



ELSEVIER

Contents lists available at SciVerse ScienceDirect

Journal of Algebra

[www.elsevier.com/locate/jalgebra](http://www.elsevier.com/locate/jalgebra)



# Further solvable analogues of the Baer–Suzuki theorem and generation of nonsolvable groups

Simon Guest<sup>1</sup>

Department of Mathematics, Baylor University, Waco, TX 76798, USA

## ARTICLE INFO

### Article history:

Received 11 December 2010

Available online 6 April 2012

Communicated by Martin Liebeck

### Keywords:

Solvable radical

Generation by conjugates

## ABSTRACT

Let  $G$  be an almost simple group. We prove that if  $x \in G$  has prime order  $p \geq 5$ , then there exists an involution  $y$  such that  $\langle x, y \rangle$  is not solvable. Also, if  $x$  is an involution then there exist three conjugates of  $x$  that generate a nonsolvable group, unless  $x$  belongs to a short list of exceptions, which are described explicitly. We also prove that if  $x$  has order 6 or 9, then there exist two conjugates that generate a nonsolvable group.

© 2012 Elsevier Inc. All rights reserved.

## 1. Introduction

The following theorem is proved in [Gue10], and provides a solvable analogue of the classical Baer–Suzuki theorem for elements of certain orders.

**Theorem 1.1.** *Let  $G$  be a finite group and suppose that  $x$  is an element of prime order  $p$  where  $p \geq 5$ . Then  $x$  is contained in the solvable radical of  $G$  if and only if  $\langle x, x^g \rangle$  is solvable for all  $g \in G$ . In other words, if  $x$  is not contained in the solvable radical of  $G$  then there exists  $g \in G$  such that  $\langle x, x^g \rangle$  is not solvable.*

The proof of Theorem 1.1 is by induction, and it is shown that a minimal counterexample to Theorem 1.1 would have to be an almost simple group. Theorem 1.1 is then proved (in [Gue10]) with the following result for almost simple groups.

**Theorem 1.2.** *Let  $G$  be an almost simple group with socle  $G_0$ . Let  $x \in G$  have odd prime order  $p$ . Then one of the following holds.*

E-mail address: [simon\\_guest@baylor.edu](mailto:simon_guest@baylor.edu).

<sup>1</sup> Current address: School of Mathematics, University of Southampton, Southampton, SO17 1BJ, UK.

- (1) There exists  $g \in G$  such that  $\langle x, x^g \rangle$  is not solvable;
- (2)  $p = 3$  and  $x$  is a long root element in a simple group of Lie type defined over  $\mathbb{F}_3$ ,  $x$  is a short root element in  $G_2(3)$ , or  $x$  is a pseudoreflection and  $G_0 \cong \text{PSU}_d(2)$ .

In this paper, we prove a result that is quite similar to Theorem 1.2.

**Theorem 1.3.** *Suppose that the finite group  $G$  is not solvable and satisfies one of the following conditions:*

- (1)  $G$  is almost simple;
- (2)  $\text{SL}_d(q) \leq G \leq \text{GL}_d(q)$  or  $\text{SU}_d(q) \leq G \leq \text{GU}_d(q)$ , and if  $d = 2$  and  $q$  is odd, then  $\text{SL}_2(q)$  or  $\text{SU}_2(q)$  has even index in  $G$ ;
- (3)  $G \cong K/Z$ , where  $Z \leq Z(K)$ ,  $K$  is the universal version of a group of Lie type,  $K/Z(K)$  is simple and  $G \not\cong \text{SL}_2(q)$  ( $q$  odd).

*If  $x \in G$  has prime order  $p \geq 5$  in  $G/Z(G)$ , then there exists an involution  $y \in G$  such that  $\langle x, y \rangle$  is not solvable.*

Following [Ste68] (see also [GLS98, 2.2.6]), we refer to the groups  $K/Z$  in part (3) of Theorem 1.3 as finite groups of Lie type. We note that if  $p \geq 5$  and  $G$  is almost simple, then Theorem 1.3 shows that there exists an involution  $y$  such that  $\langle x, x^y \rangle$  is not solvable. For  $\langle x, x^y \rangle$  has index 1 or 2 in  $\langle x, y \rangle$  and so either both groups are solvable, or both of them are not solvable. Also, Theorem 1.2 shows that when the order of  $x$  has a prime divisor  $p \geq 5$  and  $G$  is almost simple, there exist two conjugates that generate a nonsolvable group. In this paper we prove an analogous result for elements of order divisible by 3.

**Theorem 1.4.** *Suppose that  $G$  is an almost simple group and that  $x$  has order 6 or 9. Then there exists an element  $g \in G$  such that  $\langle x, x^g \rangle$  is not solvable.*

Theorems 1.2 and 1.4 yield the following corollary immediately.

**Corollary 1.5.** *Let  $G$  be an almost simple group with socle  $G_0$  and suppose that  $x$  in  $G$  is not a 2-element. Then there exists  $g$  in  $G$  such that  $\langle x, x^g \rangle$  is not solvable or  $x$  has order 3 and  $x$  is a long root element in a simple group of Lie type defined over  $\mathbb{F}_3$ , a pseudoreflection in  $\text{PGU}_d(2)$  or a short root element in  $G_2(3)$ . Moreover, there exist three conjugates of  $x$  that generate a nonsolvable group unless  $G_0 \cong \text{PSU}_d(2)$  or  $\text{PSP}_d(3)$ .*

Guralnick, Flavell, and the author prove in [FGG10] that for all nontrivial elements  $x$  in a finite (or linear) group  $G$ ,  $x$  is contained in the solvable radical of  $G$  if and only if any four conjugates of  $x$  generate a solvable group. In particular, if  $x$  is contained in an almost simple group  $G$ , then there exist four conjugates of  $x$  that generate a nonsolvable group (this result and Theorem 1.1 are obtained independently by Gordeev, Grunwald, Kunyavski, and Plotkin in [GGKP10]). Thus, if we allow  $x$  to be a 2-element, then a similar result to Corollary 1.5 is true but with four conjugates of  $x$ . Corollary 1.5 and Theorem 1.6 show that in most cases, there exist three conjugates of  $x$  that generate a nonsolvable group.

**Theorem 1.6.** *Let  $G$  be an almost simple group with socle  $G_0$  and  $x$  an involution in  $G$ . Then either there exist  $g_1, g_2 \in G$  such that  $\langle x, x^{g_1}, x^{g_2} \rangle$  is not solvable or  $(x, G_0)$  belongs to Table 1.*

We note that if  $x$  is an involution, then  $\langle x, x^g \rangle$  is dihedral and so we need at least three conjugate involutions to generate a nonsolvable group.

In a future work, the author hopes to improve Corollary 1.5 to find the minimal number of conjugates in an almost simple group required to generate a nonsolvable group for 2-elements as well. This requires a proof that for an element of order 4, there exist two conjugates that generate a nonsolvable group with a short list of exceptions, and that two conjugates always suffice for an element of order 8.

**Table 1**

Pairs  $(x, G_0)$  such that any three conjugates of  $x$  in  $\text{Aut}(G_0)$  generate a solvable group.

$G_0$	$x$
$A_n$	transposition
$A_6$	triple transposition
$\text{PSU}_d(2)$	unitary transvection
$\text{PSU}_4(2) \cong \text{PS}\Omega_5(3)$	graph automorphism
$\text{PSL}_4(2) \cong A_8$	graph automorphism
$\text{P}\Omega_d^\pm(2), d \text{ even}$	orthogonal transvection
$\text{PSp}_d(2) \cong \text{PS}\Omega_{d+1}(2)$	symplectic transvection
$\text{P}\Omega_d(3), d \text{ odd}$	reflection
$F_{i22}$	$x$ in class 2A
$F_{i23}$	$x$ in class 2A
$F'_{i24}$	$x$ in class 2C in $F'_{i24} : 2$

Also, using Lemma 2.1 below, we obtain the following corollary to Theorem 1.6.

**Corollary 1.7.** *Let  $G$  be a finite group with trivial Fitting subgroup and let  $x$  be an involution in  $G$ . If  $\langle x, x^{g_1}, x^{g_2} \rangle$  is solvable for all  $g_1, g_2 \in G$ , then for every component  $L$  of  $G$  we have  $x \in N_G(L)$  and either  $x \in C_G(L)$  or  $L$  and the image of  $x \in \text{Aut}(L)$  appear in Table 1.*

## 2. Preliminaries

Throughout the paper, we will use the notation  $L_d^\epsilon(q)$  to denote  $\text{PSL}_d(q)$  when  $\epsilon = +$  and  $\text{PSU}_d(q)$  when  $\epsilon = -$ . Similarly,  $D_n^\epsilon(q)$  will refer to  $D_n(q)$  and  ${}^2D_n(q)$  and  $E_6^\epsilon(q)$  will refer to  $E_6(q)$  and  ${}^2E_6(q)$  for  $\epsilon = +$  and  $\epsilon = -$  respectively.

Lemma 2.1 below relies on the result of Aschbacher and Guralnick [AG84] that every finite simple group is 2-generated. Corollary 1.7 follows immediately from Theorem 1.6 and Lemma 2.1.

**Lemma 2.1.** *Let  $G$  be a finite group with trivial Fitting subgroup. Let  $L$  be a component of  $G$  and suppose that  $x \notin N_G(L)$ . Then there exist  $g_1, g_2 \in G$  such that  $\langle x, x^{g_1}, x^{g_2} \rangle$  is not solvable.*

**Proof.** See [Gue10, Lemma 1].  $\square$

**Lemma 2.2.** *Let  $G_0$  be a simple group of Lie type, suppose  $G_0 \triangleleft G \leq \text{Inndiag}(G_0)$  and let  $x \in G$ .*

- If  $x$  is unipotent, let  $P_1$  and  $P_2$  be distinct maximal parabolic subgroups containing a common Borel subgroup of  $G$ , with unipotent radicals  $U_1$  and  $U_2$ . Then  $x$  is conjugate to an element of  $P_i \setminus U_i$  for  $i = 1$  or  $i = 2$ .*
- If  $x$  is semisimple, assume that  $x$  lies in a parabolic subgroup of  $G$ . If the rank of  $G_0$  is at least 2, then there exists a maximal parabolic subgroup  $P$  with a Levi complement  $J$  such that  $x$  is conjugate to an element of  $J$  not centralized by any (possibly solvable) Levi component of  $J$ .*

**Proof.** See [GS03, Lemma 2.2].  $\square$

## 3. Proof of Theorem 1.3

Let  $(x, G)$  be a minimal counterexample. If  $G$  is almost simple, then let  $G_0$  be the simple group satisfying  $G_0 \triangleleft G \leq \text{Aut}(G_0)$ .

**Lemma 3.1.** *If  $G$  is almost simple and  $G_0 \cong A_n$ , then  $(x, G)$  is not a minimal counterexample.*

**Proof.** Since  $x$  has odd order  $p$ , it must lie in  $A_n$ . It suffices to assume that  $x = (12 \cdots p) \in A_p$ . If we let  $y = (12)(34)$ , then  $\langle x, y \rangle = A_p$ , which is not solvable.  $\square$

### Lemma 3.2.

- (a) If  $x \in G \leq \text{PGL}_d^\epsilon(q)$  does not lift to an element of order  $p$  in  $\text{GL}_d(q)$ , then  $(x, G)$  is not a minimal counterexample.  
 (b) If  $Z(G) \neq \{1\}$ , then we may assume that  $x \in G$  has order  $p$ .

**Proof.** To prove (a), note that if  $x$  does not lift to an element of order  $p$  in  $\text{GL}_d^\epsilon(q)$ , then  $p \mid (q - \epsilon, d)$  and the natural  $\langle x \rangle$ -module  $V$  decomposes into  $p$ -dimensional spaces (see [Bur07, Lemma 3.11] for example). It therefore suffices to assume that  $d = p$  and  $x$  acts irreducibly on the natural module  $V$  since  $(x, G)$  is a minimal counterexample. Under these conditions on  $d$ ,  $p$  and  $q$ , a Sylow  $p$ -subgroup of  $\text{GL}_d^\epsilon(q)$  is contained in a type  $(q - \epsilon)_p$  subgroup. The irreducibility of  $x$  implies that  $x$  is nontrivial in  $S_p$ , and we can take an involution  $y \in \text{SL}_p^\epsilon(q)$  that induces any involution in  $S_p$ ; thus  $(x, G)$  cannot be a minimal counterexample.

To prove (b), if  $\text{SL}_d^\epsilon(q) \leq G \leq \text{GL}_d^\epsilon(q)$ , then consider  $x \in G/Z(G) \leq \text{PGL}_d^\epsilon(q)$ . If  $x$  does not lift to an element of order  $p$  in  $G$ , then the same argument as for part (a) shows that there exists an involution  $y \in \text{SL}_d^\epsilon(q)$  such that  $\langle x, y \rangle$  is not solvable. In all other cases,  $p$  does not divide  $|Z(G)|$ , so  $x' = x^{|Z(G)|}$  will have order  $p$  in  $G$  and  $(x', G)$  will also be a minimal counterexample to Theorem 1.3.  $\square$

**Lemma 3.3.** If  $\text{PSL}_2(q) \leq G \leq \text{Aut}(\text{PSL}_2(q))$  or  $\text{SL}_2^\epsilon(q) \not\leq G \leq \text{GL}_2^\epsilon(q)$  with  $[G : \text{SL}_2^\epsilon(q)]$  even, then  $(x, G)$  cannot be a minimal counterexample.

**Proof.** First note that if  $\text{PSL}_2(q) \leq G \leq \text{Aut}(\text{PSL}_2(q))$ , then the order of  $x$  implies that  $x$  is either in  $\text{PSL}_2(q)$ , or it is a field automorphism. In this case, we may assume that  $q \geq 7$  since we have eliminated the case that  $A_n \leq G \leq \text{Aut}(A_n)$ . First, let us assume that  $x \in \text{PSL}_2(q)$ .

