FINITE GROUPS WITH MANY VALUES ON A COLUMN OF THE CHARACTER TABLE

PHAM HUU TIEP AND HUNG P. TONG-VIET

Abstract. In this paper, we classify all finite groups whose character tables have some column with pairwise distinct values.

1. Introduction

Characterizing finite groups using the full or just partial information on the (ordinary) character tables of the groups is one of the main problems in the character theory of finite groups. Many important results in this direction have been found using just the first column of the character table, i.e. the set $\mathrm{cd}(G)$ of the degrees of complex irreducible characters of the finite group G. In this paper, we are interested in the behavior of other columns. For a finite group G, we denote by $\mathrm{Irr}(G)$ the set of all irreducible complex characters of G. An element $g \in G$ is called a *non-vanishing* element if $\chi(g)$ is non-zero for all $\chi \in \mathrm{Irr}(G)$, that is, the column of the character table of G labeled by the conjugacy class g^G of G containing g has no zero entry. In [DNPST, INW], the authors proved that a non-vanishing element g of a finite group G lies in the Fitting subgroup $\mathbf{F}(G)$ of G provided that $|g|$, the order of g, is coprime to 6, or coprime to 2 when G is solvable. A finite group G is called an $\mathsf{MV}(g)$-group for some element $g \in G$ if $\chi(g) \neq \psi(g)$ for every $\chi \neq \psi \in \mathrm{Irr}(G)$. In other words, G is an $\mathsf{MV}(g)$-group if distinct irreducible characters of G take distinct values at g, that is to say the column of the character table of G labeled by g^G has pairwise distinct entries. Clearly, if G is an $\mathsf{MV}(g)$-group, then g is a non-vanishing element or there is exactly one zero entry in the column labeled by g^G. The $\mathsf{MV}(g)$-groups (or just MV-groups) have been studied in [BCG, QZ]. In this latter reference, the authors classified all finite solvable MV-groups; and in the former, Bianchi, Chillag and Gillio classified $\mathsf{MV}(g)$-groups under the assumption that g is rational. As it turns out the only nontrivial $\mathsf{MV}(g)$-groups, where g is rational, are the symmetric groups of degree 2 or 3. From this result, one can deduce that if G is an $\mathsf{MV}(g)$-group

Date: November 4, 2014.

2000 *Mathematics Subject Classification.* Primary 20C15, secondary 20D05.

Key words and phrases. character tables, character values.

The first author gratefully acknowledges the support of the NSF (grant DMS-1201374) and the Simons Foundation Fellowship 305247. Tong-Viet's research had been financed by the German Research Council (DFG), via project C13 'The geometry and combinatorics of groups' within the CRC 701.

Part of the paper was written while the first author visited the Department of Mathematics, Harvard University. It is a pleasure to thank Harvard University for generous hospitality and stimulating environment.

with $g = 1$, the identity of G, equivalently, all irreducible characters of G have pairwise distinct degrees, then G is trivial.

The purpose of this paper is to classify nonsolvable MV-groups.

Theorem A. *Let G be a finite nonsolvable group. Suppose that the complex irreducible characters of G take pairwise distinct values at some $g \in G$. Then $G \cong \mathsf{A}_5$ and $|g| = 5$.*

The converse of this statement is also true. In fact, A_5 is an $\mathsf{MV}(g)$-group for every $g \in \mathsf{A}_5$ of order 5 (there are two conjugacy classes of such elements in A_5, see Table 1). Combining with [QZ, Theorem 1.1], we obtain the complete classification of MV-groups.

Theorem B. *Let G be a finite group. Then the complex irreducible characters of G take pairwise distinct values at some $g \in G$ if and only if*

(1) *G is solvable, $G = \langle g \rangle G'$ and the following cases hold.*

  (*a*) *$G = \langle g \rangle$ is a cyclic group with generator g.*

  (*b*) *G is a Frobenius group of order $p^n(p^n - 1)$ with a cyclic complement of order $p^n - 1$.*

  (*c*) *$G = \mathrm{SL}_2(3)$ or $3^2 : \mathrm{SL}_2(3)$ and g is of order 3.*

(2) *$G \cong \mathsf{A}_5$ and $|g| = 5$.*

As one may expect, we prove the main Theorem A by reducing it to almost simple groups, and of course using the Classification of Finite Simple Groups. We emphasize that the treatment of almost simple groups requires a quite delicate consideration of the influence of outer automorphisms of simple groups S on irreducible characters of S.

There is a dual question for the row of the character table, that is, to classify all the pairs (G, χ) where G is a finite group and $\chi \in \mathrm{Irr}(G)$ is nonlinear such that χ takes distinct values at distinct conjugacy classes of G, or equivalently, the row labeled by χ has pairwise distinct values. Unlike the columns, the row corresponding to a nonlinear irreducible character always contains a zero by the famous Burnside's theorem and thus such χ vanishes on a unique conjugacy class of G. The case when χ is imprimitive was studied in [BT]. Finally, one can generalize the concept of MV-groups by considering finite groups G with some element $g \in G$ in which distinct nonlinear irreducible characters of G take distinct values at g. This would give a generalization of the result in [BCH].

2. Proof of Theorem A

For a finite group G and $N \trianglelefteq G$, we define $\mathrm{Irr}(G|N) = \mathrm{Irr}(G) - \mathrm{Irr}(G/N)$ and $\mathrm{cd}(G|N) = \{\chi(1) | \chi \in \mathrm{Irr}(G|N)\}$. If $\theta \in \mathrm{Irr}(N)$, then the inertia group of θ in G is denoted by $I_G(\theta)$ and we write $\mathrm{Irr}(G|\theta)$ for the set of irreducible constituents of θ^G. Let $\rho(G)$ be the set consisting of primes dividing some character degree of G. Finally, let $\Delta(G)$ be a graph with vertex set $\rho(G)$ and there is an edge between two distinct primes r and s if rs divides some character degree of G. We begin with the following obvious lemma whose proof will be omitted.

Lemma 2.1. *Let G be a finite $\mathsf{MV}(g)$-group for some $g \in G$ and let $N \trianglelefteq G$ be a proper normal subgroup of N. Then*
(a) $G = \langle g^G \rangle = \langle g \rangle G'$.
(b) *G/N is an $\mathsf{MV}(gN)$-group.*

In the next statement, we study a minimal counterexample to Theorem A.

Proposition 2.2. *Let (G, g) be a counterexample to Theorem A with $|G|$ minimal. Then*
(i) *If $\theta \in \mathrm{Irr}(G')$ is not G-invariant, then $\theta^G \in \mathrm{Irr}(G)$.*
(ii) *If $G \neq G'$, then G has a unique nonlinear irreducible character which is not irreducible upon restriction to G'.*
(iii) *G is an almost simple group with nonabelian simple socle G' and G/G' is cyclic with generator gG'.*

Proof. Suppose that (G, g) is a counterexample to Theorem A with $|G|$ minimal. Then G is a nonsolvable $\mathsf{MV}(g)$-group but $G \ncong \mathsf{A}_5$. If G is nonabelian simple, then we have nothing to prove. So assume that G is not simple. By Lemma 2.1(a), G/G' is cyclic with generator gG'. Let $\theta \in \mathrm{Irr}(G')$ and suppose that θ is not G-invariant. Let $T = I_G(\theta)$. Then $G' \trianglelefteq T \trianglelefteq G$ and $T \neq G$. Notice that $g^G \cap T = g^G \cap G' = \emptyset$ since $G = \langle g^G \rangle$ by Lemma 2.1(a). We need to show that $T = G'$. Suppose by contradiction that $T \neq G'$. Then T/G' is a nontrivial cyclic subgroup of G/G'. Hence θ extends to $\theta_0 \in \mathrm{Irr}(T)$ by [Is, Corollary 11.22] and by Gallagher's Theorem [Is, Corollary 6.17], $\theta_0\lambda$ with $\lambda \in \mathrm{Irr}(T/G')$ are all the irreducible constituents of θ^T and are distinct for distinct λ. Hence, since T/G' is nontrivial, we can find $\phi_1 \neq \phi_2 \in \mathrm{Irr}(T|\theta)$ and thus $\phi_i^G \in \mathrm{Irr}(G)$ are distinct and both vanish at g as $g^G \cap T = \emptyset$, a contradiction. Therefore, $\theta^G \in \mathrm{Irr}(G)$ whenever $\theta \in \mathrm{Irr}(G')$ is not G-invariant which proves (i). For (ii), suppose that G has two distinct nonlinear irreducible characters $\chi_i, i = 1, 2$ which are not irreducible upon restriction to G' and let $\theta_i \in \mathrm{Irr}(G')$ be an irreducible constituent of $(\chi_i)_{G'}$. Now for $i = 1, 2$, θ_i is not G-invariant as otherwise since G/N is cyclic θ_i extends to G by [Is, Corollary 11.22] and thus χ_i is an extension of θ_i, a contradiction. Therefore, both θ_i are not G-invariant and hence by (i), $\chi_i = \theta_i^G \in \mathrm{Irr}(G)$, so they both vanish at g, a contradiction. We now prove (iii), let M be a fixed minimal normal subgroup of G.

Claim 1. G/M is solvable and M is nonabelian. It suffices to show that G/N is solvable and since G is nonsolvable, M must be nonabelian. Suppose to the contrary that G/M is nonsolvable. By Lemma 2.1(b), G/M is a nonsolvable $\mathsf{MV}(gM)$-group. As $|G/M| < |G|$, by the minimality of $|G|$, $G/M \cong \mathsf{A}_5$ and $g^5 \in M$. From the character table of A_5 given in Table 1, there exists $\chi_5 \in \mathrm{Irr}(G/M)$ with $\chi_5(g) = \chi_5(gM) = 0$. Moreover, if $\chi \in \mathrm{Irr}(G|M)$, then $\chi(g) \notin \{0, \pm 1\}$. We proceed by proving the following.

(a) M is abelian. Suppose by contradiction that M is nonabelian. Then $M \cong S^k$ for some nonabelian simple group S and some integer $k \geq 1$. By [BCLP, Theorems 2,3,4], S has a nontrivial irreducible character $\theta \in \mathrm{Irr}(S)$ which is extendible to $\mathrm{Aut}(S)$ and thus $\varphi = \theta^k \in \mathrm{Irr}(M)$ extends to $\varphi_0 \in \mathrm{Irr}(G)$ by [BCLP, Lemma 5]. By Gallagher's Theorem [Is, Corollary 6.17], we know that $\psi = \varphi_0\chi_5 \in \mathrm{Irr}(G)$ and definitely $\chi_5 \neq \psi$. But then $\psi(g) = \varphi_0(g)\chi_5(g) = 0 = \chi_5(g)$, which is impossible. Hence, M is abelian.

