-6} < 2^{8t^2-12t}$. Then $(i^2t^2 - it - 3it(i-1) - 6) \cdot \log_p q < (8t^2-12t) \cdot \log_p 2 < (8t^2-12t) \times 0.7$, and so $10i^2t(t-3) + 20it - 60 < 56t^2 - 84t$. Since $i \geqslant 5$, it follows that $250t^2 - 650t - 60 \leqslant 10i^2t(t-3) + 20it - 60 < 56t^2 - 84t$, Thus, $250t^2 - 650t - 60 < 56t^2 - 84t$, and so $194t^2 - 566t - 60 < 0$, this inequality does not hold for any $t \geqslant 4$, which is a contradiction.

(3.2.3) Let i be even. Then by [23, Proposition 4.2.11], the $H \cap X$ is isomorphic to

$$d^{-1}\Omega_i^{\epsilon_1}(q)^t.2^{2(t-1)}.\mathrm{Sym}_t,$$

where $\epsilon = \epsilon_1^t$ and $d \in \{1, 2, 4\}$.

If $t = 2$, then $m = i$, as $2m = it$. Let u be a positive integer such that $i = 2u$. Then by (1), we have that

$$v = \frac{q^{2u^2}(q^u + \epsilon_1 1) \cdot (q^{4u-2}-1)(q^{4u-4}-1)\cdots(q^2-1)}{2 \cdot (q^{2u-2}-1)^2(q^{2u-4}-1)^2\cdots(q^2-1)^2}.$$

This contradicts the fact that v is odd. Therefore, $t \geqslant 3$.

If $i = 2$, then $m = t$, and so by (1) and Lemma 15, we have that $v > q^{2t^2-t}/[2^{t-2}(t!) \cdot (q+1)^t]$. By [35, p. 333], the parameter k is at most $2^5 \cdot 3 \cdot \lambda a \cdot t(t-1)(q+1)^2$, and so by Lemma 8(b), we conclude that $\lambda q^{2t^2-t}/[2^{t-2}(t!) \cdot (q+1)^t] < \lambda v < k^2 \leqslant 2^{10}3^2\lambda^2 a^2 \cdot t^2(t-1)^2(q+1)^4$. Since $a^2 < q$, $2^{10}3^2 < 2^{14}$ and $t^2(t-1)^2 < t^4$, it follows that

$$q^{2t^2-t-1} < 2^{t+12}\lambda t^4(t!)(q+1)^{t+4}. \tag{82}$$

Table 6: Some parameters for Case 3.2.3 in Proposition 21

Line	X	$H \cap X$	v	k divides
1	$P\Omega_{12}^{+}(3)$	$\hat{}\Omega_4^{+}(3)^3.2^2.\mathrm{Sym}_3$	5898080746972747508175	18345885696
2	$P\Omega_{12}^{+}(5)$	$\hat{}\Omega_4^{+}(5)^3.2^2.\mathrm{Sym}_3$	181234396436428964138031005859375	286654464000000

Note that λ is a prime divisor of k. Thus by Lemma 8(b), λ must divide a, t or $(q+\epsilon 1)/2$. Therefore $\lambda \leqslant \max\{a, t, (q+1)/2\} < t(q+1)/2$, and so by (82), we have that

$$q^{2t^2-t-1} < 2^{t+11}t^5(t!)(q+1)^{t+5}. \tag{83}$$

As $q+1 < 2q$ and $t^5 \leqslant 2^{3t}$, we conclude that $q^{2t^2-2t-6} < 2^{5t+15}(t!)$. Note that $t = m \geqslant 4$. Then by Lemma 16(b), we have that $q^{2t^2-2t-6} < 2^{5t+15}(t!) < 2^{5t+15}2^{4t(4-3)/3}$. Thus $q^{6t^2-6t-18} < 2^{4t^2+3t+45}$, and so $(6t^2-6t-18)\cdot\log_p q < (4t^2+3t+45)\cdot\log_p 2 \leqslant (4t^2+3t+45)\times 0.7$. Hence $60t^2-60t-180 < 28t^2+21t+300$, and so $32t^2-81t-480 < 0$, then $t = 4, 5$. If $t = 5$, then (83) implies that $q^{44} < 2^{16}\cdot 5^5(5!)\cdot(q+1)^{10} < 2^{26}\cdot 5^5(5!)q^{10}$, and so $q^{34} < 2^{26}\cdot 5^5\cdot(5!)$, which is impossible. If $t = 4$, then by the same manner, we must have $q^{18} < 2^{37}\cdot 3$, which is valid for $q = 3$. Since λ divides $a = 1$, $t = 4$ or $(q+\epsilon 1)/2 = (3+\epsilon 1)/2$, we conclude that $\lambda = 2$, which is a contradiction.