If  $p \mid q$ , then  $x \in \text{PSL}_2(q)$  is a transvection, and there is only one  $\text{PGL}_2(q)$ -class of transvections so we may assume that  $x = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ . Now let  $y = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ ; it follows that  $\langle x, x^y \rangle = \text{PSL}_2(p)$ , which is not solvable.

If  $x$  is semisimple in  $\text{PSL}_2(q)$ , then either  $p \mid q + 1$  or  $p \mid q - 1$ . Suppose first that  $p \mid q + 1$ . Then consider the possibilities for the maximal subgroups of  $\text{PSL}_2(q)$  containing  $x$ . Since  $(x, G)$  is a minimal counterexample,  $x$  cannot be contained in  $A_5$ , and it cannot be contained in  $A_4$  or  $S_4$  since  $p \geq 5$ . Moreover,  $x$  cannot be contained in a subfield subgroup since, because of the order of  $x$ , any such subfield subgroup would be almost simple. So  $x$  can only be contained in a dihedral group  $D$  of order  $\frac{2(q+1)}{(2, q-1)}$ . It can be contained in only one dihedral subgroup since  $C_G(x)$  is the cyclic subgroup of  $D$  of order  $\frac{q+1}{(2, q-1)}$ . So, let  $y$  be an involution in  $G$  that is not contained in  $D$ .

Now suppose that  $p \mid q - 1$ . The possible maximal subgroups containing  $x$  are a dihedral group  $D$  of order  $\frac{2(q-1)}{(2, q-1)}$  and (at most two) Borel subgroups. Let  $i_2(H)$  denote the number of involutions in a group  $H$ . Then

$$i_2(G) \geq \begin{cases} q^2 - 1 & \text{for } q \text{ even;} \\ q(q-1)/2 & \text{for } q \text{ odd.} \end{cases}$$

Moreover, if  $B$  is a Borel subgroup, then

$$i_2(B) \leq \begin{cases} q - 1 & \text{for } q \text{ even;} \\ q & \text{for } q \text{ odd.} \end{cases}$$

If  $D$  is the dihedral group above, then

$$i_2(D) \leq \begin{cases} (q+1)/2 & \text{for } q \text{ odd;} \\ q-1 & \text{for } q \text{ even.} \end{cases}$$

So if  $q$  is odd, then we may assume that  $q \geq 7$ ; thus

$$i_2(G) \geq (q^2 - q)/2 > 2q + (q+1)/2 \geq 2i_2(B) + i_2(D).$$

Also, if  $q$  is even, then we may assume that  $q \geq 8$  and so

$$i_2(G) \geq q^2 - 1 > 2(q-1) + (q-1) \geq 2i_2(B) + i_2(D).$$

Thus  $x \notin \text{PSL}_2(q)$ .

Now suppose that  $x$  is a field automorphism of  $\text{PSL}_2(q)$ . We may assume that  $x$  is a standard field automorphism by [GL83, 7.2]. Define  $q_0$  by  $q := q_0^p$  and let

$$\Gamma = \{y \in G_0 \mid y^2 = 1, \langle x, y \rangle \neq G\}.$$

We will show that  $|\Gamma| < i_2(G_0)$ . Indeed, if  $y \in \Gamma$  then  $\langle x, y \rangle \cap G_0$  is contained in a subgroup of  $G_0 = \text{PSL}_2(q_0^p)$ . From the description of the subgroups of  $\text{PSL}_2(q)$ , since  $p$  is odd,  $\langle x, y \rangle \cap G_0$  must be contained in a Borel subgroup, a dihedral group of order  $\frac{2(q \pm 1)}{(2, q-1)}$ , or a subfield subgroup of type  $\text{PSL}_2(q_0)$ . We note that since  $(x, G)$  is a minimal counterexample,  $\langle x, y \rangle \cap G_0$  cannot be contained in any other maximal subfield subgroups. Now, if  $H$  is a torus of order  $\frac{(q \pm 1)}{(2, q-1)}$ , a Borel or subfield subgroup, then the  $G$ -conjugates of  $H$  fixed by  $x$  form one  $C_{G_0}(x)$  orbit (see the proof of [GS03, Lemma 3.1] for example). If  $H$  is a  $G$ -conjugate of a maximal dihedral group that is fixed by  $x$ , then  $x$  must also normalize the characteristic cyclic subgroup of  $H$  (a torus of order  $(q \pm 1)/(2, q-1)$ ). Since the  $G$ -conjugates of the torus that are fixed by  $x$  are all  $C_{G_0}(x)$ -conjugate, it follows that the  $G$ -conjugates of the dihedral group that are fixed by  $x$  are also  $C_{G_0}(x)$ -conjugate. So the number of conjugates of  $H$  that can contain  $\langle x, y \rangle \cap G_0$  is at most  $|C_{G_0}(x)|/|C_H(x)|$ . Thus the number of involutions  $y$  in  $G_0$  such that  $\langle x, y \rangle \cap G_0$  is contained in a conjugate of  $H$  is at most

$$\frac{i_2(H)|C_{G_0}(x)|}{|C_H(x)|}.$$

Let  $X_1, \dots, X_k = C_{G_0}(x)$  be representatives for the conjugacy classes of maximal subgroups containing  $\langle x, y \rangle \cap G_0$ . Note that there are no nontrivial conjugates of  $X_k = C_{G_0}(x)$  fixed by  $x$  and so a crude upper bound for the number of involutions in  $G$  such that  $\langle x, y \rangle \cap G_0$  is contained in  $C_{G_0}(x)$  is  $|C_{G_0}(x)|$ . So if  $(x, G)$  is a minimal counterexample, then we have

$$|\Gamma| \leq \sum_{i=1}^{k-1} \frac{i_2(X_i)|C_{G_0}(x)|}{|C_{X_i}(x)|} + |C_{G_0}(x)|.$$

If  $q$  is odd, then

$$\begin{aligned} \sum_{i=1}^k \frac{i_2(X_i)|C_{G_0}(x)|}{|C_{X_i}(x)|} &\leq \frac{q_0^p q_0 (q_0^2 - 1)}{q_0 (q_0 - 1)} + \frac{(q_0^p + 1) q_0 (q_0^2 - 1)}{2(q_0 - 1)} + \frac{(q_0^p + 3) q_0 (q_0^2 - 1)}{2(q_0 + 1)} + \frac{q_0 (q_0^2 - 1)}{2} \\ &\leq \frac{q_0 (q_0 + 1) (3q_0^p + q_0 + 3)}{2}; \end{aligned}$$

but this is less than  $i_2(G_0) \geq q_0^p(q_0^p - 1)/2$ . If  $q$  is even, then

$$\begin{aligned} \sum_{i=1}^k \frac{i_2(X_i)|C_{G_0}(x)|}{|C_{X_i}(x)|} &\leq \frac{(q_0^p - 1)q_0(q_0^2 - 1)}{q_0(q_0 - 1)} + \frac{(q_0^p - 1)q_0(q_0^2 - 1)}{2(q_0 - 1)} + \frac{(q_0^p + 1)q_0(q_0^2 - 1)}{2(q_0 + 1)} + q_0(q_0^2 - 1) \\ &\leq 2(q_0^p + q_0)(q_0 + 1)q_0; \end{aligned}$$

but  $i_2(G_0) \geq (q_0^{2p} - 1)$  and so  $|F| < i_2(G_0)$ .

If  $\mathrm{SL}_2^\epsilon(q) \leq G \leq \mathrm{GL}_2^\epsilon(q)$  with  $[G : \mathrm{SL}_2^\epsilon(q)]$  even and  $x \in G$ , then we may assume that  $x$  has order  $p$  by Lemma 3.2. Moreover, the assumption on the index implies that  $q$  is odd. If  $x$  is semisimple, then since  $\mathrm{GL}_2^\epsilon(5)$  does not contain *semisimple* elements of order  $p \geq 5$ , we may assume that  $q \geq 7$ . If  $(x, G)$  is a minimal counterexample then  $x$  must be contained in  $\mathrm{SL}_2^\epsilon(q)$ , for otherwise  $p \mid q - \epsilon$  and there exists a scalar  $\lambda$  such that  $\lambda x \in \mathrm{SL}_2^\epsilon(q)$ . Thus  $\mathrm{SL}_2^\epsilon(q)$  has index 2 in  $G$ , and there are at least  $q^2 + q$  involutions in  $G$ . Now the same counting argument as for  $\mathrm{PSL}_2(q)$  shows that  $(x, G)$  cannot be a minimal counterexample.

If  $x$  is unipotent in  $\mathrm{SL}_2^\epsilon(q)$ , then  $q \geq 5$ , and by minimality,  $\mathrm{SL}_2^\epsilon(q)$  has index 2 in  $G$ . We may assume that  $x$  is not contained in any subfield subgroups by minimality. So choose an involution  $y$  such that  $[x, x^y] \neq 1$ . Another inspection of the maximal subgroups shows that  $\langle x, y \rangle$  is not solvable.  $\square$

We remark that if  $q$  is odd,  $\mathrm{SL}_2(q) \leq G \leq \mathrm{GL}_2(q)$  and  $\mathrm{SL}_2(q)$  has odd index in  $G$ , then in particular,  $G = \langle \mathrm{SL}_2(q), A \rangle$  where  $A = \begin{pmatrix} \lambda^2 & 0 \\ 0 & 1 \end{pmatrix}$  and  $\lambda \in \mathbb{F}_q^*$ . But then  $G = \langle \mathrm{SL}_2(q), \lambda I_2 \rangle = \mathrm{SL}_2(q)Z(G)$  and  $-I_2$  is the only involution in  $G$ ; thus the conclusion of Theorem 1.3 does not hold. A similar argument holds if  $q$  is odd,  $\mathrm{SU}_2(q) \leq G \leq \mathrm{GU}_2(q)$  and  $\mathrm{SU}_2(q)$  has odd index in  $G$ .

**Lemma 3.4.** *If  $G$  is almost simple and  $x$  is an outer automorphism of  $G_0$ , then  $(x, G)$  cannot be a minimal counterexample, except possibly if  $G_0 \cong {}^2B_2(2^a)$ .*

**Proof.** We may assume that the untwisted Lie rank is at least 2 since the case where  $G_0 \cong \mathrm{PSL}_2(q)$  has already been eliminated. Since  $x$  has order  $p$ , it is a field automorphism, and by [GL83, 7.2] we may assume that  $x$  is a standard field automorphism. Now if  $G_0$  is not a Suzuki–Ree group, then  $x$  normalizes but does not centralize an  $\mathrm{SL}_2(q)$  subgroup  $S$ . So if  $q$  is even and  $G_0$  is not a Suzuki–Ree group, then there exists an involution  $y \in S$  such that  $\langle x, y \rangle$  is not solvable. Thus we may assume that either  $G_0$  is a Suzuki–Ree group or that  $q$  is odd.

If  $q$  is odd, then an inspection of the (extended) Dynkin diagram shows that  $x$  normalizes but does not centralize a type  $\mathrm{SL}_3(q)$  subgroup  $H$ , unless  $G_0 \cong \mathrm{PSL}_2(q)$ ,  $\mathrm{PSL}_3(q)$ ,  $\mathrm{PSp}_4(q)$ ,  ${}^3D_4(q)$ ,  ${}^2G_2(3^a)$ , or  $\mathrm{PSU}_d(q)$ . If  $G_0 = \mathrm{L}_3^\epsilon(q)$  and  $q$  is odd, then  $x$  normalizes a subgroup of type  $\mathrm{SO}_3(q)$ . If  $G_0 \cong \mathrm{PSU}_d(q)$  and  $d \geq 4$ , then  $x$  normalizes but does not centralize a subgroup  $H$  of  $G_0$  that is isomorphic to  $\mathrm{PSO}_d^\epsilon(q).(d, 2)$  (when  $d = 4$ , take  $\epsilon = -$ ; see [KL90, 4.5.5]). If  $G_0 \cong {}^3D_4(q)$  then  $x$  normalizes but does not centralize a subgroup  $H$  isomorphic to  $G_2(q)$ . If  $G_0 \cong \mathrm{PSp}_4(q)$ , then  $x$  normalizes a subgroup  $H$  isomorphic to  $\mathrm{PSP}_2(q^2).2$  (see [KL90, Proposition 4.3.10]). If  $G_0 \cong {}^2G_2(3^a)$ , then let  $z$  be an involution in  $C_{G_0}(x)$ . Then  $x \in C_G(z)$ , which is a subgroup  $H$  of type  $\mathrm{PSL}_2(3^a)$  by [GLS98, Table 4.5.1]. Moreover,  $x$  does not centralize a subgroup of type  $\mathrm{PSL}_2(3^a)$  since it does not centralize an element of order divisible by  $3^a + 1$ . If  $G_0 \cong {}^2F_4(2^a)$ , then a field automorphism normalizes, but does not centralize, a subgroup of  $G_0$  isomorphic to  $\mathrm{PGU}_3(2^a) : 2$  (see [Mal91]). It follows that  $(x, G)$  cannot be a minimal counterexample in all of these cases.  $\square$

**Lemma 3.5.** *If  $x$  is a unipotent element in  $G$ , then  $(x, G)$  cannot be a minimal counterexample.*

**Proof.** Since  $p \geq 5$  and  $p \mid q$ ,  $G$  cannot be a Suzuki–Ree group, and by Lemma 3.3, we may assume that the untwisted Lie rank is at least 2. If  $G$  is an almost simple group, then we may assume that  $G = G_0$  and by Lemma 3.2, we can lift  $x$  to an element of order  $p$  in the universal version of  $G_0$ .

By Lemma 2.2, we may assume that  $x$  is nontrivial in  $P/U$  for some end node maximal parabolic subgroup  $P$ , with unipotent radical  $U$ , unless  $G$  is  ${}^3D_4(q)$ , or  $SU_d(q)$ .