(b) G is perfect. Assume by contradiction that $G' \neq G$. Since $G/M \cong \mathsf{A}_5$, we have $G'M = G$. Moreover, as M is a minimal normal subgroup of G, either $G' \cap M = 1$ or $M \leq G'$. If the latter case holds, then $G'/M \trianglelefteq G/M \cong \mathsf{A}_5$ so $G = G'$ as required. Now assume that $G' \cap M = 1$. It follows that $G = MG' \cong M \times G'$. Thus $G' \cong \mathsf{A}_5$. We show that $M = 1$. Assume that $M \neq 1$ and let $1_M \neq \lambda \in \mathrm{Irr}(M)$. Let $\psi_1 = 1_M \times \chi_5$ and $\psi_2 = \lambda \times \chi_5$. Then $\psi_i, i = 1, 2$ are distinct irreducible characters of $G \cong M \times \mathsf{A}_5$ and they both vanish at g, which is a contradiction as G is an $\mathsf{MV}(g)$-group. Thus $M = 1$ and $G \cong \mathsf{A}_5$, a contradiction. Hence, $G = G'$ as wanted.

(c) There exists $1_M \neq \lambda \in \mathrm{Irr}(M)$ which is not G-invariant. Suppose that every $\theta \in \mathrm{Irr}(M)$ is G-invariant. We have $[G, M] \leq \ker(\theta)$ for every $\theta \in \mathrm{Irr}(M)$ since M is abelian by (a), therefore, $[G, M] \leq \cap_{\lambda \in \mathrm{Irr}(M)} \ker(\lambda) = M' = 1$ and thus $M \leq \mathbf{Z}(G) = \mathbf{Z}(G) \cap G'$ as G is perfect by (b). It follows that $|M|$ divides the order of the Schur multiplier of $G/M \cong \mathsf{A}_5$ so $|M|$ divides 2. If $M = 1$, then $G \cong \mathsf{A}_5$, a contradiction. Thus $|M| = 2$ and $G \cong 2 \cdot \mathsf{A}_5$. However $2 \cdot \mathsf{A}_5$ is not an MV-group by checking [CCNPW].

(d) If $\theta \in \mathrm{Irr}(M)$ and $T = I_G(\theta) \neq G$, then $T/M \cong \mathbb{Z}_5$ or D_{10} and $\varphi^G(1) \in \{6, 12\}$ for every $\varphi \in \mathrm{Irr}(T|\theta)$. Suppose that $\theta \in \mathrm{Irr}(M)$ is not G-invariant with $T = I_G(\theta)$ and write $\theta^T = \sum_{i=1}^s e_i\phi_i$, where $\phi_i \in \mathrm{Irr}(T|\theta)$. As $G = \langle g^G \rangle$ and $M \trianglelefteq G$, $g^G \cap M = \emptyset$. If $5 \nmid |T/M|$, then $g^G \cap T = \emptyset$ and so $\phi_i^G(g) = 0$, which is a contradiction since $\chi_5 \neq \phi_i^G \in \mathrm{Irr}(G|M)$. Thus T/M contains a Sylow 5-subgroup K/M of G/M. Without loss of generality, we can assume that $g \in K \leq T$. Then $K = M\langle g \rangle$ and K/M is cyclic of order 5. By Table 2, the only proper over-group of a Sylow 5-subgroup of A_5 is a group isomorphic to D_{10}, so $T/M = K/M \cong \mathbb{Z}_5$ or $K/M \leq T/M \cong \mathrm{D}_{10}$. In both cases, the Schur multiplier of T/M is trivial and since θ is T-invariant, θ extends to $\theta_0 \in \mathrm{Irr}(T)$ by [Is, Theorem 11.7]. Let $\varphi \in \mathrm{Irr}(T|\theta)$. By Gallagher's Theorem, $\varphi = \theta_0\mu$ for some $\mu \in \mathrm{Irr}(T/M)$ and $\varphi^G(1) = |G : T|\varphi(1) = |G : T|\theta(1)\mu(1) = |G : T|\mu(1)$. If $T/M \cong \mathbb{Z}_5$ then $\mu(1) = 1$ and $|G : T| = 12$; and if $T/M \cong \mathrm{D}_{10}$, then $\mu(1) \in \{1, 2\}$ and $|G : T| = 6$. Therefore, $\varphi^G(1) = |G : T|\mu(1) \in \{6, 12\}$.

(e) $\{1, 3, 4, 5\} \subseteq \mathrm{cd}(G) \subseteq \{1, 2, 3, 4, 5, 6, 12\}$. Clearly $\mathrm{cd}(G/M) = \{1, 3, 4, 5\} \subseteq \mathrm{cd}(G)$. For the other inclusion, we need to show that if $1_M \neq \theta \in \mathrm{Irr}(M)$ and $\chi \in \mathrm{Irr}(G|\theta)$, then $\chi(1) \in \{2, 4, 6, 12\}$. This proves our claim since $\mathrm{cd}(G) = \mathrm{cd}(G/M) \cup \mathrm{cd}(G|M)$. Let $1_M \neq \theta \in \mathrm{Irr}(M)$. If θ is not G-invariant, then $\chi(1) \in \{6, 12\}$ for all $\chi \in \mathrm{Irr}(G|\theta)$ by (d). Now assume that θ is G-invariant. Since G is perfect, θ cannot extend to G. So, θ is G-invariant but not extendible to G. Write $\theta^G = \sum_{i=1}^k e_i\chi_i$, where $\{\chi_i\}_{i=1}^k = \mathrm{Irr}(G|\theta)$ and $e_i \geq 1$ for $1 \leq i \leq k$. Since θ is not extendible to G, $e_i > 1$ for all i and thus each e_i is the degree of a proper projective irreducible representation of A_5. By [CCNPW], we have $e_i \in \{2, 4, 6\}$. So $\chi_i(1) = e_i\theta(1) = e_i \in \{2, 4, 6\}$. Hence the result follows.

(f) $\Delta(G)$ has exactly two connected components. From (e), we have $\rho(G) = \{2, 3, 5\}$. By (c) and (d) above, 2 and 3 are adjacent in $\Delta(G)$ and by (e), 5 is an isolated vertex, therefore $\Delta(G)$ has exactly two connected components, namely $\{2, 3\}$ and $\{5\}$.

(g) The contradiction. Since G is perfect but not simple and $\Delta(G)$ has two connected components, [LW, Theorem 6.2] yields that either $G \cong \mathrm{SL}_2(q)$ for some odd prime power

$q \geq 5$ or G has a normal subgroup L such that $G/L \cong \mathrm{SL}_2(q)$ for some prime power $q \geq 4$, L is elementary abelian of order q^2, and G/L acts transitively on $\Omega = \mathrm{Irr}(L) \setminus \{1_L\}$.

Assume first that $G \cong \mathrm{SL}_2(q)$ for some odd prime $q \geq 5$. Let $Z := \mathbf{Z}(G) \cong C_2$. Since $ZM/M \trianglelefteq G/M \cong \mathsf{A}_5$ and ZM/M is abelian, we have $Z \leq M$. As M is a minimal normal subgroup of G, we obtain $M = Z$ which implies that $\mathrm{PSL}_2(q) \cong \mathsf{A}_5$ with q odd. Therefore, $q = 5$ and thus $G \cong \mathrm{SL}_2(q)$. However, $\mathrm{SL}_2(5) \cong 2 \cdot \mathsf{A}_5$ is not an MV-group.

Assume that the latter case holds. As above, we see that $LM/M \trianglelefteq G/M \cong \mathsf{A}_5$ and LM/M is abelian, so $L \leq M$. Since M is a minimal normal subgroup of G, we deduce that $L = M$, which implies that $\mathrm{SL}_2(q) \cong \mathsf{A}_5$ hence $q = 4$ so that $|L| = 4^2$, $G/L \cong \mathrm{SL}_2(4) \cong \mathsf{A}_5$ and G/L acts transitively on Ω. Let $1_L \neq \theta \in \mathrm{Irr}(L)$ and let $T = I_G(\theta)$. As G/L acts transitively on Ω, we deduce that $|\Omega| = |G : T|$, hence $|G : T| = 4^2 - 1 = 15$ so T/L is a 2-group, contradicting (d). This final contradiction shows that G/M is solvable.

Claim 2. $G' = G'' = M$.

We first claim that $G' = G''$. Suppose to the contrary that $G' \neq G''$. Then G/G'' is a solvable $\mathsf{MV}(gG'')$-group by Lemma 2.1(b). As G/G'' is solvable of derived length 2, we deduce from [QZ, Theorem 1.1] that G/G'' is a Frobenius group with cyclic Frobenius complement of order $p^n - 1$ for some prime p and some integer $n \geq 1$ and a Frobenius kernel F/G'' of order p^n. Moreover, $G = \langle g \rangle F$ and $g^{p^n-1} \in F$. Clearly, G/G'' has an irreducible character $\phi \in \mathrm{Irr}(G/G'')$ of degree $p^n - 1$ and $\phi(g) = \phi(gG'') = 0$. As in the proof of Claim 1a, M possesses an irreducible character $\varphi \in \mathrm{Irr}(M)$ which is extendible to $\varphi_0 \in \mathrm{Irr}(G)$ and by Gallagher's Theorem, $\psi = \varphi_0\phi \in \mathrm{Irr}(G)$ and so $\psi(g) = \varphi_0(g)\phi(g) = 0 = \phi(g)$, which is impossible as $\psi \neq \phi$. Therefore, $G' = G''$ as wanted. It follows that $G^{(\infty)} = G'$, where $G^{(\infty)}$ is the last term of the derived series of G. Now as G/M is solvable by Claim 1, we deduce that $G' = G^{(\infty)} \leq M$, which implies that $M = G'$ since M is a minimal normal nonabelian subgroup of G.

Claim 3. G is almost simple with nonabelian simple socle G'.