If $i = 4$, then $m = 2t$, and so by Corollary 12 and Lemma 15, we conclude that $q^{m(2m-1)} < |\mathrm{Out}(X)|^2\cdot 2^{6t-3}\cdot(t!)^3\cdot q^{6t}(q^4-1)^{3t}$. Thus, $q^{m(2m-1)} < |\mathrm{Out}(X)|^2\cdot 2^{6t-3}\cdot(t!)^3\cdot q^{18t}$. Note that $|\mathrm{Out}(X)|$ divides $24a$, $a^2 < q$ and $m = 2t$. Thus, $q^{8t^2-2t} = q^{m(2m-1)} < 2^{6t+3}3^2(t!)^3q^{18t+1}$, and so

$$q^{8t^2-20t-3} < 2^{6t-3}\cdot(t!)^3. \tag{84}$$

If $t = 3$, then (84) yields $q^9 < 2^{18}\cdot 3^3$, and so $q = 3, 5$. In each of these cases, $H \cap X$ and v are recorded as in Table 6. By Lemma 8(b), the parameter k divides $|\mathrm{Out}(X)|\cdot|H\cap X|$ as in the fifth column of Table 6. It is easy to check for each possible parameters v and k that the fraction $k(k-1)/(v-1)$ is not prime, which is a contradiction. If $t \geqslant 4$, then by Lemma 16(b), we have that $t! < 2^{4t(t-3)/3}$, and so (84) implies that $q^{8t^2-20t-3} < 2^{6t-3}\cdot(t!)^3 < 2^{4t^2-6t-3}$. Thus $q^{8t^2-20t-3} < 2^{4t^2-6t-3}$, and so $(8t^2-20t-3)\cdot\log_p q < (4t^2-6t-3)\cdot\log_p 2 \leqslant (4t^2-6t-3)\times 0.7$. Hence $80t^2-200t-30 < 28t^2-42t-21$, and so $52t^2-158t-9 < 0$, which has no solution for $t \geqslant 4$, which is a contradiction.

If $i \geqslant 6$, then Corollary 12 and Lemma 15 imply that $q^{m(2m-1)} < |\mathrm{Out}(X)|^2\cdot 2^{6t-3}\cdot(t!)^3\cdot q^{3it(i-1)/2}$. Thus, $q^{4m^2-2m} < |\mathrm{Out}(X)|^4\cdot 2^{12t-6}\cdot(t!)^6\cdot q^{3it(i-1)}$. Note that $|\mathrm{Out}(X)|$ divides $24a$ and $a^2 < q$. Thus, $q^{4m^2-2m} < 2^{12t+6}3^4(t!)^6q^{3it(i-1)+2}$. Since $2m = it$, we conclude that

$$q^{i^2t(t-3)+2it-6} < 2^{12t+6}\cdot(t!)^6. \tag{85}$$

If $t = 3$, then (85) yields $q^{6i-6} < 2^{48}\cdot 3^6$. As q is odd and $i \geqslant 6$, it follows that $q^{6i-6} < 2^{48}\cdot 3^6$. This inequality holds only for $(i, q) = (6, 3)$ in which case by (1), we easily

Table 7: Some parameters for Cases 4 and 5 in Proposition 21

Line	X	H_0	Conditions	v	k divides	q
1	$\Omega_7(q)$	$\mathrm{SO}_7(2)$	$q = p \equiv \pm 3 \pmod 8$	$\frac{q^9(q^6-1)(q^4-1)(q^2-1)}{2^{10}\cdot 3^4\cdot 5\cdot 7}$	$2^{10}\cdot 3^4\cdot 5\cdot 7$	3, 5
2	$\mathrm{P}\Omega_8^+(q)$	$\Omega_8^+(2)$	$q = p \equiv \pm 3 \pmod 8$	$\frac{q^{12}(q^6-1)(q^4-1)^2(q^2-1)}{2^{14}\cdot 3^5\cdot 5^2\cdot 7}$	$2^{15}\cdot 3^5\cdot 5^2\cdot 7$	3, 5
3	$\Omega_8^+(q)$	$2^3{\cdot}2^6{\cdot}\mathrm{PSL}_3(2)$	$q = p \equiv \pm 3 \pmod 8$	$\frac{q^{12}(q^6-1)(q^4-1)^2(q^2-1)}{2^{14}\cdot 3\cdot 7}$	$2^{15}\cdot 3^2\cdot 7$	3