So we may assume that  $x$  acts nontrivially on a Levi subgroup  $L$ , and since  $G$  is simply connected, so is  $L$  (see [GLS98, 2.6.5(f)] for example). By induction, there exists an involution  $y \in L$  such that  $\langle x, y \rangle$  is not solvable; thus there exists an involution  $y' \in G_0$  such that  $\langle x, y' \rangle$  is not solvable.

If  $G_0 \cong {}^3D_4(q)$ , then we may assume that  $x$  is nontrivial in  $P/U$ , for a maximal parabolic subgroup  $P$ . The Levi complement is of type  $SL_2(q)$  or  $SL_2(q^3)$ , but a split torus normalizes both of these Levi complements and induces diagonal automorphisms on them. Thus we can reduce to the case that  $SL_2(q) \leq G \leq GL_2(q)$ , where  $SL_2(q)$  has even index in  $G$  when  $q$  is odd.

Now suppose that  $G = SU_d(q)$ . Then Lemma 2.2 implies that we may assume that  $x$  is nontrivial in  $P/U$ , for some (not necessarily end-node) maximal parabolic subgroup  $P$ . Therefore  $x$  will act nontrivially on one of the components of the Levi complement of  $P$ , and if  $d \geq 6$  then these components are all nonsolvable since  $p \geq 5$ , and we may assume that none of them are of type  $SL_2(q)$ . If  $G = SU_5(q)$  then we may assume that  $x$  is nontrivial in  $P/U$  for some maximal parabolic subgroup  $P$ . The Levi complement is either of type  $SU_3(q)$  or isomorphic to  $GL_2(q^2)$ ; thus  $\langle x, G \rangle$  cannot be a minimal counterexample. If  $G = SU_4(q)$  then we argue in the same way: the Levi complement  $L$  of  $P$  is either a normal subgroup of  $GL_2(q^2)$  of index  $q+1$  or a normal subgroup of  $GL_1(q^2) \times GU_2(q)$  of index  $q+1$ , where the projection onto the second factor is  $GU_2(q)$ ; thus  $\langle x, G \rangle$  cannot be a minimal counterexample.

The only other possibility is  $G = SU_3(q)$ . If  $x$  is a transvection, then it is contained in a subgroup isomorphic to  $GU_2(q)$ . So we may assume that  $x$  is not a transvection and  $x$  is therefore regular unipotent. Since all inner diagonal involutions of  $PSU_3(q)$  lift to involutions in  $SU_3(q)$ , we can work in  $PSU_3(q)$ . From the list of maximal subgroups of  $PSU_3(q)$  (see [GLS98, Theorem 6.5.3] for example), we may assume that the only maximal subgroups that could contain  $x$  are the maximal parabolic subgroups since the other maximal subgroups of order divisible by  $p$  are almost simple. Now  $x$  only stabilizes one totally singular 1-space, and so is only contained in one maximal parabolic subgroup. So choose an involution  $y$  that is not contained in this maximal parabolic subgroup. Then  $\langle x, y \rangle$  is not solvable.  $\square$

**Lemma 3.6.** *If  $G$  or  $G_0$  is a classical group, then  $\langle x, G \rangle$  cannot be a minimal counterexample.*

**Proof.** By Lemmas 3.2, 3.3, 3.4, and 3.5 we may assume that  $x$  is semisimple and that  $G_0$  or  $G/Z(G)$  is not  $PSL_2(q)$ . Moreover, we can and will assume that  $x$  is an element of order  $p$  in  $G$  where  $SL_d(q) \leq G \leq GL_d(q)$ ,  $SU_d(q) \leq G \leq GU_d(q)$ ,  $G = Sp_d(q)$  or  $G = \Omega_d^\epsilon(q)$  by Lemma 3.2 and [Bur07, Lemma 3.11]. In case O, we may assume that  $d \geq 7$ . If  $G$  is a unitary group, let  $e$  be the smallest positive integer such that  $p \mid q^{2e} - 1$ ; otherwise let  $e$  be the smallest positive integer such that  $p \mid q^e - 1$ . Consider a decomposition of  $V$  into irreducible  $\langle x \rangle$ -invariant spaces

$$V = (W_1 \oplus W'_1) \perp \cdots \perp (W_k \oplus W'_k) \perp U_1 \perp \cdots \perp U_l, \quad (1)$$

where the  $W_i$  and  $W'_i$  are totally singular, and the  $U_i$  and  $W_i \oplus W'_i$  are nondegenerate. Each irreducible subspace on which  $x$  acts nontrivially has dimension  $e$ . In case U, we can and will assume that the 1-spaces on which  $x$  acts trivially are nondegenerate. We consider five cases separately.

- (i) Suppose that  $e = 1$ . In cases L, S, and O, all of the irreducible subspaces on which  $\langle x \rangle$  acts nontrivially must be totally singular since  $p \mid q - 1$ . Moreover,  $q \geq 8$  since  $p \geq 5$ . So in cases S and L, we may assume that  $x$  acts nontrivially on  $W_1 \oplus W_2$  and so we reduce to the case of  $GL_2(q)$ , and  $\langle x, G \rangle$  is not a minimal counterexample in this case. In case O, since  $d \geq 7$ , we may assume that there are totally singular subspaces  $W_1, W_2, W_3$  such that  $W_1 \oplus W_2 \oplus W_3$  is totally singular and  $x$  invariant; thus we reduce to the case of  $SL_3(q)$ . In case U, if  $p \mid q - 1$ , then we can argue as in cases S and L to reduce to the 2-dimensional case, which has been eliminated. If  $p \nmid q - 1$ , then  $q \geq 4$  and we may assume that all of the subspaces in (1) are nondegenerate; so  $x$  is contained in a type  $GU_1(q)^d$  subgroup and therefore we can reduce to the case  $G \cong GU_2(q)$ .

- (ii) Suppose that  $e = 2$ . In case U, all of the 2-spaces in (1) are totally singular since even dimensional unitary groups do not contain irreducible elements. So in case U,  $x$  acts irreducibly on  $W_1$  and we reduce to the case  $G \cong \mathrm{GL}_2(q^2)$ . In the other cases,  $q \geq 4$  since  $p \geq 5$ . In cases L and S, if there is a totally singular 2-space  $W_1$  in (1), then we can reduce to the case  $G \cong \mathrm{GL}_2(q)$ . If there are no totally singular 2-spaces in case S, then all of the 2-spaces in (1) are nondegenerate, and we can reduce to the case  $G \cong \mathrm{Sp}_4(q)$ . In this case, we may assume that  $q$  is odd since if  $q$  is even then we can reduce to the case  $G \cong \mathrm{Sp}_2(q)$ . But when  $q$  is odd, a Sylow  $p$ -subgroup is contained in a subgroup isomorphic to  $\mathrm{GU}_2(q)$  (see [KL90, p. 118]); thus we do not have a minimal counterexample in this case either. In case O, either we can reduce to the case  $G \cong \Omega_d(q)$  with  $d = 5$  or  $6$ , or all of the subspaces are totally singular. In this case,  $x$  stabilizes  $W_1 \oplus W_2$ , and we reduce to the case of  $\mathrm{SL}_4(q)$ . Thus  $(x, G)$  cannot be a minimal counterexample.
- (iii) Suppose that  $e = 3 < d$ . If there is a totally singular 3-space  $W_1$  in (1), then in all cases we reduce to the case of  $\mathrm{SL}_3(q)$  (or  $\mathrm{SL}_3(q^2)$ ). Otherwise, all of the 3-spaces in (1) are nondegenerate and we are in case U or O. In case U, we can reduce to the case  $G \cong \mathrm{SU}_3(q)$ , and  $q \neq 2$  since  $\mathrm{GU}_3(2)$  has order  $2^3 3^4$ . In case O, we have  $d \geq 7$  and so we can reduce to the case  $G = \Omega_6^\pm(q)$ .
- (iv) Suppose that  $4 \leq e < d$ . If there is a totally singular  $e$ -space in (1), then we can reduce to the  $e$ -dimensional linear case. Otherwise  $x$  acts irreducibly on a nondegenerate  $e$ -space, and we can reduce to the case  $G = \mathrm{Sp}_e(q)$  in case S,  $G = \mathrm{SU}_e(q)$  in case U ( $e$  odd), and  $G = \Omega_e^\pm(q)$  ( $e$  even) in case O.
- (v) Suppose that  $e = d$ , so that  $x$  acts irreducibly. In case S,  $x$  must be contained in a type  $\mathrm{GU}_{d/2}(q)$  subgroup [KL90, p. 118]. In case O, if  $d/2$  is odd then  $x$  must be contained in a subgroup  $H$  of type  $\mathrm{GU}_{d/2}(q)$ . If  $d/2$  is even, then  $H$  is contained in an  $\Omega_{d/2}^-(q^2)$  subgroup. So we may assume that  $G$  is linear or unitary. Now observe that if  $d$  is even, then  $G$  is linear and  $x$  is contained in a normal subgroup of  $\mathrm{GL}_2(q^{d/2})$  of index dividing  $q - 1$  (see [KL90, (4.3.16)]), and so if  $(x, G)$  is a minimal counterexample, then  $d/2$  must be odd. But if  $d/2$  is odd, then  $x$  is contained in a type  $\mathrm{GL}_{d/2}(q^2)$  subgroup and so  $(x, G)$  cannot be a minimal counterexample in this case either. So  $d$  must be odd and in fact  $d$  must be an odd prime since otherwise  $x$  is contained in a type  $\mathrm{GL}_{d/r}^\epsilon(q^r)$  subgroup. We can list the possible maximal subgroups of  $G$  that could contain  $x$  using [GPPS99] and [KL90]. Since  $d$  is odd, all involutions in  $\mathrm{PGL}_d^\epsilon(q)$  lift to involutions in  $\mathrm{SL}_d^\epsilon(q)$ ; thus we can work in the almost simple group  $G/Z(G)$ . In particular, we may assume that  $x$  is not contained in any almost simple subgroup of  $G/Z(G)$ . In this case, the only possible maximal subgroups containing  $x$  are of type  $\mathrm{GL}_1^\epsilon(q^d).d$ . Since  $p \nmid d$ ,  $x$  is contained in a cyclic maximal torus  $T$ , and since  $C_G(x) = T$ ,  $x$  is contained in only one maximal subgroup. Thus we can pick an involution  $y$  not contained in this maximal subgroup, and  $\langle x, y \rangle$  will not be solvable.  $\square$

**Lemma 3.7.** *If  $G$  is a finite group of Lie type and  $Z(G) \neq 1$ , then  $(x, G)$  cannot be a minimal counterexample unless  $G$  is (simply connected)  $E_7(q)$ .*

**Proof.** By our previous work, we may assume that  $G$  is an exceptional group or  $G = \mathrm{Spin}_d^\pm(q)$  with  $d \geq 7$  and  $q$  odd. In the former case, the center of  $G$  is either trivial or of odd order, or  $G$  is  $E_7(q)$ . So if  $(x, G)$  is a minimal counterexample, then Theorem 1.3 holds for  $G/Z(G)$ . But then there exists  $y \in G$  such that  $\langle x, y \rangle$  is not solvable and  $y^2 \in Z(G)$ . Since  $Z(G)$  has odd order,  $y' = y^{|Z(G)|}$  is an involution in  $G$  and  $\langle x, y' \rangle$  is not solvable.

Now suppose that  $G = \mathrm{Spin}_d^\epsilon(q)$  and we may assume that  $x$  is semisimple by Lemma 3.5. If the image of  $x$  in  $G/Z(G) \cong \mathrm{P}\Omega_d^\epsilon(q)$  is contained in a subsystem subgroup or parabolic subgroup, then  $x$  will be contained in a subsystem or parabolic subgroup of  $G$  and we can use the same arguments as in Lemma 3.6 to reduce to the case where  $G = \mathrm{Spin}_d^\pm(q)$ ,  $e = d$  is even and the image of  $x$  acts irreducibly in  $\Omega_{d/2}^\pm(q)$ . In particular,  $p \mid q^{d/2} + 1$  and a Sylow  $p$ -subgroup is contained in a subgroup of  $G$  of type  $\Omega_{d/2}^\pm(q^2)$  or  $\mathrm{SU}_{d/2}(q)$  in the cases  $d/2$  is even and odd respectively. Thus,  $(x, G)$  cannot be a minimal counterexample in this case.  $\square$



**Table 2**Subgroups of  $E_7(q)$  containing a Sylow  $p$ -subgroup.

$e$	$p$ divides	$p$ -part of $ G $ is $p$ -part of	Subgroup type containing a Sylow $p$ -subgroup
18	$q^9 + 1$	$q^6 - q^3 + 1$	${}^2E_6(q)$
18	$q^9 - 1$	$q^6 + q^3 + 1$	$E_6(q)$
14	$q^7 + 1$	$(q^7 + 1)/(q + 1)$	$SU_7(q)$
14	$q^7 - 1$	$(q^7 - 1)/(q - 1)$	$SL_7(q)$
12	$q^6 + 1$	$(q^6 + 1)/(q^2 + 1)$	$F_4(q)$
12	$q^6 - 1$	$x$	
10	$q^5 + 1$	$(q^5 + 1)/(q + 1)$	$SU_7(q)$
10	$q^5 - 1$	$(q^5 - 1)/(q - 1)$	$SL_7(q)$
8	$q^4 + 1$	$q^4 + 1$	$SL_8(q)$
8	$q^4 - 1$	$(q^2 + 1)^2$	$F_4(q)$
6	$q^3 + 1$	$(q^2 - q + 1)^3$	${}^2E_6(q)$
6	$q^3 - 1$	$(q^2 + q + 1)^3$	$E_6(q)$
2	$q + 1$	$(7, p)(5, p)(q + 1)^7$	$SU_8(q)$
2	$q - 1$	$x$	

**Lemma 3.8.** Suppose that  $G$  is almost simple or a finite group of Lie type, and that  $G_0$  or  $G/Z(G)$  is one of the simple groups  $F_4(q)$ ,  $E_6(q)$ ,  $E_7(q)$ ,  $E_8(q)$ , or  ${}^2E_6(q)$ . Then  $\langle x, G \rangle$  cannot be a minimal counterexample.