We have that $G = G'\langle g \rangle$ by Lemma 2.1(a), so G/G' is cyclic. By Claim 2, G' is the unique minimal normal subgroup of G, which implies that $\mathbf{C}_G(G') = 1$. Hence G embeds into $\mathrm{Aut}(S) \wr \mathsf{S}_k$, where $G' \cong S^k$ for some nonabelian simple group S and some $k \geq 1$. Let $B = \mathrm{Aut}(S)^k \cap G$. Then $G' \leq B \trianglelefteq G$ and G/B is a cyclic subgroup of S_k. Suppose that $k \geq 2$. Let $\theta \in \mathrm{Irr}(S)$ be a nontrivial character of S which is extendible to $\mathrm{Aut}(S)$ and let $\alpha \in \mathrm{Irr}(S) \setminus \{1_S, \theta\}$. Let $\varphi = \theta \times 1_S \times \cdots \times 1_S$ and $\psi = \theta \times \alpha \times \cdots \times \alpha$. Then φ and ψ are distinct irreducible characters of G' with distinct degrees and they are both not G-invariant. By (i), ψ^G and φ^G are irreducible characters of G and are distinct by comparing their degree; however this contradicts (ii). Hence $k = 1$ and thus G is almost simple with nonabelian simple socle G' as wanted. □

Proposition 2.3. *Let G be a finite almost simple group with nonabelian simple socle G'. Suppose that G is an $\mathsf{MV}(g)$-group for some $g \in G$ and that G' is a simple sporadic group, the Tits group or an alternating group of degree at least 5. Then $G \cong \mathsf{A}_5$ and $|g| = 5$.*

TABLE 1. Character table of A_5

	1A	2A	3A	5A	5B
χ_1	1	1	1	1	1
χ_2	3	-1	0	$\frac{1-\sqrt{5}}{2}$	$\frac{1+\sqrt{5}}{2}$
χ_3	3	-1	0	$\frac{1+\sqrt{5}}{2}$	$\frac{1-\sqrt{5}}{2}$
χ_4	4	0	1	-1	-1
χ_5	5	1	-1	0	0

TABLE 2. The maximal subgroups of A_5

Group	Order	Index
A_4	12	5
D_{10}	10	6
S_3	6	10

Proof. Let $S = G'$ be a one of the nonabelian simple groups in the lemma and suppose that G is an almost simple $\mathsf{MV}(g)$-group for some $g \in G$ with socle S. We consider the following cases:

(a) S is an alternating group of degree at least 5.

We know that $\mathrm{Aut}(\mathsf{A}_n) \cong \mathsf{S}_n$ if $n \neq 6$ and $\mathrm{Aut}(\mathsf{A}_6) \cong C_2^2$.

(i) $S \cong \mathsf{A}_n, 5 \leq n \leq 9$ and $S \trianglelefteq G \leq \mathrm{Aut}(S)$. By using [CCNPW], we can check that only A_5 is an $\mathsf{MV}(g)$-group with $|g| = 5$.

(ii) $S \cong \mathsf{A}_n, n \geq 10$ and $G \cong \mathsf{S}_n$. By Proposition 2.2(ii), it suffices to show that S_n possesses two distinct nonlinear irreducible characters which are reducible upon restriction to A_n. It is well known that the irreducible complex characters of S_n are parametrized by partitions of n. Denote by χ^λ the irreducible character of S_n corresponding to partition λ of n. The irreducible characters of the alternating group A_n are then obtained by restricting χ^λ to A_n. In fact, χ^λ is still irreducible upon restriction to A_n if and only if λ is not self-conjugate. Otherwise, χ^λ splits into two irreducible characters $\chi^{\lambda\pm}$ of A_n having the same degree. Therefore, it suffices to find two different partitions of n, which are self-conjugate.

If $n = 2k + 9$ is odd, where $k \geq 1$, then we choose

$$(1) \qquad \begin{cases} \lambda_1 & = & (k+5, 1^{k+4}) \\ \lambda_2 & = & (k+3, 3^2, 1^k) \end{cases}$$

and if $n = 2k+8$ is even then one can choose

$$\begin{cases} \lambda_1 &= (k+4, 2, 1^{k+2}) \\ \lambda_2 &= (k+3, 3, 2, 1^k). \end{cases} \tag{2}$$

Obviously both λ_i are distinct self-conjugate partitions of n as required.

(iii) $G = S \cong \mathsf{A}_n, n \geq 10$. Assume that $n = 2k+9$ is odd. Let

$$g_1 = (1, 2, \cdots, n) \text{ and } g_2 = (1, 2, \cdots, n-4)(n-3, n-2, n-1)$$

be elements in A_n. Let $\lambda_i, i = 1, 2$ be partitions of n given in (1). As both λ_i are self-conjugate, we deduce that $(\chi^{\lambda_i})_{\mathsf{A}_n} = \chi^{\lambda_i^+} + \chi^{\lambda_i^-}$, where $\chi^{\lambda_i^\pm} \in \mathrm{Irr}(\mathsf{A}_n)$. It follows from [JK, Theorem 2.5.13] that if x is not conjugate to g_1 in A_n, then $\chi^{\lambda_1^+}(x) = \chi^{\lambda_1^-}(x)$, and similarly, if x is not conjugate to g_2, then $\chi^{\lambda_2^+}(x) = \chi^{\lambda_2^-}(x)$. As g_1 and g_2 lie in different A_n-conjugacy classes, A_n is not an MV-group when n is odd. Assume next that $n = 2k+8$ is even. The same argument as above applies by taking

$$g_1 = (1, 2, \cdots, n-1),\ g_2 = (1, 2, \cdots, n-3)(n-2, n-1, n) \in \mathsf{A}_n$$

and $\lambda_i, i = 1, 2$ the partitions of n given in (2).

(b) S is a sporadic simple groups or the Tits group. Using [CCNPW], except for $\mathrm{M}_{11}, \mathrm{M}_{12}, \mathrm{M}_{22}, \mathrm{M}_{22} \cdot 2, \mathrm{M}_{24}$ and Co_2, every almost simple group with socle S has at least two zeros in a column different from the first column of the ordinary character table. For the remaining cases, it is routine to check that these groups are not MV-groups. □

Let $\mathcal{S}$ denote the set consisting of the following nonabelian simple groups:

$$\mathrm{PSL}_2(q)(4 \leq q \leq 31), \mathrm{PSL}_3(q)(2 \leq q \leq 9), \mathrm{PSU}_3(q)(3 \leq q \leq 11), \mathrm{PSL}_4(q)(2 \leq q \leq 4),$$
$$\mathrm{PSU}_4(q)(q = 2, 3, 5), \mathrm{PSp}_4(q)'(2 \leq q \leq 7), \mathrm{PSL}_5(q)(q = 2, 3), \mathrm{PSL}_6(2), \mathrm{PSL}_7(2),$$
$$\mathrm{PSU}_6(2), \mathrm{PSp}_6(q)(2 \leq q \leq 4), \mathrm{PSp}_8(2), \Omega_7(3), \mathrm{P}\Omega_8^\pm(q)(q = 2, 3), \mathrm{P}\Omega_{10}^\pm(2),$$
$${}^2\mathrm{B}_2(2^{2n+1})(n = 1, 2), {}^2\mathrm{G}_2(3^3), {}^2\mathrm{F}_4(2)', {}^3\mathrm{D}_4(2), {}^2\mathrm{E}_6(2), \mathrm{G}_2(q)(q = 3, 4), \mathrm{F}_4(2).$$

For an integer $n \geq 1$, denote by $\Phi_n(x)$ the nth cyclotomic polynomial in variable x. For $n = 4, 6, 12$, we also define

$$\Phi_4^+(x) = x + \sqrt{2x} + 1 \qquad \Phi_4^-(x) = x - \sqrt{2x} + 1$$
$$\Phi_6^+(x) = x + \sqrt{3x} + 1 \qquad \Phi_6^-(x) = x - \sqrt{3x} + 1$$
$$\Phi_{12}^+(x) = x^2 + \sqrt{2x^3} + x + \sqrt{2x} + 1 \qquad \Phi_{12}^-(x) = x^2 - \sqrt{2x^3} + x - \sqrt{2x} + 1$$

Notice that $\Phi_n(x) = \Phi_n^+(x)\Phi_n^-(x)$ for $n = 4, 6, 12$.

Let $q, n \geq 2$ be integers. Suppose that $(q, n) \neq (2, 6)$ and if $n = 2$, assume $q+1$ is not a 2-power. Then $q^n - 1$ has a *primitive prime divisor* (p.p.d) $r = r(q, n)$ by Zsigmondy's theorem [Zs], that is, $r | (q^n - 1)$ but $r \nmid \prod_{i=1}^{n-1}(q^i - 1)$.

TABLE 3. Two maximal tori of exceptional groups of Lie type

S	$\lvert T_1\rvert$	$\lvert T_2\rvert$	$\lvert \mathbf{N}_S(T_1)/T_1\rvert$	$\lvert \mathbf{N}_S(T_2)/T_2\rvert$	conditions
${}^2\mathrm{B}_2(q)$	$\Phi_4^+(q)$	$\Phi_4^-(q)$	4	4	$q = 2^{2k+1} \geq 8$
${}^2\mathrm{G}_2(q)$	$\Phi_6^+(q)$	$\Phi_6^-(q)$	6	6	$q = 3^{2k+1} \geq 27$
${}^3\mathrm{D}_4(q)$	$\Phi_3(-q^2)$	$-\Phi_1(-q)\Phi_1(q^3)$	4	4	
${}^2\mathrm{F}_4(q)$	$\Phi_{12}^+(q)$	$\Phi_{12}^-(q)$	12	12	$q = 2^{2k+1} \geq 8$
${}^2\mathrm{E}_6(q)$	$\frac{1}{d}\Phi_3(-q^3)$	$-\frac{1}{d}\Phi_1(-q^4)\Phi_1(q^2)$	9	8	$d = (3, q+1)$
$\mathrm{G}_2(q)$	$\Phi_3(q)$	$\Phi_3(-q)$	6	6	$q > 2$
$\mathrm{F}_4(q)$	$\Phi_3(-q^2)$	$-\Phi_1(-q)\Phi_1(q^3)$	12	12	
$\mathrm{E}_6(q)$	$\frac{1}{d}\Phi_3(q^3)$	$-\frac{1}{d}\Phi_1(-q^4)\Phi_1(q^2)$	9	8	$d = (3, q-1)$
$\mathrm{E}_7(q)$	$\frac{1}{d}\Phi_1(q^7)$	$-\frac{1}{d}\Phi_1(-q^7)$	14	14	$d = (2, q-1)$
$\mathrm{E}_8(q)$	$\Phi_{15}(q)$	$\Phi_{15}(-q)$	30	30	