observe that v is even, which is a contradiction. If $t \geqslant 4$, then $t! < 2^{4t(t-3)/3}$ by Lemma 16(b). Thus by (85), we conclude that $q^{i^2t(t-3)+2it-6} < 2^{12t+6}(t!)^6 < 2^{12t+6}2^{8t^2-24t}$, and so $q^{i^2t(t-3)+2it-6} < 2^{8t^2-12t+6}$. Then $[i^2t(t-3)+2it-6] \times \log_p q < (8t^2-12t+6) \times \log_p 2 \leqslant (8t^2-12t+6) \times 0.7$. Hence $10i^2t(t-3)+20it-60 < 56t^2-84t+42$. Since $i \geqslant 6$, it follows that $360t^2-960t-60 \leqslant 10i^2t(t-3)+20it-60 < 56t^2-84t+42$ and so $304t^2-876t-102 < 0$, which is impossible for $t \geqslant 4$.

(4)-(5) In these cases, the pairs (X, H_0) are recorded in Table 7, and for each case, by (1), we obtain the parameter v as in the fifth column of the same table. Moreover, for each pairs $(X, H \cap X)$, by Lemmas 7 and 8(b), the parameter k divides the number listed in the sixth column of Table 7. We now apply Lemma 8(b), and so $v < k^2$. For each row, this inequality is true only for q given in the last column of Table 7. It is easy to check that for each appropriate pairs (v, k), the fraction $k(k-1)/(v-1)$ is not a prime number.

(6) Let $H = N_G(X(q_0))$ with $q = q_0^t$ odd and t odd prime. Here, as noted before, we only need consider the case where $X = \mathrm{P}\Omega_{2m}^{\epsilon}(q)$ with q odd, $n = 2m$ and $\epsilon = \pm$. By [23, Proposition 4.5.10], the subgroup H_0 is isomorphic to $\mathrm{P}\Omega_{2m}^{\epsilon}(q_0)$, where $m \geqslant 4$. Note that $|\mathrm{Out}(X)|$ divides $6a$. Then by Lemma 15 and the inequality $|X| < |\mathrm{Out}(X)|^2{\cdot}|H \cap X|^3$, we have that $q_0^{tm(2m-1)} < 2^5{\cdot}3^2{\cdot}a^2{\cdot}q_0^{3m(2m-1)}{\cdot}(1+q_0^{-m})^3$. Since $a^2 < 2q$ and $1+q_0^{-m} < 2$, it follows that $q_0^{(2m^2-m)(t-3)-t} < 2^9{\cdot}3^2$. If $t \geqslant 5$, then $q_0^{4m^2-2m-5} \leqslant q_0^{(2m^2-m)(t-3)-t} < 2^9{\cdot}3^2$, which is impossible. Hence $t = 3$ in which case by (1) and Lemma 15, we have that $v > q_0^{4m^2-2m-4}$. Since k divides $\lambda(v-1, |H|)$ and $v-1$ is coprime to q_0, the parameter k must divide $6a\lambda{\cdot}|H \cap X|_{p'}$. Since $|H \cap X|_{p'} < q_0^{2m(m-1)}(q_0^m+1)^2$, Lemma 8(b) implies that $\lambda q_0^{4m^2-2m-4} < \lambda v < k^2 \leqslant 36a^2\lambda^2 q_0^{2m(m-1)}(q_0^m+1)^2$. Therefore,

$$q_0^{2m^2-4} < 36a^2\lambda{\cdot}(q_0^m+1)^2. \tag{86}$$

Note that λ is an odd prime divisor of k. Thus Lemmas 7 and 8(b) imply that λ divides 3, a, p, $q_0^m - \epsilon 1$ or $q_0^{2j}-1$, for some $j \in \{1, \ldots, m-1\}$, and so $\lambda \leqslant q_0^m + 1$. Then by inequality (86), we have that $q_0^{2m^2-4} < 36a^2{\cdot}(q_0^m+1)^3$. Since $q_0^m + 1 < 2q_0$, $q_0^{2m^2-3m-4} < 2^5{\cdot}3^2a^2$. As $a = 3s$, $m \geqslant 4$ and q_0 is odd, $3^{16s} \leqslant q_0^{2m^2-3m-4} < 2^5{\cdot}3^3s^2$, and so $3^{16s} < 2^5{\cdot}3^3s^2$, which is impossible. □