**Proof.** We may assume that  $G$  is almost simple with  $x \in \text{Inndiag}(G_0)$  or that  $G$  is (simply connected)  $E_7(q)$  by Lemmas 3.4 and 3.7. Moreover, we may assume that  $x$  is semisimple in both cases by Lemma 3.5. First suppose that  $G$  is one of the untwisted groups. If  $p \mid q - 1$  then  $x$  is contained in a Borel subgroup and, in particular, in  $P_1$  and  $P_4$  maximal parabolic subgroups. By [GS03, Lemma 2.1], we may therefore assume that  $x$  acts noncentrally on a Levi subgroup of type  $B_3(q)$ ,  $C_3(q)$ ,  $A_{l-1}(q)$ , or  $D_{l-1}(q)$  and so  $\langle x, G \rangle$  cannot be a minimal counterexample. So we may assume that  $p \nmid q - 1$  in the untwisted cases. Now suppose that  $x$  is contained in some maximal parabolic subgroup. Again we may assume that  $x$  acts noncentrally on each component of the Levi complement. It is easily verified that  $\langle x, G \rangle$  cannot be a minimal counterexample since we can work in one of the groups of Lie type in the Levi complement to find an involution  $y$  such that  $\langle x, y \rangle$  is not solvable.

So we may assume that  $x$  is not contained in any parabolic subgroups. If this is the case, then the centralizer of  $x$  is reductive and contains no unipotent elements. First suppose that  $G = E_7(q)$ , and without loss of generality we may assume that  $G$  is simply connected. We know that

$$|G| = q^{63} \prod_{d_i \in \{2, 6, 8, 10, 12, 14, 18\}} (q^{d_i} - 1),$$

so let  $e$  be the smallest  $d_i$  such that  $p \mid q^{d_i} - 1$ . If  $e = 14$  then either  $p \mid q^7 - 1$  or  $p \mid q^7 + 1$ . If  $p \mid q^7 - 1$  then the  $p$ -part of  $|G|$  (that is, the largest power of  $p$  dividing  $|G|$ ) is the  $p$ -part of  $(q^7 - 1)/(q - 1)$  and so a Sylow  $p$ -subgroup is contained in a type  $SL_7(q)$  subsystem subgroup. Thus  $\langle x, G \rangle$  cannot be a minimal counterexample in this case. If  $p \mid q^7 + 1$ , then the  $p$ -part of  $|G|$  is the  $p$ -part of  $(q^7 + 1)/(q + 1)$  and so a Sylow  $p$ -subgroup is contained in a type  $SU_7(q)$  subgroup. Similarly we can show that  $\langle x, G \rangle$  cannot be minimal counterexample for all values of  $p$ . We illustrate this work in Table 2 (note that  $p \nmid q - 1$  since we are assuming that  $x$  is not contained in any parabolic subgroups). We do the same for  $F_4(q)$ ,  $E_6(q)$ ,  ${}^2E_6(q)$ , and  $E_8(q)$  and record our results in Tables 3, 4, 5 and 6 respectively.

The only case where we have not shown that  $\langle x, G \rangle$  is not a minimal counterexample is when  $G = E_8(q)$  and  $p$  is a primitive prime divisor of  $q^{30} - 1$  or  $q^{15} - 1$ . It follows that  $p \equiv 1 \pmod{15}$  or  $p \equiv 1 \pmod{30}$ , and in particular, that  $p \geq 31$ . If  $p = 31$ , then the Sylow 31-subgroups are cyclic and  $x$  is contained in an exotic local subgroup  $5^3.SL_3(5)$ . Therefore we may assume that  $p \neq 31$ . The maximal subgroups of  $E_8(q)$  are described in [LS03, Theorem 8] and if  $\langle x, G \rangle$  is a minimal counterexample, then  $x$  can only be contained in a (single) torus  $T$  of type  $q^8 + q^7 - q^5 - q^4 - q^3 + q + 1$  or  $q^8 - q^7 + q^5 - q^4 + q^3 - q + 1$ . In this situation, we can pick an involution  $y \in G$  that is not contained in the normalizer of  $T$  and  $\langle x, y \rangle$  will not be solvable.  $\square$

**Table 3**Subgroups of  $F_4(q)$  containing a Sylow  $p$ -subgroup.

$e$	$p$ divides	$p$ -part of $ G $ is $p$ -part of	Subgroup type containing a Sylow $p$ -subgroup
12	$q^6 + 1$	$q^4 - q^2 + 1$	${}^3D_4(q)$
12	$q^6 - 1$	$x$	
8	$q^4 + 1$	$q^4 + 1$	$Spin_9(q)$
8	$q^4 - 1$	$(q^2 + 1)^2$	$Spin_9(q)$
6	$q^3 + 1$	$(q^2 - q + 1)^2$	${}^3D_4(q)$
6	$q^3 - 1$	$(q^2 + q + 1)^2$	${}^3D_4(q)$
2	$q + 1$	$(q + 1)^4$	$Spin_9(q)$
2	$q - 1$	$x$	

**Table 4**Subgroups of  $E_6(q)$  containing a Sylow  $p$ -subgroup.

$e$	$p$ divides	$p$ -part of $ G $ is $p$ -part of	Subgroup type containing a Sylow $p$ -subgroup
12	$q^6 + 1$	$q^4 - q^2 + 1$	$F_4(q)$
12	$q^6 - 1$	$x$	
9	$q^9 - 1$	$q^6 + q^3 + 1$	$SL_3(q^3)$
8	$q^4 + 1$	$q^4 + 1$	$F_4(q)$
8	$q^4 - 1$	$(q^2 + 1)^2$	$F_4(q)$
6	$q^3 + 1$	$(q^2 - q + 1)^2$	$F_4(q)$
6	$q^3 - 1$	$(q^2 + q + 1)^3$	$SL_3(q) \circ SL_3(q) \circ SL_3(q)$
5	$q^5 - 1$	$q^4 + q^3 + q^2 + q + 1$	$SL_5(q)$
2	$q + 1$	$(q + 1)^4$	$F_4(q)$
2	$q - 1$	$x$	

**Table 5**Subgroups of  ${}^2E_6(q)$  containing a Sylow  $p$ -subgroup.

$e$	$p$ divides	$p$ -part of $ G $ is $p$ -part of	Subgroup type containing a Sylow $p$ -subgroup
12	$q^6 + 1$	$q^4 - q^2 + 1$	$F_4(q)$
12	$q^6 - 1$	$x$	
9	$q^9 + 1$	$q^6 - q^3 + 1$	$SU_3(q^3)$
8	$q^4 + 1$	$q^4 + 1$	$F_4(q)$
8	$q^4 - 1$	$(q^2 + 1)^2$	$F_4(q)$
6	$q^3 + 1$	$(q^2 - q + 1)^3$	$SU_3(q) \circ SU_3(q) \circ SU_3(q)$
6	$q^3 - 1$	$(q^2 + q + 1)^2$	$F_4(q)$
5	$q^5 + 1$	$q^4 - q^3 + q^2 - q + 1$	$Spin_{10}^-(q)$
2	$q + 1$	$(q + 1)^6$	$SU_3(q) \circ SU_3(q) \circ SU_3(q)$
2	$q - 1$	$(q - 1)^4$	$F_4(q)$

**Lemma 3.9.** If  $G_0 \cong G_2(q)$ ,  ${}^3D_4(q)$ , or  ${}^2F_4(2^a)$ , then  $(x, G)$  cannot be a minimal counterexample.

**Proof.** The proof is similar to that of Lemma 3.8. We may assume that  $x$  is semisimple by Lemmas 3.5 and 3.4. Also, since  $G_2(2)' \cong PSU_3(3)$ , we can eliminate this case. If  $G_0 \cong G_2(q)$ , then  $x$  normalizes but does not centralize a subgroup of type  $SL_3^{\epsilon}(q)$  (see [GS03, p. 546]). So  $G_0 \not\cong G_2(q)$ . If  $G_0$  is  ${}^3D_4(q)$  or  ${}^2F_4(2^a)$ , then we list the possible expressions in  $q$  that could be divisible by  $p$  in Tables 8 and 7. Since  $p \geq 5$ ,  $p$  divides precisely one of these expressions. In most cases, we can deduce that  $(x, G)$  cannot be a minimal counterexample. If  $G_0 \cong {}^2F_4(2^a)$ , then we may therefore assume that  $p \mid q^4 - q^2 + 1$ . In this case, either  $p \mid q^2 + \sqrt{2q^3} + q + \sqrt{2q} + 1$  or  $p \mid q^2 - \sqrt{2q^3} + q - \sqrt{2q} + 1$ , and from the list of maximal subgroups of  $G$  (see [Mal91]), we may assume that  $x$  is only contained in a (single) torus  $T$  of order  $q^2 + \sqrt{2q^3} + q + \sqrt{2q} + 1$  or  $q^2 - \sqrt{2q^3} + q - \sqrt{2q} + 1$ . Thus we can pick an involution  $y \in G$  that is not contained in the normalizer of  $T$  and  $\langle x, y \rangle$  will not be solvable.

Suppose that  $G_0 \cong {}^3D_4(q)$ . We note that if  $p \mid q^2 - q + 1$ , then  $x$  is contained in a subgroup of type  $(q^2 - q + 1) \circ SU_3(q)$ . If  $x$  does not centralize the  $SU_3(q)$ , then  $(x, G)$  cannot be a minimal counterexample. But if  $x$  does centralize the  $SU_3(q)$  subgroup, then  $x$  centralizes unipotent elements

**Table 6**Subgroups of  $E_8(q)$  containing a Sylow  $p$ -subgroup.

$e$	$p$ divides	$p$ -part of $ G $ is $p$ -part of	Subgroup type containing a Sylow $p$ -subgroup
30	$q^{15} + 1$	$q^8 + q^7 - q^5 - q^4 - q^3 + q + 1$	see Lemma 3.8
30	$q^{15} - 1$	$q^8 - q^7 + q^5 - q^4 + q^3 - q + 1$	see Lemma 3.8
24	$q^{12} + 1$	$q^8 - q^4 + 1$	$SU_3(q^4)$
24	$q^{12} - 1$	$x$	
20	$q^{10} + 1$	$q^8 - q^6 + q^4 - q^2 + 1$	$SU_5(q^2)$
20	$q^5 + 1$	$(q^4 - q^3 + q^2 - q + 1)^2$	$SU_5(q) \circ SU_5(q)$
20	$q^5 - 1$	$(q^4 + q^3 + q^2 + q + 1)^2$	$SL_5(q) \circ SL_5(q)$
18	$q^9 + 1$	$q^6 - q^3 + 1$	$SU_9(q)$
18	$q^9 - 1$	$q^6 + q^3 + 1$	$SL_9(q)$
14	$q^7 + 1$	$q^6 - q^5 + q^4 - q^3 + q^2 - q + 1$	$SU_9(q)$
14	$q^7 - 1$	$q^6 + q^5 + q^4 + q^3 + q^2 + q + 1$	$SL_9(q)$
12	$q^6 + 1$	$(q^4 - q^2 + 1)^2$	$SU_3(q^2) \circ SU_3(q^2)$
12	$q^3 + 1$	$(q^2 - q + 1)^4(5, p)$	${}^3D_4(q) \circ {}^3D_4(q)$
12	$q^3 - 1$	$(q^2 + q + 1)^4(5, p)$	${}^3D_4(q) \circ {}^3D_4(q)$
8	$q^4 + 1$	$(q^4 + 1)^2$	$SU_3(q^4)$
8	$q^2 + 1$	$(q^2 + 1)^4(5, p)$	$SU_5(q^2)$
2	$q + 1$	$(7, p)(5, p)^2(q + 1)^8$	$SU_5(q) \circ SU_5(q)$ or $SU_9(q)$
2	$q - 1$	$x$	

**Table 7**Subgroups of  ${}^2F_4(q)$  containing a Sylow  $p$ -subgroup,  $q = 2^a$ .

$p$ divides	$p$ -part of $G$ is $p$ -part of	Subgroup type containing a Sylow $p$ -subgroup
$q^4 - q^2 + 1$	$q^4 - q^2 + 1$	see Lemma 3.9
$q^2 + 1$	$(q^2 + 1)^2$	${}^2B_2(q) \circ {}^2B_2(q)$
$q + 1$	$(q + 1)^2$	$SU_3(q)$
$q^2 - q + 1$	$q^2 - q + 1$	$SU_3(q)$
$q - 1$	$(q - 1)^2$	$Sp_4(q)$

**Table 8**Subgroups of  ${}^3D_4(q)$  containing a Sylow  $p$ -subgroup.

$p$ divides	$p$ -part of $G$ is $p$ -part of	Subgroup type containing a Sylow $p$ -subgroup
$q^4 - q^2 + 1$	$q^4 - q^2 + 1$	see Lemma 3.9
$q^2 - q + 1$	$(q^2 - q + 1)^2$	$(q^2 - q + 1) \circ SU_3(q)$
$q^2 + q + 1$	$(q^2 + q + 1)^2$	$(q^2 + q + 1) \circ SL_3(q)$
$q + 1$	$(q + 1)^2$	$G_2(q)$
$q - 1$	$(q - 1)^2$	$G_2(q)$

and is therefore contained in a parabolic subgroup. By Lemma 2.2 we may assume that  $x$  is noncentral in the Levi subgroup, which is of type  $SL_2(q)$  or  $SL_2(q^3)$ . But if  $q > 3$ , then  $x$  cannot be a minimal counterexample since these Levi components are normalized by a split torus, which induces diagonal automorphisms, and we can therefore reduce to the case  $SL_2(q) \leq G \leq GL_2(q)$  where  $SL_2(q)$  has even index in  $G$  when  $q$  is odd. We can verify the cases  $q = 2$  and  $q = 3$  in MAGMA [BCP97]. The case where  $p \mid q^2 + q + 1$  is the same argument. The only remaining case is where  $p \mid q^4 - q^2 + 1$ . In this case, the list of maximal subgroups in [Kle88b] allows us to assume that  $x$  is only contained a (single) torus  $T$  of order  $(q^4 - q^2 + 1)$ . We can then choose an involution  $y$  that is not contained in the normalizer of  $T$ .  $\square$

**Lemma 3.10.** *If  $G_0 \cong {}^2G'_2(3^a)$ , then  $(x, G)$  cannot be a minimal counterexample.*

**Proof.** We may assume that  $a \neq 1$  since  ${}^2G'_2(3) \cong PSL_2(8)$ . Since  $q = 3^a$  and by Lemma 3.4, we may assume that  $x$  is semisimple. Now  $|G_0| = q^3(q^3 + 1)(q - 1)$  and the maximal subgroups are given in [Kle88a]. Since  $p \nmid q$  there are three mutually exclusive possibilities:  $p \mid q^2 - 1$ ,  $p \mid q - \sqrt{3q} + 1$ , and

$p \mid q + \sqrt{3q} + 1$ . First suppose that  $p \mid q^2 - 1$ . Then a Sylow  $p$ -subgroup lies inside a maximal subgroup  $2 \times \text{PSL}_2(q)$ , so  $(x, G)$  cannot be a minimal counterexample in this case.