TABLE 4. Two maximal tori of simple classical groups

S	$\lvert T_1\rvert$	$\lvert T_2\rvert$	d	conditions
$\mathrm{PSL}_n(q)$	$\frac{1}{d}\frac{q^n-1}{q-1}$	$\frac{1}{d}(q^{n-1}-1)$	$(n, q-1)$	$n \geq 2; q \geq 4$ if $n = 2$
$\mathrm{PSU}_n(q)$	$\frac{1}{d}\frac{q^n-(-1)^n}{q+1}$	$\frac{1}{d}(q^{n-1}-(-1)^{n-1})$	$(n, q+1)$	$n \geq 3; q \geq 3$ if $n = 3$
$\mathrm{PSp}_n(q)$	$\frac{1}{d}(q^{\frac{n}{2}}+1)$	$\frac{1}{d}(q^{\frac{n}{2}}-1)$	$(2, q-1)$	$n \geq 4$ even$; q \geq 3$ if $n = 4$
$\Omega_n(q)$	$\frac{1}{d}(q^{\frac{n-1}{2}}+1)$	$\frac{1}{d}(q^{\frac{n-1}{2}}-1)$	2	$n \geq 7$ odd$; q$ odd
$\mathrm{P}\Omega_n^-(q)$	$\frac{1}{d}(q^{\frac{n}{2}}+1)$	$\frac{1}{d}(q^{\frac{n}{2}-1}+1)(q-1)$	$(4, q^{\frac{n}{2}}+1)$	$n \geq 8$ even
$\mathrm{P}\Omega_n^+(q)$	$\frac{(q^{\frac{n}{2}-1}-1)(q-1)}{d}$	$\frac{(q^{\frac{n}{2}-1}+1)(q+1)}{d}$	$(2, q-1)^2$	$n \geq 8, n \equiv 0 \pmod 4$
$\mathrm{P}\Omega_n^+(q)$	$\frac{1}{d}(q^{\frac{n}{2}}-1)$	$\frac{(q^{\frac{n}{2}-1}+1)(q+1)}{d}$	$(4, q^{\frac{n}{2}}-1)$	$n \geq 10, n \equiv 2 \pmod 4$

Recall that an element x in a finite group G is called *rational* if x and x^k are G-conjugate for every integer k with $(|x|, k) = 1$. Observe that x is rational if and only if $\mathbf{N}_G(\langle x\rangle)/\mathbf{C}_G(x) \cong \mathrm{Aut}(\langle x\rangle)$. If $|x| = m$ then $\mathrm{Aut}(\langle x\rangle)$ is a cyclic group of order $\phi(m)$. Hence if $|\mathbf{N}_G(\langle x\rangle) : \mathbf{C}_G(x)| < \phi(|x|)$, then x is not rational in G.

The following lower bounds for $\phi(m)$ might be useful for checking (4). For a proof, see, for example, [BT, Lemma 3.1].

Lemma 2.4. *If $n \geq 1$ is an integer, then $\phi(n) \geq \sqrt{n/a}$, where $a = 2$ if $n \equiv 2 \pmod 4$, otherwise $a = 1$.*

Proposition 2.5. *Let H be an almost simple group with non-abelian simple socle $S = H' < H = \langle g, S\rangle$. Suppose that H is an* $\mathsf{MV}(g)$*-group, S is a simple group of Lie type in characteristic p, and $S \notin \mathcal{S}$. Then $H \leq \mathrm{Inndiag}(S)$.*

Proof. (i) We can find a simple, simply connected algebraic group $\mathcal{G}$ defined over a field of characteristic p and a Frobenius morphism $F : \mathcal{G} \to \mathcal{G}$ such that $S = G/\mathbf{Z}(G)$ for $G := \mathcal{G}^F$. We refer to [Ca] and [DM] for basic facts on the Deligne-Lusztig theory of complex representations of finite groups of Lie type. In particular, irreducible characters of G are partitioned into (rational) Lusztig series which are labeled by conjugacy classes of semisimple elements s in the dual group G^*, where the pair $(\mathcal{G}^*, F^*)$ is dual to $(\mathcal{G}, F)$ and $G^* := (\mathcal{G}^*)^{F^*}$. If $\mathbf{C}_{\mathcal{G}^*}(s)$ is connected, then the G^*-conjugacy class $[s]$ of s corresponds to a (unique) irreducible (semisimple) character χ_s of G of degree $[G^* : \mathbf{C}_{G^*}(s)]_{p'}$, see [DM, §14]. Since χ_s belongs to the Lusztig series defined by $[s]$, two semisimple characters χ_s and χ_t are equal precisely when s and t are conjugate in G^*. Moreover, χ_s is trivial at $\mathbf{Z}(G)$ (and so can be viewed as an irreducible character of S) if $s \in [G^*, G^*]$ (cf. [NT2, Lemma 4.4(ii)]).

The structure of $\mathrm{Aut}(S)$ is described in [GLS, Theorem 2.5.12]; in particular, it is a split extension of $J := \mathrm{Inndiag}(S)$ by an abelian group $A(S) = \Phi\Gamma$, where Φ is the group of (outer) field automorphisms and Γ is the group of (outer) graph automorphisms. We will let Δ denote the *cyclic* subgroup induced by $J\Phi H$ in $\mathrm{Aut}(S)/J\Phi$. Also, let G be defined over $\mathbb{F}_q$ with $q = p^f$.

By way of contradiction, assume that $H \not\leq J$. By Proposition 2.2, H acts transitively on the set $\mathcal{X}$ of non-H-invariant irreducible characters of S.

(ii) First we consider the case where S is of type D_{2n} with $n \geq 2$ and $\Delta \neq 1$. Note that $\Gamma \hookrightarrow \mathsf{S}_3$, and every unipotent character of S is $J\Phi$-invariant by [M2, Theorem 2.5]. If $\Delta \cong C_3$, then $n = 2$ and Δ has two nontrivial orbits (of length 3) on the set of unipotent characters of S by [M2, Theorem 2.5(b)]. If $\Delta \cong C_2$, then Δ has at least two nontrivial orbits (of length 2) on the set of unipotent characters of S by [M2, Theorem 2.5(a)], for instance the pairs of unipotent characters labeled by the degenerate symbols

$$\begin{pmatrix} n \\ n \end{pmatrix}, \begin{pmatrix} 1 & n \\ 1 & n \end{pmatrix}.$$

The same argument applies to the case where $S = \mathrm{F}_4(2^{2a+1})$ (with $a \geq 1$) and $\Delta \neq 1$, by using [M2, Theorem 2.5(e)].

(iii) Next we consider the situation (*) where we can find a prime $r_1 \geq 5$ and an integer $r_2 \neq r_1$ which is either 1 or a prime ≥ 5 and a maximal torus $\mathcal{T} < \mathcal{G}^*$, such that $\gcd(r, |G^*/[G^*, G^*]|) = 1$ and the following conditions hold for any semisimple element $s \in \mathcal{T} \cap G^*$ of order $r := r_1 r_2$:

(a) $\mathbf{C}_{\mathcal{G}^*}(s) = \mathcal{T}$ (since $s \in [G^*, G^*]$, this implies that one can consider χ_s as an irreducible character of S);
(b) χ_s is not H-invariant.

First we observe that conditions (a) and (b) also hold for any semisimple element $t \in [G^*, G^*]$ of order divisible by r. Indeed, since $r_1 \neq r_2$, we may assume that $s = t^k$ has order r for some integer k. Now $\mathbf{C}_{\mathcal{G}^*}(t) \leq \mathbf{C}_{\mathcal{G}^*}(s) = \mathcal{T}$ and $\mathbf{C}_{\mathcal{G}^*}(t)$ contains a maximal torus, whence $\mathbf{C}_{\mathcal{G}^*}(t) = \mathbf{C}_{\mathcal{G}^*}(s) = \mathcal{T}$ and so it is connected. So we may consider $\chi_t \in \mathrm{Irr}(S)$. Suppose that χ_t is H-invariant. Then t and t^g are G^*-conjugate, whence s and s^g are G^*-conjugate, and so χ_s is H-invariant, a contradiction.

Denote $T := \mathcal{T}^{F^*}$, $T_0 := T \cap [G^*, G^*]$, and write $T_0 = T_1 \times T_2 \times T_3$, where $T_1 = \mathbf{O}_{r_1}(T_0)$, $T_2 = \mathbf{O}_{r_2}(T_0)$ if $r_2 \neq 1$ and $T_2 = 1$ if $r_2 = 1$. Now we show our assumptions on H imply that

$$T_3 = 1, \text{ and } |\mathbf{N}_{G^*}(\mathcal{T})/T| \cdot |\Phi| \cdot |\Delta| \geq \begin{cases} (2/3)|T_0| & \text{if } r_2 > 1, \\ |T_0| - 1 & \text{if } r_2 = 1. \end{cases} \tag{3}$$

Indeed, since H is transitive on $\mathcal{X}$, the above observation implies that H fuses the G^*-classes of all elements $t \in T_0$ of order divisible by r; in particular, all of them have the same order r. It follows that $T_3 = 1$, and $\exp(T_i) = r_i$ for $i = 1, 2$. Consider any two elements $t = xy$ and $t' = x'y'$ of order r with $x, x' \in T_1$ and $y, y' \in T_2$. We then have that $[t]$ and $[t']$ are fused by some $h \in H$. Since inner-diagonal automorphisms preserve semisimple characters, we may assume that $h \in A(S)$ and h acts on G^*. Now we have $t' = hutu^{-1}h^{-1}$ for some $u \in G^*$, whence hu conjugates $\mathbf{C}_{\mathcal{G}^*}(t) = \mathcal{T}$ to $\mathbf{C}_{\mathcal{G}^*}(t') = \mathcal{T}$. Note that T centralizes $\mathcal{T} \ni t$. If $r_2 = 1$ then $T_1 = T_0$, whereas if $r_2 > 1$ then $(|T_1| - 1)(|T_2| - 1) > 2|T_0|/3$. Hence the claim follows.