Proof of Theorem 1 Suppose that $\mathcal{D}$ is a nontrivial symmetric (v, k, λ) design admitting a flag-transitive and point-primitive automorphism group G with socle X a finite simple group of Lie type. Suppose also that λ is prime. The symmetric designs with $\lambda = 2, 3$ admitting flag-transitive transitive automorphism groups are classified in [18, 30, 32], and so by a quick check, we observe that the pairs $(\mathcal{D}, G)$ are as in Table 1. Therefore, we can assume that $\lambda \geqslant 5$. Since $k(k-1) = \lambda(v-1)$, it follows that λ is coprime to k or λ divides k. In the former case, by [9, Corollary 1.2], we conclude that $\mathcal{D}$ is a projective space $\mathrm{PG}_n(q)$ or $\mathcal{D}$ is the unique Hadamard design with parameters $(11, 5, 3)$ which has been already recorded in Table 1. We now consider the latter case where λ divides k. We first observe by [6, Corollary 1.2] that the socle X cannot be a finite simple exceptional group. Let now X be a finite simple classical groups. Since G is point-primitive, the point-stabiliser $H = G_\alpha$ is maximal in G, and considering the fact that $k(k-1) = \lambda(v-1)$, we conclude that v is odd, and our main result then follows from Propositions 18-21.

Proof of Corollary 1 Suppose that $\mathcal{D}$ is a nontrivial symmetric (v, k, λ) design with λ prime admitting a flag-transitive and point-imprimitive automorphism group G. Suppose also that (c, d, l) is as in the statement of Corollary 1. If (v, k, λ) is not one of the possibilities mentioned in Corollary 1, then [34, Theorem 1.1] implies that $k = \lambda^2/2$, and since λ is prime, we conclude that $\lambda = 2$, and hence $k = 4/2 = 2 = \lambda$, which is a contradiction.

Acknowledgements

The authors are grateful to the anonymous referees for helpful and constructive comments.

References

[1] S. H. Alavi and M. Bayat. Flag-transitive point-primitive symmetric designs and three dimensional projective special linear groups. *Bulletin of Iranian Mathematical Society (BIMS)*, 42(1):201–221, 2016.

[2] S. H. Alavi, M. Bayat, J. Choulaki, and A. Daneshkhah. Flag-transitive block designs with prime replication number and almost simple groups. *Designs, Codes and Cryptography*, 88(5):971–992, 2020.

[3] S. H. Alavi, M. Bayat, and A. Daneshkhah. Symmetric designs admitting flag-transitive and point-primitive automorphism groups associated to two dimensional projective special groups. *Designs, Codes and Cryptography*, 79(2):337–351, 2016.

[4] S. H. Alavi, M. Bayat, and A. Daneshkhah. Flag-transitive block designs and unitary groups. *Monatshefte für Mathematik*, 193(3):535–553, 2020.

[5] S. H. Alavi, M. Bayat, and A. Daneshkhah. Symmetric designs and projective special linear groups of dimension at most four. *Journal of Combinatorial Designs*, 28(9):688–709, 2020.

[6] S. H. Alavi, M. Bayat, and A. Daneshkhah. Finite exceptional groups of Lie type and symmetric designs. Submitted.

[7] S. H. Alavi, M. Bayat, A. Daneshkhah, and S. Zang Zarin. Symmetric designs and four dimensional projective special unitary groups. *Discrete Mathematics*, 342(4):1159 – 1169, 2019.

[8] S. H. Alavi and T. C. Burness. Large subgroups of simple groups. *J. Algebra*, 421:187–233, 2015.

[9] S. H. Alavi, A. Daneshkhah, and F. Mouseli. A classification of flag-transitive block designs. Submitted.

[10] T. Beth, D. Jungnickel, and H. Lenz. *Design theory. Vol. I*, volume 69 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, Cambridge, second edition, 1999.

[11] S. Braić, A. Golemac, J. Mandić, and T. Vučičić. Primitive symmetric designs with up to 2500 points. *J. Combin. Des.*, 19(6):463–474, 2011.