If  $p \mid q^2 - q + 1$ , then a Sylow  $p$ -subgroup is contained in one of the abelian Hall subgroups of order  $q \pm \sqrt{3q} + 1$ , so we may assume that  $x$  lies in one of these Hall subgroups and that  $|C_G(x)| = q \pm \sqrt{3q} + 1$  (see part (4) of the main theorem in [War66]). If  $(x, G)$  is a minimal counterexample, then  $x$  can only be contained in a single subgroup  $H$ , which is either of type  $\mathbb{Z}_{q+\sqrt{3q}+1} : \mathbb{Z}_6$  or  $\mathbb{Z}_{q-\sqrt{3q}+1} : \mathbb{Z}_6$ . We choose an involution  $y \in G$  that is not contained in  $H$  and then  $\langle x, y \rangle$  is not solvable.  $\square$

For the Suzuki groups, we will use a counting argument.

**Lemma 3.11.** *Let  $G$  be an almost simple group with socle  $G_0$ . Suppose that  $X_1, \dots, X_k$  are representatives for the conjugacy classes of maximal subgroups of  $G$  that contain  $x$  and that do not contain  $G_0$ . Let  $Y$  be the set of involutions in  $G_0$ . If*

$$|Y| > \sum_{i=1}^k \frac{|x^G \cap X_i| |G : X_i| |Y \cap X_i|}{|x^G|}, \quad (2)$$

then there exists an involution  $y$  in  $G_0$  such that  $\langle x, y \rangle$  contains  $G_0$ .

**Proof.** Suppose that  $\langle x, y \rangle$  does not contain  $G_0$  for all  $y \in Y$ . For each  $i$ , let  $X_{i1}, \dots, X_{in_i}$  be the conjugates of  $X_i$  that contain  $x$ . In particular,  $n_i$  is the number of conjugates of  $X_i$  that contain  $x$ . Thus we have

$$\left| Y \cap \bigcup_{i,j} X_{ij} \right| \leq \sum_{i=1}^k n_i |Y \cap X_i|.$$

But by counting the pairs in  $\{(y, Y) \mid y \in x^G, y \in Y, \text{ and } Y \text{ is } G\text{-conjugate to } X_i\}$  in two ways, we obtain the equation

$$n_i |x^G| = |x^G \cap X_i| |G : X_i|;$$

thus

$$\left| Y \cap \bigcup_{i,j} X_{ij} \right| \leq \sum_{i=1}^k \frac{|x^G \cap X_i| |G : X_i| |Y \cap X_i|}{|x^G|}.$$

This is a contradiction, since we assumed that  $Y = Y \cap \bigcup_{i,j} X_{ij}$ .  $\square$

**Lemma 3.12.** *If  $G_0 \cong {}^2B_2(2^a)$  then  $(x, G)$  cannot be a minimal counterexample.*

**Proof.** There are  $(q^2 + 1)(q - 1)$  involutions in  $G_0 = {}^2B_2(q)$ , and the maximal subgroups of  $G_0$  are given in [Suz62]. If  $x \in G_0$ , then since  $p$  is odd, there are three mutually exclusive possibilities:  $p \mid q - 1$ ,  $p \mid q + \sqrt{2q} + 1$ , and  $p \mid q - \sqrt{2q} + 1$ . We will show that  $(x, G)$  cannot be a minimal counterexample using Lemma 3.11. If  $p \mid q - 1$ , then the maximal subgroups that could contain  $x$  are Frobenius groups of order  $q^2(q - 1)$ , dihedral groups of order  $2(q - 1)$  and  ${}^2B_2(2)$ . If  $X_i$  is a Frobenius group, then  $|Y \cap X_i| = q - 1$ , by [Suz62, Theorem 2], and

$$\frac{|x^G \cap X_i| |G : X_i| |Y \cap X_i|}{|x^G|} \leq \frac{(q^3 - q^2 - q)(q^2 + 1)(q - 1)}{q^2(q^2 + 1)} \leq q^2 - q - 1.$$

It follows that

$$\sum_{i=1}^k \frac{|x^G \cap X_i| |G : X_i| |Y \cap X_i|}{|x^G|} \leq (q^2 - q - 1) + \frac{(q-1)^2}{2} + (q-1),$$

which is less than the number of involutions  $(q^2 + 1)(q - 1)$  in  $G_0$  for  $q \geq 8$ . If  $p \mid q + \sqrt{2q} + 1$ , then  $x$  could be contained in a group  $\mathbb{Z}_{(q+\sqrt{2q}+1)} : [4]$  or  ${}^2B_2(2)$ , thus

$$\sum_{i=1}^k \frac{|x^G \cap X_i| |G : X_i| |Y \cap X_i|}{|x^G|} \leq (q + \sqrt{2q} + 1)^2 + (q + \sqrt{2q} + 1)$$

and this is less than  $(q^2 + 1)(q - 1)$  for  $q \geq 8$ . Similarly, if  $p \mid q - \sqrt{2q} + 1$ , then  $x$  could be contained in  $\mathbb{Z}_{(q-\sqrt{2q}+1)} : [4]$  or  ${}^2B_2(2)$ , so

$$\sum_{i=1}^k \frac{|x^G \cap X_i| |G : X_i| |Y \cap X_i|}{|x^G|} \leq (q - \sqrt{2q} + 1)^2 + (q - \sqrt{2q} + 1).$$

So  $(x, G)$  is not a minimal counterexample when  $x \in G_0$ .

If  $x$  is a field automorphism, then we can use the same counting argument as for the case  $G_0 = \text{PSL}_2(q)$ . Indeed, we would like to show that the right-hand side of

$$|\Gamma| \leq \sum_{i=1}^{k-1} \frac{i_2(X_i) |C_{G_0}(x)|}{|C_{X_i}(x)|} + |C_{G_0}(x)| \quad (3)$$

is less than the number of involutions  $(q^2 + 1)(q - 1)$  in  $G_0$ . The possibilities for the maximal subgroups of  $G_0$  containing  $\langle x, y \rangle \cap G_0$  are a Frobenius group of order  $q^2(q - 1)$ , a dihedral group of order  $2(q - 1)$ , the normalizer of a cyclic group  $\mathbb{Z}_{(q-\sqrt{2q}+1)} : [4]$ , the normalizer of a cyclic group  $\mathbb{Z}_{(q+\sqrt{2q}+1)} : [4]$ , and the centralizer of  $x$ ,  ${}^2B_2(q^{1/p})$ . We label these subgroups  $X_1, X_2, X_3, X_4$ , and  $X_5$  respectively.

Therefore, if  $q_0 := q^{1/p}$ , then we have

$$\begin{aligned} \sum_{i=1}^{k-1} \frac{i_2(X_i) |C_{G_0}(x)|}{|C_{X_i}(x)|} + |C_{G_0}(x)| &\leq \frac{(q_0^p - 1)q_0^2(q_0^2 + 1)(q_0 - 1)}{q_0^2(q_0 - 1)} \\ &\quad + \frac{(q_0^p - 1)q_0^2(q_0^2 + 1)(q_0 - 1)}{2(q_0 - 1)} \\ &\quad + \frac{3(q_0^p - \sqrt{2q_0^p} + 1)q_0^2(q_0^2 + 1)(q_0 - 1)}{4(q_0 + \sqrt{2q_0} + 1)} \\ &\quad + \frac{3(q_0^p + \sqrt{2q_0^p} + 1)q_0^2(q_0^2 + 1)(q_0 - 1)}{4(q_0 - \sqrt{2q_0} + 1)} \\ &\quad + q_0^2(q_0^2 + 1)(q_0^2 - 1) \\ &\leq (q_0^p - 1)(q_0^2 + 1) + \frac{(q_0^p - 1)q_0^2(q_0^2 + 1)}{2} \end{aligned}$$

$$+ 2(q_0^p + (2q_0^p)^{\frac{1}{2}} + 1)q_0^2(q_0 + (2q_0)^{\frac{1}{2}} + 1)(q_0 - 1) \\ + q_0^2(q_0^2 + 1)(q_0^2 - 1).$$

Since  $p \geq 5$ , an elementary calculation shows that (3) holds; thus  $(x, G)$  cannot be a minimal counterexample.  $\square$

**Lemma 3.13.** *Let  $G_0$  be a sporadic group. Then  $(x, G)$  cannot be a minimal counterexample.*

**Proof.** We can verify the sporadic groups in GAP using the character table library [GAP08]. We use Thompson's result [Tho68, Corollary 3] that a group  $H$  is nonsolvable if and only if there exist  $a, b, c \in H$  of pairwise coprime order such that  $abc = 1$ . Using the character table, we can check that for any  $x$  of prime order  $p \geq 5$ , there exists an involution  $y$  such that  $yx$  has order coprime to 2 and  $p$ .  $\square$

This completes the proof of Theorem 1.3.

#### 4. Proof of Theorem 1.6

Note that if there is a unique class of involutions, then  $G$  cannot be a minimal counterexample since Malle, Saxl and Weigel [MSW94] prove that there exist three involutions in  $G_0$  that generate  $G_0$  unless  $G_0 \cong \text{PSU}_3(3)$ . Also, Guralnick and Saxl [GS03] prove that there exist three conjugates of any involution in an almost simple group that generate a subgroup containing the socle when the Lie rank is small. We will appeal to both of these results throughout the proof.

**Lemma 4.1.** *Suppose that  $G_0 \cong A_n$ . Then  $(x, G)$  cannot be a minimal counterexample.*

**Proof.** Suppose that  $(x, G)$  is a minimal counterexample with  $G_0 \cong A_n$ . We may assume by minimality that one of the following four cases holds: (i)  $x = (12)(34)$  and  $n = 5$ ; (ii)  $x = (16)(25)(34)$  and  $n = 7$ ; (iii)  $x = (12)(34)(56)(78)$  and  $n = 8$ ; (iv)  $x$  is an automorphism of  $A_6$  not contained in  $S_6$ . In case (i), let  $g_1 = (12345)$ ,  $g_2 = (345)$  so that  $xx^{g_1} = (13542)$ ,  $xx^{g_2} = (354)$  and so  $\langle x, x^{g_1}, x^{g_2} \rangle \cong A_5$ . In case (ii), let  $g_1 = (1743526)$  and  $g_2 = (23654)$  so that  $xx^{g_1} = (1234567)$ ,  $xx^{g_2} = (12)(56)$ , and  $\langle x, x^{g_1}, x^{g_2} \rangle \cong S_7$ . In case (iii), let  $g_1 = (143)(28567)$ ,  $g_2 = (13)(265874)$ , then  $xx^{g_1} = (1574)(2386)$ ,  $xx^{g_2} = (375)(468)$ , and  $xx^{g_2}x^{g_1} = (1364725)$  and thus  $\langle x, x^{g_1}, x^{g_2} \rangle \cong \text{PSL}_2(7)$ . It is straightforward to eliminate case (iv) in MAGMA.  $\square$

**Lemma 4.2.** *Suppose that  $G_0$  is a simple group of Lie type and  $G_0 \triangleleft G \leq \text{Inndiag}(G_0)$ . Then  $(x, G)$  is not a minimal counterexample.*

**Proof.** If the twisted Lie rank of  $G_0$  is 1, then  $G_0 \cong \text{PSL}_2(q)$ ,  $\text{PSU}_3(q)$ ,  ${}^2B_2(2^a)$ , or  ${}^2G_2(3^a)$ . For all of these groups except  $\text{PSL}_2(q)$ , there is a unique class of involutions in  $\text{Inndiag}(G_0)$  and so [MSW94] implies that  $(x, G)$  is not a minimal counterexample unless  $G_0 \cong \text{PSU}_3(3)$ . And if  $G_0 \cong \text{PSL}_2(q)$ , then there exist three conjugates that generate a group containing  $G_0$  or  $q = 4$  or 5 by [GS03, Lemma 3.1]. So we may assume that the twisted Lie rank of  $G_0$  is at least 2.

First suppose that  $q \geq 4$ . If  $q$  is odd and  $x$  is contained in a maximal parabolic subgroup, then by Lemma 2.2 we may assume that  $x$  acts nontrivially on all of the components of the Levi complement. In fact, the involution  $x$  is always contained in a parabolic subgroup. Indeed, if  $q$  is odd, then  $x$  is semisimple and  $x$  always centralizes a unipotent element  $u$  (see the list of semisimple involutions and their centralizers in [GLS98, Table 4.5.1]) and the Borel–Tits theorem implies that  $C_G(u)$  is contained in a parabolic subgroup of  $G$ . If  $q$  is even then  $x$  is unipotent and contained in a Borel subgroup. By Lemma 2.2, for any two distinct types of parabolic subgroup  $P_1, P_2$ , we may assume that  $x$  acts nontrivially on at least one of the components of the Levi complement of some  $P_i$ . Since  $q \geq 4$ , the only possible components that are contained in Table 1 are of type  $\text{PSL}_2(4)$ ,  $\text{PSL}_2(5)$ , and  $\text{PSL}_2(9)$ .