(iv) Suppose that $S = \mathrm{E}_6^\epsilon(q) = \mathrm{E}_6(q)$ or ${}^2\mathrm{E}_6(q)$. Set $d := \gcd(3, q - \epsilon)$. Arguing as in Cases IIe and IIf of the proof of [MT, Proposition 4.7], one can show that (*) holds with

$$(r_1, r_2) = \begin{cases} (r(p, 9f), r(p, 9f/2)), & \text{if } \epsilon = +, 2|f, \\ (r(p, 9f), 1), & \text{if } \epsilon = +, 2 \nmid f, \\ (r(p, 18f), 1), & \text{if } \epsilon = -. \end{cases}$$

Furthermore, $|T| = \Phi_9(q)$ if $\epsilon = +$ and $|T| = \Phi_{18}(q)$ if $\epsilon = -$, $|\mathbf{N}_{G^*}(\mathcal{T})/T| = 9$, and $|\Phi| \cdot |\Delta| \leq 2f$. As $|T_0| \geq |T|/d \geq \Phi_{18}(q)/d$, (3) cannot hold (recall $(q, \epsilon) \neq (2, -)$ as $S \notin \mathcal{S}$).

Consider the case $S = \mathrm{PSL}_n^\epsilon(q)$ with $n \geq 3$, and set $d := \gcd(n, q - \epsilon)$. Also choose $m \in \{n, n-1\}$ to be *odd*. Arguing as in Cases IIa and IIb of the proof of [MT, Proposition 4.7], one can show that (*) holds with

$$(r_1, r_2) = \begin{cases} (r(p, mf), r(p, mf/2)), & \text{if } \epsilon = +,\ 2|f, \\ (r(p, mf), 1), & \text{if } \epsilon = +,\ 2 \nmid f, \\ (r(p, 2mf), 1), & \text{if } \epsilon = -. \end{cases}$$

Furthermore, $|T| = (q^m - \epsilon)(q - \epsilon)^{n-m-1}$, $|T_0| \geq |T|/d$, $|\mathbf{N}_{G^*}(\mathcal{T})/T| = m$, and $|\Phi| \cdot |\Delta| \leq 2f$. As $S \notin \mathcal{S}$, direct computations show that (3) cannot hold.

Next, let $S = \mathrm{D}_n^\epsilon(q) = \mathrm{D}_n(q)$ or ${}^2\mathrm{D}_n(q)$, with $2 \nmid n \geq 5$, and set $d := \gcd(4, q^n - \epsilon)$. Arguing as in Cases IIc and IId of the proof of [MT, Proposition 4.7], one can show that (*) holds with

$$(r_1, r_2) = \begin{cases} (r(p, nf), r(p, nf/2)), & \text{if } \epsilon = +,\ 2|f, \\ (r(p, nf), 1), & \text{if } \epsilon = +,\ 2 \nmid f, \\ (r(p, 2nf), 1), & \text{if } \epsilon = -. \end{cases}$$

Furthermore, $|T| = q^n - \epsilon$, $|\mathbf{N}_{G^*}(\mathcal{T})/T| = 2n$, and $|\Phi| \cdot |\Delta| \leq 2f$. As $|T_0| \geq |T|/d$, (3) cannot hold.

We can argue similarly in the case $S = {}^2\mathrm{D}_n(q)$ with $2|n \geq 4$, following the proof of [MT, Proposition 4.5] (recall $(n, q) \neq (4, 2)$ as $S \notin \mathcal{S}$).

Suppose $S = \mathrm{G}_2(q)$ with $q \geq 5$. Arguing as in the proof of [MT, Proposition 4.4], one can show that (*) holds with $r_2 = 1$ and

$$r_1 = \begin{cases} r(p, 3f), & \text{if } p = 3,\ 2 \nmid f, \\ r(p, 6f), & \text{otherwise.} \end{cases}$$

Furthermore, $|T| = \Phi_3(q)$ or $\Phi_6(q)$, $|\mathbf{N}_{G^*}(\mathcal{T})/T| = 6$, and $|\Phi| \cdot |\Delta| \leq 2f$. As $|T_0| = |T|$, (3) cannot hold.

Let $S = \mathrm{F}_4(q)$ with $q \geq 3$. Arguing as in the proof of [MT, Proposition 4.4], one can show that (*) holds with $r_2 = 1$ and $r_1 = r(p, 12f)$. Furthermore, $|T| = \Phi_{12}(q)$, $|\mathbf{N}_{G^*}(\mathcal{T})/T| = 12$, and $|\Phi| \cdot |\Delta| \leq 2f$. As $|T_0| = |T|$, (3) cannot hold.

Let $S = \mathrm{B}_2(q)$ with $q \geq 5$. Arguing as in the proof of [MT, Proposition 4.5], one can show that (*) holds with $r_2 = 1$ and $r_1 = r(p, 4f)$. Furthermore, $|T| = \Phi_4(q)$, $|\mathbf{N}_{G^*}(\mathcal{T})/T| = 4$, and $|\Phi| \cdot |\Delta| \leq 2f$. As $|T_0| \geq |T|/2$, (3) cannot hold.

(v) The results of (ii) and (iv) show in particular that $|\Delta| = 1$, i.e. H can induce only outer field automorphisms of S.

Consider the case S is one of the following groups: ${}^2\mathrm{B}_2(q)$ with $q \geq 2^5$, ${}^2\mathrm{G}_2(q)$ with $q \geq 3^5$, ${}^3\mathrm{D}_4(q)$ with $q > 2$, ${}^2\mathrm{F}_4(q)$ with $q \geq 8$, or $\mathrm{E}_8(q)$. Following the proof of [MT, Proposition 4.4], one can show that (*) holds with $r_2 = 1$ and $r_1 = r(p, mf)$, and

$$m = 4,\ 6,\ 12,\ 12,\ 30,$$

respectively. Furthermore, $|\Phi| \cdot |\Delta| = 3f$ if $S = {}^3\mathrm{D}_4(q)$ and f otherwise, and

$$|T| = \Phi_4^\epsilon(q),\ \Phi_6^\epsilon(q),\ \Phi_{12}(q),\ \Phi_{12}^\epsilon(q),\ \Phi_{30}(q),$$

$$|\mathbf{N}_{G^*}(\mathcal{T})/T| = 4,\ 6,\ 4,\ 12,\ 30,$$

respectively, where $\epsilon = \pm$ is chosen suitably. As $|T_0| = |T|$, (3) cannot hold.

Next let S be one of the following groups: $\mathrm{B}_n(q)$ or $\mathrm{C}_n(q)$ with $n \geq 3$, or $\mathrm{E}_7(q)$. Following the proof of [MT, Proposition 4.5], one can show that (*) holds with $r_2 = 1$ and $r_1 = r(p, mf)$, and $m = 2n,\ 2n,\ 18$ respectively. Furthermore, $|\Phi| \cdot |\Delta| = f$, and $|T| = q^n + 1,\ q^n + 1$ or $\Phi_2(q)\Phi_{18}(q)$, respectively. Also, $T/T_0 \hookrightarrow C_{\gcd(2,q-1)}$. Hence, if

$S = \mathrm{E}_7(q)$ then $T_3 \neq 1$, contradicting (3). In the remaining cases, $|\mathbf{N}_{G^*}(\mathcal{T})/T| = 2n$, and so (3) cannot hold either.

In the case $S = \mathrm{PSL}_2(q)$ with $q \geq 11$, one can check that (*) holds with $r_2 = 1$, $r_1 = r(p, 2f)$, $|T| = q + 1$, $|\mathbf{N}_{G^*}(\mathcal{T})/T| = 2$. Since $|\Phi| \cdot |\Delta| = f$, we see that (3) is violated.

We are left with the case $S = \mathrm{D}_n(q)$ with $2|n$ and $\Delta = 1$. Following the proof of [MT, Proposition 4.5], one can show that (*) holds with $r_2 = 1$ and $r_1 = r(p, (2n-2)f)$, $|\Phi| \cdot |\Delta| = f$, $|T| = (q+1)(q^{n-1}+1)$, $|T/T_0| \leq \gcd(4, q^n - 1)$, and $|\mathbf{N}_{G^*}(\mathcal{T})/T| = 2n-2$. Again, we can check that (3) cannot hold. ☐

Proposition 2.6. *Let H be an almost simple group with non-abelian simple socle $S = H'$. Suppose that H is an $\mathsf{MV}(g)$-group for some $g \in H$ and S is a simple groups of Lie type in characteristic p. Then $H \cong \mathrm{PSL}_2(5) \cong \mathrm{PSL}_2(4) \cong \mathsf{A}_5$ and $|g| = 5$.*

Proof. **(I) Case 0:** *$S \in \mathcal{S}$ or $S \cong \mathrm{PSL}_2(q)$ with $q = p^f \geq 32$.*

If $S \in \mathcal{S}$, then $H \cong \mathsf{A}_5$ by checking [CCNPW] or [GAP]. So, assume $S \notin \mathcal{S}$. By Proposition 2.5, we may assume that $H \leq \mathrm{Inndiag}(S)$.

Assume that $S \cong \mathrm{PSL}_2(q)$ with $q \geq 32$. We have that $H \cong S$ or $H \cong \mathrm{PGL}_2(q)$. The character tables of $\mathrm{SL}_2(q)$ and $\mathrm{PGL}_2(q)$ can be found in [Do, §38] and [St], respectively. Assume first that $q \geq 32$ is even. Then $H \cong \mathrm{SL}_2(q)$ and the result follows by checking [Do, Theorem 38.2]. So, assume $q > 32$ is odd. By [Do, Theorem 38.1], $\mathrm{SL}_2(q)$ has irreducible characters labeled by χ_i $(1 \leq i \leq (q-3)/2)$ of degree $q+1$ and θ_j $(1 \leq j \leq (q-1)/2)$ of degree $q-1$. Let $\langle z \rangle = \mathbf{Z}(\mathrm{SL}_2(q))$. Then $\chi_i(z) = (-1)^i(q+1)$ and $\theta_j(z) = (-1)^j(q-1)$ and thus if i and j are even, then χ_i and θ_j can be considered to be irreducible characters of $\mathrm{PSL}_2(q)$. By our assumption on q, the characters χ_2, χ_4 and θ_2, θ_4 are irreducible characters of S. We also have that $|g| = p$ or divides $q \pm 1$ for every $g \in S$. If the first case holds, then $\chi_2(g) = 1 = 1_H(g)$. For the latter case, since g is nontrivial, r divides $|g|$ for some prime $r \neq p$. As $|S| = q(q^2-1)/2$, χ_i or θ_i with $i \in \{2, 4\}$ are of r-defect zero and thus there are two distinct irreducible characters of S which vanish at g. Finally, assume that $H \cong \mathrm{PGL}_2(q)$ with $q > 32$ odd. As $H/S \cong C_2$, we have $\mathrm{Irr}(H/S) = \{1_{H/S}, \lambda\}$ with $\lambda(x) = -1$ for $x \in H \setminus S$. Since $g \in H \setminus S$, we have $\lambda(g) = -1$ and also $1_{H/S}(g) = 1$. By [St, §2], the two irreducible characters of H of degree q take values ± 1 on every element lying outside S. Thus H is not an MV-group in this case.