[12] J. N. Bray, D. F. Holt, and C. M. Roney-Dougal. *The maximal subgroups of the low-dimensional finite classical groups*, volume 407 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 2013. With a foreword by Martin Liebeck.

[13] C. J. Colbourn and J. H. Dinitz, editors. *Handbook of combinatorial designs*. Discrete Mathematics and its Applications (Boca Raton). Chapman & Hall/CRC, Boca Raton, FL, second edition, 2007.

[14] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, and R. A. Wilson. *Atlas of finite groups*. Oxford University Press, Eynsham, 1985. Maximal subgroups and ordinary characters for simple groups, With computational assistance from J. G. Thackray.

[15] A. Daneshkhah and S. Zang Zarin. Flag-transitive point-primitive symmetric designs and three dimensional projective special unitary groups. *Bull. Korean Math. Soc.*, 54(6):2029–2041, 2017.

[16] U. Dempwolff. Primitive rank 3 groups on symmetric designs. *Designs, Codes and Cryptography*, 22(2):191–207, 2001.

[17] J. D. Dixon and B. Mortimer. *Permutation groups*, volume 163 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1996.

[18] H. Dong and S. Zhou. Affine groups and flag-transitive triplanes. *Sci. China Math.*, 55(12):2557–2578, 2012.

[19] The GAP Group. *The GAP Group – Groups, Algorithms, and Programming, Version 4.10.2* , 2019.

[20] W. M. Kantor. Classification of 2-transitive symmetric designs. *Graphs Combin.*, 1(2):165–166, 1985.

[21] W. M. Kantor. Primitive permutation groups of odd degree, and an application to finite projective planes. *J. Algebra*, 106(1):15–45, 1987.

[22] W. M. Kantor and R. A. Liebler. The rank 3 permutation representations of the finite classical groups. *Trans. Amer. Math. Soc.*, 271(1):1–71, 1982.

[23] P. Kleidman and M. Liebeck. *The subgroup structure of the finite classical groups*, volume 129 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 1990.

[24] P. B. Kleidman. *The subgroup structure of some finite simple groups*. PhD thesis, University of Cambridge, 1987.

[25] V. V. Korableva. Primitive parabolic permutation representations of finite special linear and unitary groups. *Proc. Steklov Inst. Math.*, 267(suppl. 1):S100–S110, 2009.

[26] E. S. Lander. *Symmetric designs: an algebraic approach*, volume 74 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 1983.

[27] M. W. Liebeck and J. Saxl. The primitive permutation groups of odd degree. *J. London Math. Soc. (2)*, 31(2):250–264, 1985.

[28] M. W. Liebeck, J. Saxl, and G. Seitz. On the overgroups of irreducible subgroups of the finite classical groups. *Proc. Lond. Math. Soc.*, 50(3):507–537, 1987.

[29] R. Mathon and E. Spence. On 2-$(45, 12, 3)$ designs. *J. Combin. Des.*, 4(3):155–175, 1996.

[30] E. O'Reilly-Regueiro. *Flag-transitive symmetric designs*. PhD thesis, University of London, 2003.

[31] E. O'Reilly-Regueiro. Biplanes with flag-transitive automorphism groups of almost simple type, with classical socle. *J. Algebraic Combin.*, 26(4):529–552, 2007.

[32] E. O'Reilly-Regueiro. Classification of flag-transitive symmetric designs. *Electronic Notes in Discrete Mathematics*, 28:535 – 542, 2007. 6th Czech-Slovak International Symposium on Combinatorics, Graph Theory, Algorithms and Applications.

[33] C. E. Praeger. The flag-transitive symmetric designs with 45 points, blocks of size 12, and 3 blocks on every point pair. *Des. Codes Cryptogr.*, 44(1-3):115–132, 2007.

[34] C. E. Praeger and S. Zhou. Imprimitive flag-transitive symmetric designs. *J. Combin. Theory Ser. A*, 113(7):1381–1395, 2006.

[35] J. Saxl. On finite linear spaces with almost simple flag-transitive automorphism groups. *J. Combin. Theory Ser. A*, 100(2):322–348, 2002.

[36] G. M. Seitz. Flag-transitive subgroups of Chevalley groups. *Ann. of Math. (2)*, 97:27–56, 1973.

[37] Y. Zhang, Z. Zhang, and S. Zhou. Reduction for primitive flag-transitive symmetric 2- (v, k, λ) designs with λ prime. *Discrete Math.*, 343(6):111843, 4, 2020.