Now unless

$$G_0 \in \{A_2(q), A_3^\epsilon(q), B_2(q), B_3(q), C_3(q), D_4^\pm(q), {}^3D_4(q), G_2(q) \mid q = 4, 5, \text{ or } 9\},$$

every maximal parabolic subgroup has a component in the Levi complement that is not of type  $\mathrm{PSL}_2(5)$  or  $\mathrm{PSL}_2(9)$  when  $q \geq 5$  is odd, and there exist maximal parabolic subgroups  $P_1, P_2$  both without a type  $\mathrm{PSL}_2(4)$  component in the Levi complements when  $q \geq 4$  is even.

However we can eliminate the groups that have a unique classes of involutions in  $\mathrm{Inndiag}(G_0)$ . So if  $q \geq 4$ ,  $x \in \mathrm{Inndiag}(G_0)$  and  $(x, G)$  is a minimal counterexample, then  $G_0 \cong {}^3D_4(4), A_3^\epsilon(q), B_2(q), B_3(q), C_3(q), G_2(4)$ , or  $D_4^\pm(q)$  for  $q = 4, 5$ , or  $9$ . We can easily eliminate the cases  $A_2(q)$  and  $A_3^\epsilon(q)$  in MAGMA. Now a (unipotent) involution in  ${}^3D_4(4)$  is contained in a subfield subgroup  ${}^3D_4(2)$  (see [Spa82]) and so we can eliminate the case  $G_0 \cong {}^3D_4(4)$ . If  $G_0 \cong G_2(4)$ , then any involution is contained in a subgroup of type  $\mathrm{SL}_3^\pm(4) : 2$  (see [GS03, Proposition 5.6] for example). If  $G_0 \cong B_3(4) \cong C_3(4)$ , then we may assume that  $x$  is contained in an end-node parabolic subgroup  $P$  and not in the unipotent radical of  $P$ ; the Levi complement will be of type  $C_2(4)$  or  $A_2(4)$ . Thus  $G_0 \not\cong C_3(4)$ . The same reasoning eliminates  $D_4^\pm(4)$ . Thus the remaining possibilities for  $q \geq 4$  are

$$G_0 \in \{B_2(4), B_2(5), B_2(9), B_3(5), B_3(9), C_3(5), C_3(9), D_4^\pm(5), D_4^\pm(9), G_2(4)\}.$$

If  $G_0 \cong C_3(5)$  or  $C_3(9)$ , then [LS91, Proposition 1.5] shows that  $x$  stabilizes an orthogonal decomposition  $V = W \oplus W^\perp$ , where  $\dim W = 4$  and  $x$  acts noncentrally on  $W$ . So we can reduce to the case of  $C_2(5)$  or  $C_2(9)$  and  $(x, G)$  cannot be a minimal counterexample. Similarly if  $G_0 \cong B_3(5)$  or  $B_3(9)$ , by [LS91, Proposition 1.5],  $x$  stabilizes an orthogonal decomposition  $V = W \oplus W^\perp$ , where  $\dim W = 5$  or  $6$  and  $x$  acts noncentrally on  $W$ . Since  $\mathrm{P}\Omega_5^\pm(q)$  and  $\mathrm{P}\Omega_6^\pm(q)$  for  $q = 5$  and  $9$  are not listed in Table 1,  $(x, G)$  cannot be a minimal counterexample. Similarly if  $G_0 \cong D_4^\pm(5)$  or  $D_4^\pm(9)$ , then  $x$  will stabilize an orthogonal decomposition as above where  $\dim W = 6$  or  $7$  and  $x$  acts noncentrally on  $W$ . Since  $\mathrm{P}\Omega_6^\pm(q)$  and  $\mathrm{P}\Omega_7(q)$  are not listed in Table 1 for  $q = 5$  or  $9$ ,  $(x, G)$  cannot be a minimal counterexample. So for  $q \geq 4$  it remains to consider

$$G_0 \in \{B_2(4), B_2(5), B_2(9)\}.$$

We can verify in MAGMA that the theorem holds for these groups.

Now suppose that  $q = 3$ . Then  $x$  is contained in a maximal parabolic subgroup, and by Lemma 2.2, we may assume that it acts noncentrally on all of the Levi components. To prove that  $G$  is not a minimal counterexample, it suffices that one of the Levi components is not in Table 1 and is not solvable. Thus the only possibilities with  $q = 3$  are

$$G_0 \in \{A_2(3), A_3(3), {}^2A_2(3), {}^2A_3(3), {}^2A_4(3), {}^2A_5(3), B_n(3), \\ C_3(3), C_4(3), D_4^\epsilon(3), {}^3D_4(3), G_2(3), {}^2G_2(3)\}.$$

If we eliminate the cases where there is a unique class of involutions in  $\mathrm{Inndiag}(G_0)$ , then we may assume that

$$G_0 \in \{A_3(3), {}^2A_2(3), {}^2A_3(3), {}^2A_4(3), {}^2A_5(3), B_n(3), C_3(3), C_4(3), D_4^\epsilon(3)\}.$$

If  $G_0 \cong B_n(3)$ , then by [LS91, Proposition 1.5],  $x$  stabilizes an orthogonal decomposition  $W \oplus W^\perp$ , where  $W$  is chosen so that  $\dim W^\perp$  is minimal, and is therefore at most 2. If  $n \geq 4$  and  $x$  is not a reflection then we can choose  $W$  so that  $x$  acts on  $W$  noncentrally and not as a reflection. Thus  $(x, G)$  cannot be a minimal counterexample if  $G_0 = B_n(3)$  and  $n \geq 4$ . Checking the remaining cases in MAGMA shows that there are no minimal counterexamples when  $q = 3$ .

Now suppose that  $q = 2$  so that  $x$  is unipotent. Then we can use Lemma 2.2. If  $G_0 = A_n(2)$ , then we may assume that  $x$  is contained in a maximal end-node parabolic subgroup  $P$  and not contained in the unipotent radical of  $P$ . Thus we can reduce to the case that  $x \in A_{n-1}(2)$  since there are no inner exceptions in  $A_{n-1}(2)$ . This argument thus reduces to the case of  $G = \mathrm{PSL}_3(2) \cong \mathrm{PSL}_2(7)$ , and [GS03] shows that  $(x, G)$  is not a counterexample. Now suppose that  $G_0 \cong {}^2A_n(2)$ . Then [LS91, Proposition 1.4] shows that  $x$  stabilizes an orthogonal decomposition  $V = W \oplus W^\perp$  such that  $W$  has codimension 1 or 2, and if  $x$  is not a unitary transvection, we can choose  $W$  such that  $x$  does not act on  $W$  trivially, or as a transvection. Therefore if  $n \geq 6$ , then there are no minimal counterexamples with  $G_0 \cong {}^2A_n(2)$ . We verify in MAGMA that the only exceptions when  $n \leq 5$  are the unitary transvections.

Now suppose that  $G_0 \cong B_n(2) \cong C_n(2)$  or  $D_n^\pm(2)$ . Suppose that  $x$  is not a transvection. If  $n \geq 5$ , then we can take an orthogonal decomposition  $V = W \oplus W^\perp$  as above using [LS91, Proposition 1.4] such that  $x$  does not act on  $W$  trivially or as a transvection, and  $\dim W \geq 6$ . Thus  $(x, G)$  cannot be a minimal counterexample when  $n \geq 5$ . Note that  $\mathrm{Sp}_4(2) \cong S_6$  so we can just verify in MAGMA that  $\mathrm{Sp}_6(2)$ ,  $\mathrm{Sp}_8(2)$ , and  $\Omega_8^\pm(2)$  cannot be counterexamples to the theorem.

To complete the analysis when  $q = 2$ , we eliminate the cases  $G_0 \cong {}^3D_4(2)$ ,  $E_6(2)$ ,  ${}^2E_6(2)$ ,  $E_7(2)$ ,  $E_8(2)$ ,  $F_4(2)$ ,  ${}^2F_4(2)$ , and  $G_2(2)$  using MAGMA.  $\square$

We now deal with the cases where the involution  $x$  is not contained in  $\mathrm{Inndiag}(G_0)$ . We note that  $\mathrm{Aut}(G_0)/G_0$  has odd order when  $G_0$  is a Suzuki–Ree group, unless  $G_0 \cong {}^2F_4(2)'$ , and this case is eliminated in MAGMA. We may therefore assume that  $G_0$  is not a Suzuki–Ree group in Lemmas 4.3, 4.4 and 4.5. We use the terminology of [GLS98, 2.5.13].

**Lemma 4.3.** *Suppose that  $G_0$  is a simple group of Lie type and  $x$  is a field automorphism of  $G_0$ . Then  $(x, G)$  is not a minimal counterexample.*

**Proof.** Now suppose that  $x$  is a field automorphism of order 2. By [GL83, 7.2], we may assume that  $x$  is a standard field automorphism.

Now  $q \geq 4$  and  $x$  will act as a field automorphism on a  $\mathrm{SL}_2(q)$  subgroup and so  $(x, G)$  cannot be a minimal counterexample unless  $G_0 = \mathrm{PSL}_2(q)$  or  $q = 4$  or 9. If  $q = 4$  or 9, then we may assume that  $x$  acts as a field automorphism on a subgroup of type  $A_2(q)$ ,  $B_2(q)$ ,  $G_2(q)$  or  ${}^3D_4(q)$ . We can eliminate the first two cases in MAGMA. If  $G_0 \cong G_2(q)$  or  ${}^3D_4(q)$ , then  $x$  normalizes but does not centralize a subgroup of type  $\mathrm{SL}_3(q)$  or  $\mathrm{SL}_2(q^3)$  respectively. So it remains to treat the case where  $x$  is a field automorphism of  $\mathrm{PSL}_2(q)$ . If  $q$  is even, then since  $q \neq 4$ , we have  $q = q_0^2$  where  $q_0 \geq 4$ . But, then there exist  $y$  of order  $q_0 - 1$  and  $z$  of order  $q_0 + 1$  such that  $x, xy$ , and  $xz$  are conjugate, and  $y$  and  $z$  do not commute and thus  $\langle x, xy, xz \rangle$  contains  $\mathrm{PSL}_2(q_0)$ , which is not solvable. If  $q$  is odd, then suppose that  $\mathbb{F}_q^* = \langle w \rangle$ . Let  $\lambda = w^{\frac{(q_0+1)}{2}}$  so that  $\lambda^{q_0} = -\lambda$ . Then  $x$  inverts

$$\begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix}$$

and

$$\begin{pmatrix} 1 & 0 \\ \lambda & 1 \end{pmatrix};$$

thus there exist conjugates of  $x$ ,  $y$  and  $z$  say, such that  $xy$  and  $xz$  are the transvections above. It follows that  $\langle x, y, z \rangle$  is not solvable since  $q > 9$ .  $\square$

**Lemma 4.4.** *Suppose that  $G_0$  is a simple group of Lie type and  $x$  is a graph-field automorphism of  $G_0$ . Then  $(x, G)$  is not a minimal counterexample.*



**Proof.** Suppose that  $x$  is a graph-field automorphism so that  $G_0$  is an untwisted simple group of Lie type. By [GL83, 7.2], we may assume that  $x$  is a standard graph-field involution. Define  $q_0$  by  $q = q_0^2$  as before.

If  $G_0 \cong \text{PSL}_d(q)$ , with  $d \geq 3$ , then  $x$  normalizes a subfield subgroup  $\text{PSL}_d(q_0)$  (acting as a graph automorphism), which is not an exception unless  $G_0 \cong \text{PSL}_4(4)$  ( $\text{PSL}_4(2)$  is in Table 1). We can eliminate this case in MAGMA. If  $G_0 \cong D_n(q)$  and  $n \geq 4$ , then  $x$  acts as a graph-field automorphism on a  $D_{n-1}(q)$  subgroup. Similarly a graph-field automorphism of  $E_6(q)$  acts as a graph-field automorphism on  $A_5(q)$ . If  $G_0 \cong F_4(2^a)$ ,  $G_2(3^a)$ , or  $B_2(2^a)$  then the extraordinary ‘graph’ automorphism squares to a generating field automorphism. So there are involutory graph-field automorphisms (in the sense of [GLS98, 2.5.13]) only when  $a$  is odd. Now if  $a \geq 3$  is odd then  $x$  normalizes a subgroup of type  $F_4(2)$ ,  $G_2(3)$ , or  $B_2(2)$  and thus  $(x, G)$  cannot be a minimal counterexample unless  $G_0 = B_2(2^a)$ . But in this case,  $x$  has centralizer of type  ${}^2B_2(2^a)$  and  $C_{G_0}(x)$  has even index in  $G_0$ ; thus by considering the action of  $x$  on the cosets of  $C_{G_0}(x)$  we see that  $x$  fixes at least two cosets and therefore  $x$  normalizes but does not centralize a type  ${}^2B_2(2^a)$  subgroup (acting as an inner automorphism). It follows that  $(x, G)$  is not a minimal counterexample in this case either. The cases where  $a = 1$  are easily eliminated in MAGMA.  $\square$

**Lemma 4.5.** *Suppose that  $G_0$  is a simple group of Lie type and  $x$  is a graph automorphism of  $G_0$ . Then  $(x, G)$  is not a minimal counterexample.*

**Proof.** In the terminology of [GLS98, 2.5.13], there are no graph automorphisms of  $F_4(2^a)$ ,  $G_2(3^a)$ , or  $B_2(2^a)$ .