(II) From now on, we may assume that $S \notin \mathcal{S}$ and $S \ncong \mathrm{PSL}_2(q)$. We consider the setup as in Proposition 2.5. Let $\mathcal{G}$ be a simple, simply connected algebraic group defined over a field of characteristic p and a Frobenius morphism $F : \mathcal{G} \to \mathcal{G}$ such that $S = G/\mathbf{Z}(G)$ for $G := \mathcal{G}^F$. Let the pair $(\mathcal{G}^*, F^*)$ be dual to $(\mathcal{G}, F)$ and $G^* := (\mathcal{G}^*)^{F^*}$.

We consider the situation (**) where we can find a prime $r \geq 5$ and a maximal torus $\mathcal{T} \subset \mathcal{G}^*$, such that $\gcd(r, |G^*/[G^*, G^*]|) = 1$ and the following conditions hold

(i) for any semisimple element $s \in \mathcal{T} \cap G^*$ of order r, we have $\mathbf{C}_{\mathcal{G}^*}(s) = \mathcal{T}$.
(ii) $T^* := \mathcal{T} \cap G^*$ and $T := T^* \cap [G^*, G^*] = \langle x \rangle$ is cyclic where x is non-rational.

As mentioned in Proposition 2.5, condition (i) also holds for every semisimple element in $[G^*, G^*]$ whose order is divisible by r, in particular, it holds for all generators of T in condition (ii). Hence the semisimple character χ_x belongs to the Lusztig series defined by $[x]$ can be considered as an irreducible character of S. Now it follows from the proof of [NT1, Lemma 9.1] that if $x \in [G^*, G^*]$ is non-rational whose order is divisible by r and suppose x and x^j are not G^*-conjugate for some integer $j \geq 1$ with $(j, |S|) = 1$, then $\chi_1 := \chi_x$ and $\chi_2 := \chi_{x^j}$ are distinct irreducible characters of S whose fields of values are contained in the cyclotomic field $\mathbb{Q}_k$ with $k = |x|$. (These are called p-rational characters.) Notice that if $g \in S$ is a p-element and suppose $|S| = p^a m$ where $(m, p) = 1$, then $\chi_i(g) \in \mathbb{Q}_m$ (as $|x|$ divides m) and also $\chi_i(g) \in \mathbb{Q}_{p^a}$, so $\chi_i(g) \in \mathbb{Q}_m \cap \mathbb{Q}_{p^a} = \mathbb{Q}$ since $(p^a, m) = 1$, hence $\chi_i(g) \in \mathbb{Q}$. Moreover, $\chi_2 = \chi_1^\sigma$, where $\sigma \in \mathrm{Gal}(\mathbb{Q}_m/\mathbb{Q})$ mapping $e^{\frac{2\pi i}{m}}$ to its j-power. Therefore, $\chi_2(g) = \chi_1(g)^\sigma = \chi_1(g)$ as $\chi_1(g) \in \mathbb{Q}$, and so two distinct irreducible characters $\chi_{1,2}$ of S take the same value at the p-element $g \in S$. This argument will be used in Case 1b below.

In fact, since diagonal automorphisms preserve semisimple characters, χ_1 and χ_2 are $\mathrm{Inndiag}(S)$-invariant.

Case 1: $H = S$.

Case 1a: g is both p-singular and r-singular for some prime $r \neq p$.

We know that the Steinberg character St_S of S vanishes at g. Furthermore, there exists an irreducible character χ of S of r-defect zero (see [Wi, Theorem]) and since g is r-singular, we have $\chi(g) = 0$. As St_S and χ are distinct irreducible characters of S, both vanish at g, H is not an MV-group.

Case 1b: g is a p-element.

Let $\mathcal{T} \leq \mathcal{G}^*$ be a maximal torus, $T^* := \mathcal{T} \cap G^*$ and $T := T^* \cap [G^*, G^*]$. Let $\widetilde{T} \leq G$ be the maximal torus dual to T^*. Since $S \notin \mathcal{S}$, we have $d := |G^*/[G^*, G^*]| = |\mathbf{Z}(G)|$. If $s \in T$ with prime order r where $r \nmid |\mathbf{Z}(G)|$, then $\mathbf{C}_{\mathcal{G}^*}(s)$ is connected, furthermore, there is a unique element $\tilde{s} \in G$ of order r (existence follows by the fact $r = |s|$ is prime to $|\mathbf{Z}(G)|$) whose image in $G/\mathbf{Z}(G)$ is s; and if $\tilde{s}$ is regular, i.e., $\mathbf{C}_G(\tilde{s}) = \widetilde{T}$, then $\mathbf{C}_S(s) = T$. Hence $\mathbf{C}_{G^*}(s) = T^*$ as $G^* = ST^*$ and condition (i) holds.

Assume next that $T = \langle x \rangle$ is cyclic, then $\mathbf{N}_{G^*}(T) = T^*\mathbf{N}_S(T)$ and $\mathbf{C}_{G^*}(T) = T^*$, so $|\mathbf{N}_{G^*}(T)/\mathbf{C}_{G^*}(T)| = |\mathbf{N}_S(T)/T| = |\mathbf{N}_G(\widetilde{T})/\widetilde{T}|$. Hence

$$\text{if } |\mathbf{N}_S(T)/T| = |\mathbf{N}_G(\widetilde{T})/\widetilde{T}| < \phi(|x|), \text{ then } x \text{ is non-rational in } G^*. \tag{4}$$

Let $\mathcal{L}$ be the set consisting of the following simple groups: $\mathrm{PSL}_3(q), \mathrm{PSU}_3(q), \mathrm{PSp}_4(q)$ with q a Mersenne prime or $\mathrm{P}\Omega_{2n}^+(q)$ with $2|n \geq 4$.

Assume first that $S \notin \mathcal{L}$. Then one can find two maximal tori $\mathcal{T}_i \leq \mathcal{G}, i = 1, 2$, such that $T_i := \mathcal{T}_i \cap [G^*, G^*]$ has order given in Tables 3 and 4 (which are Tables II and III in [BPS]). Furthermore, each T_i is cyclic with generator x_i and there exists an integer $m_i > 1$ such that the p.p.d $r_i := r(p, m_i f)$ exists and coprime to d with $d = |\mathbf{Z}(G)|$. Now each x_i is non-rational by checking equation (4) using the bound $|\mathbf{N}_G(\widetilde{T}_i)/\widetilde{T}_i| \leq n$ for classical groups by [BPS, Lemma 4.7] and the upper bound $|\mathbf{N}_S(T_i)/T_i|$ for exceptional groups given in Table 3. This verifies condition (ii).

Let $S = \mathrm{PSL}_n(q)$ with $n \geq 4$. Then $(m_1, m_2) = (n, n-1)$ and the existence of a regular semisimple element $\tilde{s}_i$ of order r_i with $|\mathbf{C}_G(\tilde{s}_i)| = |\widetilde{T}_i|$ is guaranteed by [MoT, Lemma 2.4]. It follows that $\mathbf{C}_{\mathcal{G}^*}(s_i) = \mathcal{T}_i$ as wanted, where s_i is the image of $\tilde{s}_i$ in $S = G/\mathbf{Z}(G)$.

Consider $S = \mathrm{PSU}_n(q)$ with $n \geq 4$. Define $(m_1, m_2) = (n, 2n-2)$ if n is even and $(m_1, m_2) = (2n, n-1)$ if n is odd. By our choices of T_i and r_i, each T_i^* has the property that it is uniquely determined (up to conjugation) by their order. Furthermore, the conjugacy class of maximal tori containing T_i^* is the only classes of maximal tori whose order is divisible by r_i. Arguing as in [M3, Proposition 2.4], let $s_i \in T_i$ be any semisimple element of order r_i. If $\mathbf{C}_{G^*}(s_i)$ is not a torus of G^*, then its semisimple rank is at least 1, hence it contain two maximal tori of different order and both of these must have order divisible by r_i, which is impossible. Hence s_i is regular semisimple and $T_i^* = \mathbf{C}_{G^*}(s_i)$ which verifies (i).

For $S = \mathrm{PSp}_n(q), n \geq 4, \Omega_n(q), n \geq 7$ odd, q odd, $\mathrm{P}\Omega_n^-(q), n \geq 8$ even and $\mathrm{P}\Omega_n^+(q), n \geq 10, n \equiv 2 \pmod 4$, the same argument applies as above with $(m_1, m_2) = (n, n/2), (n-1, (n-1)/2), (n, n-2)$ and $(n, n-2)$, respectively.

Let $S = {}^2\mathrm{B}_2(q), {}^2\mathrm{G}_2(q), {}^2\mathrm{F}_4(q)$ with $q = p^{2m+1}, m \geq 1$ and $p = 2, 3, 2$, respectively. Then $G^* = S = G$ as $S \notin \mathcal{S}$. Let $m_1 = m_2 = 4, 6, 12$. Then each prime divisor of $|T_i|$ is a p.p.d of $p^{m_i f} - 1$, where $f = 2m+1$, by [BPS, Lemma 3.3]. Hence we can choose $r_i = r(p, m_i f) > 3$ and by [BPS, Theorem 3.1], every semisimple element in T_i of order r_i is regular and $\mathbf{C}_{G^*}(s_i) = T_i^*$ is a torus. The same argument applies to $\mathrm{E}_8(q)$ with $(m_1, m_2) = (15, 30)$.

Let $S = {}^3\mathrm{D}_4(q)$. We can take $m_1 = 12$ and $m_2 = 3$. By [BPS, Theorem 3.1], every semisimple element $s_1 \in T_1$ of order $r_1 = r(p, 12f)$ is regular and $\mathbf{C}_{G^*}(s_1) = T_1^*$. Let $2 < k \mid q+1$ and $3 < r_2 = r(p, 3f) \mid q^2 + q + 1$, as in the proof of [BPS, Theorem 3.4] T_2 has a regular semisimple element s of order kr_2. Hence T_2 has a regular semisimple element $s_2 = s^k$ of order r_2. The same argument applies to $\mathrm{E}_7(q), \mathrm{F}_4(q), \mathrm{E}_6(q), {}^2\mathrm{E}_6(q)$ with $(m_1, m_2) = (7, 14), (6, 3), (9, 8), (18, 8)$.

Finally, let $S = \mathrm{G}_2(q), q \geq 5$. We can choose $(m_1, m_2) = (3, 6)$ and the result follows by applying [MoT, Lemma 2.3].

For $S \in \mathcal{L}$, the same argument as above applies if one can find a maximal cyclic torus satisfying the required properties. Consider $S = \mathrm{PSL}_3(q), \mathrm{PSU}_3(q)$ or $\mathrm{PSp}_4(q)$ with q a Mersenne prime. Then $G = \mathrm{SL}_3(q), \mathrm{SU}_3(q)$ or $\mathrm{Sp}_4(q)$ and $|\mathbf{Z}(G)| = |[G^*/[G^*, G^*]]| = d \leq 3$. By our assumption on q, the p.p.d $r = r(p, m) > 3$ exists with $m = 3, 6$ and 4, respectively so $(r, d) = 1$ and $\mathcal{G}^*$ has a maximal torus $\mathcal{T}$ such that $|T| = |\mathcal{T} \cap [G^*, G^*]| = |T_1|$ as given in Table 4 and moreover $T = \langle x \rangle$ is cyclic. By [BPS, Lemma 4.6], we have $\mathbf{C}_G(s) = \widetilde{T}$ for every $s \in \widetilde{T}$ with $|s| = r$. Therefore, condition (i) holds. From [BPS, Lemma 4.7], we have that $|\mathbf{N}_G(\widetilde{T})/\widetilde{T}| \leq n$, with $n = 3, 3, 4$, respectively. Now it remains to check that $\phi(|x|) > n$. For example, assume that $S = \mathrm{PSL}_3(q)$. Then $|x| = (q^2 + q + 1)/d$ with $d = (3, q-1)$ and $n = 3$. Since $(q^2 + q + 1)/d$ is always odd, Lemma 2.4 yields that $\phi(|x|) \geq \sqrt{|x|}$ and thus, it suffices to show that $|x| > 9$ or equivalently $q^2+q+1>9d$ with $q\geq 11$ as $S\notin\mathcal{S}$. Now it is routine to check that the latter inequality holds whenever $q\geq 11$. Hence (**) holds and so we can produce two distinct irreducible characters of H which take the same value at the p-element g, hence H is not an MV-group.

Finally, assume $S\cong \mathrm{P}\Omega_n^+(q)$ with $8\leq n\equiv 0 \pmod 4$. Let $T=\mathcal{T}^F$ be a maximal torus of G and let $\theta_{1,2}\in \mathrm{Irr}(T)$. By [Ca, Corollary 7.2.9],

$$R_{T,\theta_1}(1)=R_{T,\theta_2}(1),\ R_{T,\theta_1}(g)=R_{T,\theta_2}(g),$$

where R_{T,θ_i} is the Deligne-Lusztig generalized character associated to T and θ_i. Assume furthermore that both $\theta_{1,2}$ are trivial at $\mathbf{Z}(G)$ (note that $\mathbf{Z}(G)\leq T$) and in general position. Then there is a sign $\epsilon=\pm$ such that the characters $\epsilon R_{T,\theta_i}$ of G are irreducible, trivial at $\mathbf{Z}(G)$, and take the same value at g. Hence, to rule out this case, it suffices to show there are at least two $\mathbf{N}_G(\mathcal{T})/T$-orbits on the irreducible characters of T that are in general position and trivial at $\mathbf{Z}(G)$.

Now we apply the above argument to the torus T such that $T/\mathbf{Z}(G)\cong T_2$ with T_2 given in [BPS, Table VI], in particular $|T_2|=(q^{n/2-1}+1)(q+1)/(4,q-1)^2$. Since $(n,q)\neq(8,2)$, the p.p.d $r=r(p,(n-2)f)$ exists. It is straightforward to check that if $\theta\in\mathrm{Irr}(T)$ is of order divisible by r and trivial at $\mathbf{Z}(G)$, then θ is in general position; furthermore, there are at least two $\mathbf{N}_G(\mathcal{T})/T$-orbits of such characters. Hence we are done in this case. (Note that this argument can be applied to simple groups not of type D_{2m} as well. However, we have handled them using the set-up (**) since this set-up will be useful in subsequent cases considered below.)

Case 1c: g is a p'-element.

Assume at first that $S\notin\mathcal{L}$. Assume the same setup as in the proof of Case 1b. Direct calculation shows that $(|T_1|,|T_2|)=1$. Hence, $|g|$ is coprime to $|T_k|$ for some $k=1,2$ and thus $g^S\cap T_k=\emptyset$. Since $G^*=ST_k^*=T_k^*S$ with $S\cap T_k^*=T_k$ and T_k^* is abelian, we deduce that $g^{G^*}\cap T_k^*=\emptyset$ and thus the two irreducible characters $\chi_i, i=1,2$ of S constructed in Case 1b with respect to the cyclic maximal torus $T_k=\langle x_k\rangle$, with x_k a non-rational element, vanish at g, so H is not an MV-group.

Consider $S=\mathrm{PSL}_3(q),\mathrm{PSU}_3(q)$ or $\mathrm{PSp}_4(q)$ with q a Mersenne prime. As in the proof of Case 1b, there exists a maximal torus T^* of G^* of order q^2+q+1, q^2-q+1, and q^2+1, respectively. If $T\cap g^S=\emptyset$, then H is not an MV-group as in the previous case. So, without loss of generality, one can assume $g\in T$ with $|T|=(q^2+q+1)/d,(q^2-q+1)/d$ and $(q^2+1)/d$. Since g is nontrivial, let r be a prime divisor of $|g|$. Then r divides $|T|$. From [SF], $\mathrm{PSL}_3^\epsilon(q)$ has at least two distinct irreducible characters whose degree is divisible by $q^2+\epsilon q+1$ and thus they are of r-defect zero and hence they both vanish at g. Finally, if $S\cong\mathrm{PSp}_4(q)$, then $G^*=(C_2)_{\mathrm{ad}}(q)$ and it has four distinct unipotent characters of the same degree $q(q^2+1)/2$ which are of r-defect zero (see [Ca, 13.8]). These unipotent characters when restricted to S remain irreducible and are unipotent characters of S (see [M2]) and since $|G^*:S|=2$, S has two distinct unipotent characters of degree $q(q^2+1)/2$ which are of r-defect zero so they both vanish at g.

Assume $S \cong \mathrm{P}\Omega^+_{2n}(q)$ with $2|n \geq 4$ and $q = p^f$ (note that $(n,q) \neq (4,2)$ as $S \notin \mathcal{S}$). Assume furthermore that (any inverse image of) g (in G) does not belong to a maximal torus T^- of G of order $(q+1)(q^{n-1}+1)$. Fix a prime $r_- = r(p,(2n-2)f)$. Then for any semisimple element $s \in [G^*,G^*]$ of order divisible by r_-, the corresponding semisimple character χ_s of G is trivial at s. Furthermore, $\chi_s(g) = 0$ (see for instance the arguments at the end of p. 1 of the proof of [MT, Proposition 4.5]). Moreover, arguing as in (iii) of the proof of Proposition 2.5 one can show that there are at least two G^*-classes of such s, and so at least two such characters vanish at g, a contradiction. The same arguments apply to a maximal torus T^+ of G of order $(q-1)(q^{n-1}-1)$ and $r_+ = r(p,(n-1)f)$. We have shown that g belongs to a conjugate of T^+ and to a conjugate of T^-. In this case, the proof of [GT, Lemma 2.2] shows that $g = 1$, which is impossible.

Case 2: $S < H \leq J := \mathrm{Inndiag}(S)$.

Case 2a: g is p-singular.

The Steinberg character St_S of S extends to H which will be denoted by St_H. Since $|H:S|$ is coprime to p, $\mathrm{St}_H \in \mathrm{Irr}(H)$ is of p-defect zero and thus vanishes at g. By Gallagher's Theorem, $\mathrm{St}_H \neq \lambda\mathrm{St}_H \in \mathrm{Irr}(H)$ and vanishes at g where λ is any nontrivial linear character of H/S.

Case 2b: g is a p'-element.

By assumption, $e := |H:S| > 1$ divides $d := |J/S|$. Thus we need only consider $S = \mathrm{PSL}^\epsilon_n(q)$, $\Omega_{2n+1}(q)$, $\mathrm{PSp}_{2n}(q)$, $\mathrm{P}\Omega^\epsilon_{2n}(q)$, $\mathrm{E}^\epsilon_6(q)$, and $\mathrm{E}_7(q)$, with $d = (n, q-\epsilon 1)$, 2, $(2,q-1)$, $(4,q^n-\epsilon 1)$, $(3,q-\epsilon 1)$, or $(2,q-1)$. In particular, q is odd for all but types PSL^ϵ_n and E^ϵ_6, and $q \neq 2$ if $S = \mathrm{E}^\epsilon_6(q)$ (as $S \notin \mathcal{S}$).