If  $G_0 \cong L_3^\epsilon(q)$ , then [GS03, Lemmas 3.2 and 3.3] show that  $(x, G)$  cannot be a minimal counterexample.

If  $G_0 \cong L_4^\epsilon(q)$ , then observe that  $G_0 \cong \text{P}\Omega_6^\epsilon(q)$ , and an involutory graph automorphism of  $L_4^\epsilon(q)$  is contained in  $\text{PCO}_6^\epsilon(q)$ . By [LS91, Propositions 1.4 and 1.5] for example,  $x$  will normalize (and not centralize) a subgroup of type  $\text{P}\Omega_5(q)$ ,  $\text{P}\Omega_4^\pm(q)$ , or  $\text{P}\Omega_3(q)$ . Therefore  $(x, G)$  cannot be a minimal counterexample unless  $q = 2$  or  $q = 3$ . We can verify that Theorem 1.6 holds for  $q = 2$  and 3 using MAGMA.

Suppose that  $G_0 \cong L_d^\epsilon(q)$ ,  $q$  is odd, and  $d \geq 5$ . The class representatives of graph involutions in this case are given in [GLS98, Table 4.5.1] and [LS91, 3.9]. We can deduce from these representatives that if  $d$  is even, then  $x$  will act as a graph automorphism on a type  $\text{PSL}_{d-1}(q)$  or  $\text{PSL}_{d-2}(q)$  subgroup; if  $d$  is odd, then  $x$  will act as a graph automorphism on a type  $\text{PSL}_{d-1}(q)$  subgroup. So since  $(x, G)$  is a minimal counterexample, we can reduce to the case  $G_0 \cong L_4^\epsilon(q)$  or  $L_3^\epsilon(q)$ , which have been eliminated.

Now suppose that  $G_0 \cong L_d^\epsilon(q)$ ,  $q$  is even, and  $d \geq 5$ . The class representatives for graph involutions when  $q$  is even can be found in [Lie87, Lemma 3.7]. There are two classes when  $d$  is even and one class when  $d$  is odd. In all cases,  $x$  normalizes a subgroup of type  $L_{d-1}^\epsilon(q)$  or  $L_{d-2}^\epsilon(q)$ , acting as a graph automorphism. So since  $(x, G)$  is a minimal counterexample, we may assume that  $G_0 \cong L_3^\epsilon(q)$ ,  $L_4^\epsilon(q)$ ,  $L_5^\epsilon(2)$ , or  $L_6^\epsilon(2)$ . The first two possibilities have already been eliminated and we can eliminate the last two possibilities using MAGMA.

If  $x$  is an involutory graph automorphism of  $\text{P}\Omega_d^\pm(q)$ , then  $x \in \text{PCO}_d^\pm(q)$  and we may assume that  $d \geq 8$ . By [LS91, Lemma 3.3] for example, we may assume that  $x$  normalizes but does not centralize a subgroup of type  $\text{P}\Omega_{d-b}^\epsilon(q)$ , where  $b \leq 4$ . Thus  $(x, G)$  cannot be a minimal counterexample unless  $q = 2$  or  $q = 3$ . But if  $d \geq 10$  and  $x$  is not an orthogonal transvection or reflection, then we may assume that  $x$  does not act as orthogonal transvection or reflection on the type  $\text{P}\Omega_{d-b}^\epsilon(q)$  subgroup. We can eliminate the groups  $G_0 \cong \text{P}\Omega_8^\pm(3)$  and  $\text{P}\Omega_8^\pm(2)$  in MAGMA.

If  $G_0 \cong E_6^\epsilon(q)$  and  $x$  is an involutory graph automorphism, then  $x$  normalizes but does not centralize a subgroup of type  $F_4(q)$ ; thus  $(x, G)$  cannot be a minimal counterexample. This follows from an analysis of the standard class representatives of graph involutions found in [Lie87, Lemma 3.6] for  $q$  odd and [AS76, 19.9] for  $q$  even. See the proof of [GS03, Proposition 5.2] for example.  $\square$

**Lemma 4.6.** *If  $G_0$  is a sporadic group then  $(x, G)$  is not a minimal counterexample.*

**Proof.** If  $G_0$  is not the Monster group  $M$  or the Baby Monster group  $B$ , then we can use MAGMA. If there is a unique class of involutions then  $(x, G)$  cannot be a minimal counterexample by [MSW94]. In the other cases, we use the representations in [ABN+] together with the representatives for the conjugacy classes of involutions. We search at random for conjugates  $y$  and  $z$  of  $x$  and test the subgroup  $H = \langle x, y, z \rangle$  for nonsolvability (by searching for  $a, b, c \in H$  of pairwise coprime order such that  $abc = 1$  [Tho68]).

If  $G = B$ , then there are 4 classes of involutions. The centralizer order of an element in class 2A in the Harada–Norton group  $HN$  is divisible by  $5^3$ , therefore such an involution is contained in  $B$ -class 2B. Any involution in  $Th$  is in  $B$ -class 2D by [Wil99, p. 4]. We can verify in MAGMA that an element in class 2A belongs to a triple of conjugates generating a nonsolvable group. If  $x$  belongs to class 2C, then the character table of  $G$  implies that there exist conjugates  $y$  and  $z$  such that  $xy$  has order 19 and  $xz$  has order 33. By analyzing the maximal subgroups, we have  $\langle x, y, z \rangle = B$ .

There are two classes of involutions in the Monster group  $M$ . If  $x$  is in class 2A, then  $x$  is contained in a subgroup isomorphic to  $\text{PSL}_3(2)$ ; for an involution in  $\text{PSL}_3(2)$  in the maximal subgroup  $(\text{PSL}_3(2) \times \text{Sp}_4(4) : 2).2$  must be in class 2A since it centralizes an element of order 17 in  $\text{Sp}_4(4)$  and elements in class 2B do not centralize elements of order 17. Any involution in  $\text{PSU}_3(8)$  is in  $M$ -class 2B by [NW02, 4.5]; thus neither class of involutions can be involved in a minimal counterexample.  $\square$

This completes the proof of Theorem 1.6.

## 5. Proof of Theorem 1.4

### 5.1. Order 9

First suppose that  $x$  has order 9. By Theorem 1.2, if  $(x, G)$  is a minimal counterexample, then  $G_0$  is a simple group of Lie type and  $q = 3$  or  $G_0 \cong \text{PSU}_d(2)$ . Moreover,  $x^3$  is a long root element or a pseudoreflection in each case respectively. We will consider the possible conjugacy classes for  $x$ .

Suppose that  $G_0 \cong \text{PSL}_d(3)$ ,  $\text{PSU}_d(3)$ , or  $\text{PSp}_d(3)$  and  $x^3$  is a transvection. Then  $x$  lifts to an element in  $\text{SL}_d(3)$ ,  $\text{SU}_d(3)$ , or  $\text{Sp}_d(3)$ , with Jordan form  $J_4 J_3^{r_3} J_2^{r_2} J_1^{r_1}$  (and  $r_3$  and  $r_1$  are even in the symplectic case). It is well known that in the linear and unitary cases,  $x$  must be contained in a subgroup of type  $\text{SL}_4(3) \times \text{SL}_{d-4}(3)$  or  $\text{SU}_4(3) \times \text{SU}_{d-4}(3)$ , where  $x$  has order 9 in the first factor. In the symplectic case, we can also assume that  $x \in \text{Sp}_4(3) \times \text{Sp}_{d-4}(3)$  and  $x$  has order 9 in the first factor, for example by [LSar, Theorem 7.1].

Similarly, if  $G_0 = \text{P}\Omega_d^\epsilon(3)$ ,  $x^3$  is a long root element and  $x$  is not in the coset of a graph automorphism, then  $x$  lifts to an element of order 9 in  $\Omega_d^\epsilon(3)$ , which has Jordan form  $J_4^{r_3} J_3^{r_2} J_2^{r_1}$  or  $J_5 J_3^{r_3} J_2^{r_2} J_1^{r_1}$ . Again by [LSar, Theorem 7.1] for example, we may assume that  $x$  is contained in a subgroup of type  $O_8^\epsilon(3) \times O_{d-8}^\epsilon(3)$  or  $O_5(3) \times O_{d-5}^\epsilon(3)$ , in which  $x$  has order 9 in the first factor. Thus we have reduced to the cases  $G_0 = \text{PSL}_4(3)$ ,  $\text{PSU}_4(3)$ ,  $\text{PSp}_4(3) \cong \text{P}\Omega_5(3)$ , or  $\text{P}\Omega_8^\epsilon(3)$ . If  $x$  is in the coset of a graph automorphism (of order 3), then  $G_0 = \text{P}\Omega_8^+(3)$ . It is easily verified in MAGMA that none of these groups is a counterexample, and that neither are the groups with  $G_0 = G_2(3)$ ,  ${}^3D_4(3)$ ,  ${}^2G_2(3)$ .

If  $G_0$  is one of the other exceptional groups defined over  $\mathbb{F}_3$ , then we can find representatives for the conjugacy classes of order 9 using [Miz77, Miz80, Sho74] together with [Law95, Tables D and 9] and [Law98]. Information on the unipotent conjugacy classes of  ${}^2E_6(3)$  was provided by Frank Lübeck using [GHL+96], which the author is most grateful for. In all cases, it is easily seen that  $x$  is contained in an almost simple subgroup and thus cannot be a minimal counterexample.

Suppose  $x^3 \in G$  is a pseudoreflection and  $G_0 = \text{PSU}_d(2)$ . First note that if  $x \in \text{PGU}_d(2)$  and  $x$  does not lift to an element of order 9 in  $\text{GU}_d(2)$ , then the minimal polynomial of  $x$  must be of the form  $t^9 + \mu$ , where  $\mu \in \mathbb{F}_4$ , and  $\mu \neq 0, 1$ . It follows that the eigenvalues of  $x$  must all be 9th roots of  $\mu$ , and the eigenvalues of  $x^3$  must all be cube roots of  $\mu$ ; in particular,  $x^3$  cannot be a pseudoreflection. Thus we may assume that  $x$  lifts to an element of order 9 in  $\text{GU}_d(2)$ , with minimal polynomial  $t^9 - 1$ . The eigenvalues of  $x$  must all be 9th roots of 1, and since  $x \in \text{GU}_d(2)$ , the eigenvalues are permuted by the map  $\lambda \mapsto \lambda^{-2}$ . Thus the primitive 9th roots of 1 must occur as eigenvalues of  $x$  in triples. Suppose that the eigenvalues of the pseudoreflection  $x^3$  are  $a$  with multiplicity 1 and  $b$  with multiplicity  $d - 1$ .

It follows that  $a = 1$ ,  $b$  is a primitive cube root of unity,  $d \equiv 1 \pmod{3}$  and the eigenvalues of  $x$  are  $\phi_1$  with multiplicity 1 where  $\phi_1^3 = 1$ , and  $\phi_2, \phi_2^{-2}, \phi_2^4$ , each with multiplicity  $\frac{d-1}{3}$ , where  $\phi_2$  is a primitive 9th root of unity. Since  $\mathrm{GU}_4(2) \times \mathrm{GU}_3(2) \times \cdots \times \mathrm{GU}_3(2)$  contains an element with the same eigenvalues (and the same Jordan form) we may assume that  $x$  is contained in this subgroup, and we have reduced to the case  $G_0 = \mathrm{PSU}_4(2)$ . This case is easily eliminated using MAGMA.

## 5.2. Order 6

We argue in the same way as in the case where  $x$  has order 9. By Theorem 1.2, if  $(x, G)$  is a minimal counterexample, then  $G_0$  is a simple group of Lie type and  $q = 3$  or  $G_0 \cong \mathrm{PSU}_d(2)$ . Moreover,  $x^2$  is a long root element or a pseudoreflection in each case respectively.

If  $x \in \mathrm{Inndiag}(G_0)$ , then let  $x_s := x^3$  and  $x_u := x^4$ . So  $x = x_s x_u = x_u x_s$ , and  $x_s$  is semisimple and  $x_u$  is unipotent.

**Lemma 5.1.** *If  $G_0 \cong \mathrm{PSL}_d(3)$ ,  $\mathrm{PSp}_d(3)$ , or  $\mathrm{PSU}_d(3)$ ,  $x$  is inner-diagonal and  $(x, G)$  is a minimal counterexample, then  $x$  lifts to an element of order 6 in  $\mathrm{GL}_d(3)$ ,  $\mathrm{GSp}_d(3)$ , or  $\mathrm{GU}_d(3)$  respectively.*

**Proof.** In the linear and symplectic cases, the only central elements are  $\pm I_d$ , so either  $(xz)^6 = I_d$  for all central elements  $z$ , or  $(xz)^6 = -I_d$  for all  $z$ . In the latter case, let  $y = xz$ . Then the minimal polynomial of  $y$  divides  $t^6 + 1 = (t^2 + 1)^3$ . Moreover, since  $y^2$  is a scalar multiple of a transvection and  $t^2 + 1$  is irreducible over  $\mathbb{F}_3$ , it follows that the minimal polynomial is  $(t^2 + 1)^2$ . However, this would imply that  $y^2$  had  $(t + 1)^2$  occurring twice as an invariant factor when it should occur at most once. So  $x$  lifts to an element of order 6 in the linear and symplectic cases.