Consider the case $S \notin \mathcal{L}$ or S is of type D_{2m} with $m \geq 2$. For all but types D_{2m} and E_7, we again look at the two cyclic tori $T_{1,2} \leq [G^*,G^*]$ constructed in Case 1b. If S is of type D_{2m}, we consider maximal tori T^*_1 of order $(q^{m-1}+1)(q+1)$ and T^*_2 of order $(q^{m-1}-1)(q-1)$ in G^*. If S is of type E_7, we consider maximal tori T^*_1 of order $\Phi_1(q)\Phi_7(q)$ and T^*_2 of order $\Phi_2(q)\Phi_{18}(q)$ in G^*. By their construction, each T_i contains a regular semisimple element s_i of prime order r_i with $\mathbf{C}_{G^*}(s_i) = T^*_i$, giving rise to an irreducible character χ_i of S. As mentioned above, these two characters are J-invariant. Let $\theta_i \in \mathrm{Irr}(J)$ lying above χ_i. Note that J/S is cyclic, unless S is of type D_{2m} in which case $J/S \cong C^2_2$. So we can write $\theta_i(1) = a_i\chi_i(1)$, where either $a_i = 1$, or $a_i = 2$ and S is of type D_{2m}. Also, $\chi_i(1) = [G^*:T^*_i]_{p'}$, $|G^*| = |J|$, and $J \cong (\mathcal{G}/\mathbf{Z}(\mathcal{G}))^F$ with $\mathcal{G}/\mathbf{Z}(\mathcal{G})$ being of adjoint type. Thus any semisimple element in the dual group J^* of J has connected centralizer in the underlying algebraic group. Suppose that θ_i belongs to the rational Lusztig series labeled by the semisimple element $t_i \in J^*$ and corresponds to the unipotent character ψ_i of $\mathbf{C}_{J^*}(s_i)$. As shown in [M1, §6.7], the condition $\theta_i(1)$ is coprime to p and our assumption on q imply that ψ_i is the principal character of $\mathbf{C}_{J^*}(t_i)$ and so θ_i is the semisimple character labeled by t_i. It follows that $|\mathbf{C}_{J^*}(t_i)|_{p'} = |T^*_i|/a_i$. On the other hand, $\mathbf{C}_{J^*}(t_i)$ contains a maximal torus of J^*. Comparing the order of tori in question, we see that $a_i = 1$ and in fact $\mathbf{C}_{J^*}(t_i)$ is a maximal torus of order $|T^*_i|$. In particular, χ_i extends to $\vartheta_i := (\theta_i)_H$.

Now we show there must be some $i \in \{1,2\}$ such that $\vartheta_i(g) = 0$. By Gallagher's theorem, $\vartheta_i\gamma$ belong to $\mathrm{Irr}(H)$ and vanish at g for all $\gamma \in \mathrm{Irr}(H/S)$, yielding a contradiction. Assume the contrary: $\theta_i(g) \neq 0$ for both $i = 1,2$. Arguing as in p. 1 of the proof of [MT, Proposition 4.5], we see that g belongs to two maximal tori T_1' and T_2' of J with $|T_i'| = |T_i^*|$ for $i = 1,2$; in particular, $|\mathbf{C}_J(g)|$ is divisible by both $|T_1^*|$ and $T_2^*|$ for the semisimple element $1 \neq g \in J$. This is however impossible for S of types E_6^ϵ and E_7 by the proof of [LM, Theorem 10.1]. This is also impossible for classical groups as $T_1^* \cap T_2^* = 1$, cf. [MSW, §2], [LST, §2], and [GT, Lemma 2.2].

Finally, for $S \cong \mathrm{PSL}_3^\epsilon(q)$ or $\mathrm{PSp}_4(q)$ with q a Mersenne prime, we can argue as above using the maximal torus in Case 1c and deduce that $g \in T^*$. If $H = \mathrm{PGL}_3(q)$, then by [St], g belongs to the class labeled by C_1 and H has two irreducible characters of degree q^2+q+1 and $q(q^2+q+1)$ both vanish at g. If $S = \mathrm{PSU}_3(q)$, then $q+1 = 2^r$ for some prime r and thus $3 \nmid (q+1)$. So, this case cannot happen. Finally, assume $S = \mathrm{PSp}_4(q)$ with q a Mersenne prime. Inspecting [Sr], we see that g fuses two irreducible characters of degree $(q^2+1)/2$ and two other of degree $q^2(q^2+1)/2$ of S, a contradiction. □

We are now ready to prove our main result.

Proof of Theorem A. From Table 1, if $G \cong \mathsf{A}_5$, then G is an $\mathsf{MV}(g)$-group if and only if $|g| = 5$. Let G be a finite nonsolvable $\mathsf{MV}(g)$-group for some $g \in G$. We claim that $G \cong \mathsf{A}_5$ and the result follows. So, assume that G is an $\mathsf{MV}(g)$-group for some $g \in G$ but $G \ncong \mathsf{A}_5$ and choose G with $|G|$ minimal. By Proposition 2.2(iii), G is almost simple with nonabelian simple socle G'. By Proposition 2.3, G' is not a sporadic group, the Tits group nor an alternating group of degree at least 5. Furthermore, G' is not a simple group of Lie type by Proposition 2.6. We now obtain a contradiction by invoking the classification of finite simple group. □

References

[BPS] L. Babai, P.P. Pálfy, and J. Saxl, On the number of p-regular elements in finite simple groups, *LMS J. Comput. Math.* **12** (2009), 82–119.

[BCH] Y. Berkovich, D. Chillag, and M. Herzog, Finite groups in which the degrees of the nonlinear irreducible characters are distinct, *Proc. Amer. Math. Soc.* **115** (1992), 955–959.

[BCG] M. Bianchi, D. Chillag, and A. Gillio, Finite groups with many values in a column or a row of the character table, *Publ. Math. Debrecen* **69** (2006), 281–290.

[BCLP] M. Bianchi, D. Chillag, M.L. Lewis, and E. Pacifici, Character degree graphs that are complete graphs, *Proc. Amer. Math. Soc.* **135** (2007), 671–676.

[BT] T.C. Burness and H.P. Tong-Viet, Derangements in primitive permutation groups, with an application to character theory, *Quart. J. Math.* (to appear), DOI:10.1093/qmath/hau020.

[Ca] R. W. Carter, *Finite Groups of Lie Type. Conjugacy Classes and Complex Characters,* Pure Appl. Math., Wiley-Interscience/John Wiley and Sons, New York, 1985.

[CCNPW] 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.

[DM] F. Digne and J. Michel, *Representations of Finite Groups of Lie Type,* London Mathematical Society Student Texts **21**, Cambridge University Press (1991).

[DNPST] S. Dolfi, G. Navarro, E. Pacifici, L. Sanus, and P.H. Tiep, Non-vanishing elements of finite groups, *J. Algebra* **323** (2010), 540–545.

[Do] L. Dornhoff, *Group Representation Theory. Part A: Ordinary Representation Theory,* Pure and Applied Mathematics **7**, Marcel Dekker, Inc., New York, 1971.

[FS] W. Feit and G.M. Seitz, On finite rational groups, *Ill. J. Math.* **33** (1989) 103–131.

[GAP] The GAP Group, GAP - Groups, Algorithms, and Programming, Version 4.4.10, 2007. `http://www.gap-system.org.`

[GLS] D. Gorenstein, R. Lyons, and R.M. Solomon, *The classification of the finite simple groups. Number 3. Part I. Chapter A. Almost simple K-groups,* Mathematical Surveys and Monographs, 40.3. American Mathematical Society, Providence, RI, 1998.

[GT] R.M. Guralnick and P.H. Tiep, Effective results on the Waring problem for finite simple groups, (submitted).

[Is] M. Isaacs, *Character Theory of Finite Groups,* AMS Chelsea Publishing, Providence, RI, 2006.

[INW] I.M. Isaacs, G. Navarro, and T. Wolf, Finite group elements where no irreducible character vanishes, *J. Algebra* **222** (1999), 413–423.

[JK] G. James and A. Kerber, *The Representation Theory of the Symmetric Group,* Encyclopedia of Mathematics and its Applications, **16** Addison-Wesley Publishing Co., Reading, Mass., 1981.

[LST] M. Larsen, A. Shalev, and P.H. Tiep, The Waring problem for finite simple groups, *Ann. of Math.* (2) **174** (2011), 1885–1950.

[LW] M.L. Lewis and D.L. White, Connectedness of degree graphs of nonsolvable groups, *J. Algebra* **266** (2003), 51–76.

[LM] F. Lübeck and G. Malle, $(2,3)$-generation of exceptional groups, *J. London Math. Soc.* **59** (1999), 109–122.

[M1] G. Malle, Height 0 characters of finite groups of Lie type, *Represent. Theory* **11** (2007), 192–220.

[M2] G. Malle, Extensions of unipotent characters and the inductive McKay condition, *J. Algebra* **320** (2008), 2963–2980.

[M3] G. Malle, Zeros of Brauer characters and the defect zero graph, *J. Group Theory* **13** (2010), 171–187.

[MSW] G. Malle, J. Saxl, and T. Weigel, Generation of classical groups, *Geom. Dedicata* 49 (1994), 85–116.

[MT] S. Marinelli and P.H. Tiep, Zeros of real irreducible characters of finite groups, *Algebra Number Theory* **7** (2013), 567–593.

[MoT] A. Moretó and P.H. Tiep, Prime divisors of character degrees, *J. Group Theory* **11** (2008), 341–356.

[NT1] G. Navarro and P.H. Tiep, Rational irreducible characters and rational conjugacy classes in finite groups, *Trans. Amer. Math. Soc.* **360** (2008), 2443–2465.

[NT2] G. Navarro and P.H. Tiep, Characters of relative p'-degree over normal subgroups, *Annals of Math.* **178** (2013), 1135–1171.

[QZ] G.H. Qian and Y.X. Zhu, Solvable groups admitting an element on which distinct irreducible characters take distinct values, *Chinese Ann. Math. Ser. A* **26** (2005), 1–6; translation in *Chinese J. Contemp. Math.* **26** (2005), 1–8.

[SF] W.A. Simpson and J.S. Frame, The character tables for $\mathrm{SL}(3,q)$, $\mathrm{SU}(3,q^2)$, $\mathrm{PSL}(3,q)$, $\mathrm{PSU}(3,q^2)$, *Canad. J. Math.* **25** (1973), 486–494.

[Sr] B. Srinivasan, The characters of the finite symplectic group $Sp(4,q)$, *Trans. Amer. Math. Soc.* **131** (1968), 488–525.

[St] R. Steinberg, The representations of $\mathrm{GL}(3,q), \mathrm{GL}(4,q), \mathrm{PGL}(3,q)$, and $\mathrm{PGL}(4,q)$, *Canad. J. Math.* **3** (1951), 225–235.

[Wi] W. Willems, Blocks of defect zero in finite simple groups of Lie type, *J. Algebra* **113** (1988), 511–522.

[Zs] K. Zsigmondy, Zur Theorie der Potenzreste, *Monatsh. Math. Phys.* **3** (1892), 265–284.

Department of Mathematics, University of Arizona, Tucson, AZ 85721, USA
E-mail address: tiep@math.arizona.edu

Fakultät für Mathematik, Universität Bielefeld, Postfach 10 01 31, D-33501 Bielefeld, Germany
E-mail address: ptongviet@math.uni-bielefeld.de