In the unitary case, let  $i \in \mathbb{F}_{3^2}$  be a primitive 4th root of unity so that  $Z(\mathrm{GU}_d(3)) = \langle iI_d \rangle$ . If  $(xz)^6 = -I_d$ , then  $(xzi)^6 = -I_d(-1)^3 = 1$  and  $x$  lifts to an order 6 element. The only other possibility is that  $(xz)^6 = \pm iI_d$ , in which case the minimal polynomial of  $y = xz$  would divide  $(t^2 \pm i)^3$ . As before, since  $y^2$  is a scalar multiple of a transvection, the minimal polynomial of  $y$  would divide  $(t^2 \pm i)^2$ . Now  $t^2 \pm i$  is irreducible, and if  $y$  had minimal polynomial  $t^2 \pm i$ , then  $y$  would have projective order 2. Thus the only possibility is that  $m_y(t) = (t^2 \pm i)^2$ , but then  $(t \pm i)^2$  would occur twice as an invariant factor of  $y^2$ . So  $x$  lifts to an element of order 6 in the unitary case as well.  $\square$

**Lemma 5.2.** *If  $G \leq \mathrm{PGL}_d(3)$ ,  $\mathrm{PGSp}_d(3)$  or  $\mathrm{PGU}_d(3)$  and  $x \in G$  has order 6, then there exists  $g \in G$  such that  $\langle x, x^g \rangle$  is not solvable.*

**Proof.** By Lemma 5.1, we can lift  $x$  to an element of order 6 in  $\mathrm{GL}_d(3)$ ,  $\mathrm{GSp}_d(3)$ , or  $\mathrm{GU}_d(3)$ . Since  $x = x_u x_s = x_s x_u$  and  $x_u$  is a transvection, the minimal polynomial of  $x$  divides  $(t^2 - 1)^2$ . Now  $x^2$  is a transvection and its invariant factors are  $(t - 1)^2$  with multiplicity one and  $(t - 1)$  with multiplicity  $d - 2$ ; thus the minimal polynomial of  $x$  is not  $(t^2 - 1)^2$  otherwise the multiplicity of  $(t - 1)^2$  in the invariant factors of  $x^2$  would be at least 2. In fact, we can show that the invariant factors of  $x$  must be  $t + \epsilon_1$  with multiplicity  $m_1$ ,  $t^2 - 1$  with multiplicity  $m_2$ , and  $(t^2 - 1)(t - \epsilon_2)$  with multiplicity 1, where  $\epsilon_i = \pm 1$ . In the linear and unitary cases, there exists  $y \in \mathrm{GL}_3^\epsilon(3) \times \mathrm{GL}_{d-3}^\epsilon(3)$  with  $y$  of order 6 in the first factor, having the same invariant factors as  $x$ . Thus  $x$  and  $y$  are conjugate (see [Wal63] for example) and we can reduce to the cases  $G_0 = \mathrm{PSL}_3(3)$  and  $\mathrm{PSU}_3(3)$ .

In the symplectic case we consider the elementary divisors of  $x$ , which must be  $(t - \epsilon)^2$  with multiplicity 1,  $(t + \epsilon)$  with multiplicity  $m_1 \geq 1$ , and  $(t - \epsilon)$  with multiplicity  $m_2$  ( $\epsilon = \pm 1$ ). By considering the vector space  $V$  as an  $\mathbb{F}_3\langle x \rangle$ -module, we can see that  $V$  decomposes as

$$V = U \oplus U' \cong \mathbb{F}_q(t)/(t - \epsilon)^2 \oplus (\mathbb{F}_q(t)/(t + \epsilon) \oplus \cdots \oplus \mathbb{F}_q(t)/(t \pm 1)).$$

Since  $x^2$  is a symplectic transvection, there exist  $t \in U$ , and  $\lambda \in \mathbb{F}_3$  such that  $x^2 : v \rightarrow v + \lambda(t, v)t$  for all  $v \in V$ . Moreover, since  $U \cong \mathbb{F}_q(t)/(t - \epsilon)^2$ , there exists  $u \in U$  such that  $(u, t) \neq 0$  and thus  $U = \langle u, t \rangle$  is a 2-dimensional, nondegenerate subspace. Now consider  $V = U \perp U^\perp$ . Observe that  $x$  has order 1 or 2 on  $U^\perp$  and in particular  $x$  has a semisimple action on  $U^\perp$ . Thus  $U^\perp = \bigoplus_i U_i$  where

the  $U_i$  are nondegenerate  $x$ -invariant 1- or 2-dimensional subspaces. Moreover, there exists an  $x$ -invariant decomposition  $V = (U \oplus U_j) \oplus (U \oplus U_j)^\perp$  into nondegenerate subspaces of dimension 4 and  $d-4$ , and  $x$  has order 6 on  $U \oplus U_j$ ; thus we can reduce to the case  $G_0 = \mathrm{PSp}_4(3)$ . We can easily verify in MAGMA that  $G_0 = \mathrm{PSL}_3(3)$ ,  $\mathrm{PSU}_3(3)$  and  $\mathrm{PSp}_4(3)$  are not counterexamples to the theorem.  $\square$

**Lemma 5.3.** *If  $G$  is an orthogonal group and  $x$  has projective order 6, then there exists  $g \in G$  such that  $\langle x, x^g \rangle$  is not solvable.*

**Proof.** If  $x$  is contained in  $\mathrm{PCO}_d^\epsilon(3)$ , where  $x^2$  is a long root element and  $x^3$  is an involution, then  $x$  will lift to an element  $y$  of order 6 or 12 in  $\mathrm{CO}_d^\epsilon(3)$ .

Now  $l = y^{|y|/3}$  is a long root element, and the long root elements are all conjugate, so we may assume that

$$l: v \rightarrow v + (v, e_2)e_1 - (v, e_1)e_2,$$

where  $\{e_1, f_1, e_2, f_2, \dots\}$  is a basis for  $V$ ,  $(e_i, f_j) = \delta_{ij}$  and  $(e_i, e_j) = (f_i, f_j) = 0$ .

Since the elementary divisors for  $l$  are  $(t-1)^2$  with multiplicity 2 and  $(t-1)$  with multiplicity  $d-2$ , the possibilities for the elementary divisors of  $y$  are as follows:

- (1)  $(t-\eta)^2$  with multiplicity 2,  $(t+\eta)$  with multiplicity  $m_1$  ( $m_1 \geq 1$  if  $\eta = 1$ ), and  $(t-\eta)$  with multiplicity  $m_2$  ( $\eta = \pm 1$ );
- (2)  $(t-1)^2$  with multiplicity 1,  $(t+1)^2$  with multiplicity 1,  $(t+1)$  with multiplicity  $m_1$  and  $(t-1)$  with multiplicity  $m_2$ ;
- (3)  $(t^2+1)^2$  with multiplicity 1, and  $(t^2+1)$  with multiplicity  $(d-4)/2$ .

So as an  $\mathbb{F}_3\langle y \rangle$ -module,

$$V = U_1 \oplus U_2 \oplus \cdots \oplus U_k$$

where  $U_i \cong \mathbb{F}_3(t)/f_i(t)$ , and  $f_i(t)$  is the  $i$ th elementary divisor of  $y$ . Set  $U = U_1 \oplus U_2$  in the first and second cases and set  $U = U_1$  in the third case; so  $U$  is 4-dimensional as a vector space. Now considering  $U$  as an  $\mathbb{F}_3\langle l \rangle$ -module, we have  $U = W_1 \oplus W_2$  where  $W_i \cong \mathbb{F}_3(t)/(t-1)^2$ , and we claim that  $U$  is a nondegenerate subspace of  $V$ . For there exists  $v_1 \in W_1$  such that  $v_1' - v_1 = \lambda_1 e_1 + \lambda_2 e_2 \neq 0$  and similarly there exists  $v_2 \in W_2$  such that  $v_2' - v_2 = \mu_1 e_1 + \mu_2 e_2 \neq 0$ . Since  $\lambda_1 e_1 + \lambda_2 e_2$  and  $\mu_1 e_1 + \mu_2 e_2$  are linearly independent, it follows that there exist constants  $a_1, a_2, b_1, b_2$  such that  $v_1' = a_1 v_1 + a_2 v_2$ ,  $v_2' = b_1 v_1 + b_2 v_2$ , and  $(v_i', e_j) = \delta_{ij}$  for  $i, j \in \{1, 2\}$ . Now it is easy to check that  $U = \langle e_1, e_2, v_1', v_2' \rangle$  is a nondegenerate space. For if

$$w = ae_1 + be_2 + a'v_1' + b'v_2'$$

is a degenerate vector in  $U$ , then  $(w, e_1) = (w, e_2) = 0$ ; so  $a' = b' = 0$ . Thus  $w = ae_1 + be_2$  and  $(w, v_1') = (w, v_2') = 0$ ; so  $a = b = 0$ ,  $w = 0$ , and  $U$  is nondegenerate. Now  $V = U \oplus U^\perp$ , and  $y$  has projective order 1 or 2 on  $U^\perp$ . In particular,  $y$  has a semisimple action on  $U^\perp$  and there exists a nondegenerate  $y$ -invariant subspace  $U' \leq U^\perp$  of dimension 1 or 2 such that  $y$  has projective order 6 on  $U \perp U'$ . Thus we may assume that  $d \leq 6$ , but then  $G$  is isomorphic to a linear, unitary or symplectic group.  $\square$

**Lemma 5.4.** *Suppose that  $G \leq \mathrm{PGU}_d(2)$  ( $d \geq 4$ ), that  $x$  has order 6, and that  $x^2$  is a pseudoreflection. Then there exists  $g \in G$  such that  $\langle x, x^g \rangle$  is not solvable.*

**Proof.** First observe that  $x$  lifts to an element  $y$  of order 6 in  $\mathrm{GU}_d(2)$ . Indeed, for any lift  $y$  of  $x$ , we have  $y^2 = zr$  where  $z \in Z(\mathrm{GU}_d(2))$ , and  $r$  is a pseudoreflection. But then  $y^6 = (zr)^3 = 1$  since  $Z(\mathrm{GU}_d(2))$  has order 3.

Since  $x^2$  is a pseudoreflection, we have  $C_{\mathrm{GU}_d(2)}(x^2) \cong \mathrm{GU}_1(2) \times \mathrm{GU}_{d-1}(2)$  and  $x \in C_G(x^2)$ . Moreover, by multiplying  $x$  by  $z \in Z(\mathrm{GU}_d(2))$  if necessary, we may assume that  $x$  has order 3 on the first component, and 2 on the second component. Now in  $\mathrm{GU}_{d-1}(2)$ , two unipotent elements are conjugate if and only if they have the same Jordan form (see [Wal63] for example or [LSar]). But the Jordan form of an involution is of the form  $J_2^r, J_1^{d-1-2r}$ , and so there exists a conjugate of  $x$  that is contained in  $\mathrm{GU}_1(2) \times \mathrm{GU}_4(2) \times \mathrm{GU}_{d-5}(2)$ , and on which  $x$  has order 3 on the first component, and 2 on the second component. So we may assume that  $4 \leq d \leq 5$ , and we can eliminate these cases in MAGMA.  $\square$

**Lemma 5.5.** *Suppose that  $x$  is an inner-diagonal automorphism of an exceptional group defined over  $\mathbb{F}_3$ . Then  $(x, G)$  is not a minimal counterexample.*

**Proof.** We can verify the lemma using MAGMA. For the smaller groups, we can calculate the conjugacy classes directly. For the larger groups we can use the Groups of Lie type package in MAGMA to construct a Sylow 2-subgroup  $S$  of  $C = C_G(y)$ , where  $y$  is a long root element. We can then calculate the conjugacy classes of  $S$ , to find the class representatives  $s_1, s_2, \dots, s_k$  of involutions in  $S$ . Then every element  $x$  of order 6 in  $G$  such that  $x^2$  is a long root element is conjugate to at least one element in  $\{ys_1, ys_2, \dots, ys_k\}$ . Now for each  $x = ys_i$ , we can search for a random conjugate  $x^g$  such that  $\langle x, x^g \rangle$  is not solvable.  $\square$

**Lemma 5.6.** *If  $x \notin \mathrm{Inndiag}(G_0)$ , then  $(x, G)$  is not a minimal counterexample.*

**Proof.** Suppose that  $x^2$  is a transvection and  $x^3$  is a graph automorphism. If  $G_0 \cong \mathrm{PSL}_d(3)$  and  $d$  is even, then there are three classes of graph automorphism. Representatives for the three classes are  $\iota S$ ,  $\iota S^+$  and  $\iota S^-$  where  $\iota$  is the inverse transpose automorphism (see [LS91, 3.9]). Their centralizers are of type  $\mathrm{Sp}_d(3)$ ,  $O_d^+(3)$  and  $O_d^-(3)$  respectively. Now  $x = x^4 x^3$ , and  $x^4$  is a transvection so there exists  $a \in V$  such that

$$x^4 : v \rightarrow v + f(v)a,$$

where  $f$  is a linear functional on  $V$ ,  $\dim \ker f = d - 1$ , and  $f(a) = 0$ . Now all of the graph automorphisms above stabilize a subgroup of type  $\mathrm{GL}_{d-2}(3) \times \mathrm{GL}_2(3)$ . We can conjugate  $x$  by  $h \in C_G(x^3)$  (of type  $\mathrm{Sp}_d(3)$ ,  $O_d^\pm(3)$ ) so that  $h(a) \in U$  where  $U$  is the subspace of  $V$  corresponding to the subgroup  $\mathrm{GL}_{d-2}(3)$ . Thus we can consider  $x$  acting as an automorphism on  $\mathrm{GL}_{d-2}(3)$ . There is only one class of graph involutions when  $d$  is odd, with representative  $\iota$ , and centralizer of type  $O_d(3)$ . We can make the same reduction here. So it suffices to deal with cases where  $d \leq 4$ . It is easy to eliminate these cases in MAGMA.

The case where  $G_0 \cong \mathrm{PSU}_d(3)$  is very similar. In this case,  $x^4$  is a unitary transvection and  $x^3$  is a graph automorphism. The classes of involutory graph automorphisms are described in [GLS98, Table 4.5.1]. When  $d$  is even, there are three classes as in the linear case with centralizers of type  $O_d^+(3)$ ,  $O_d^-(3)$ , and  $\mathrm{Sp}_d(3)$ . These classes are described explicitly in [Lie87, p. 43] and [LS91, p. 288], and we see that each class normalizes a subgroup of type  $\mathrm{GU}_{d-2}(3) \times \mathrm{GU}_2(3)$  or  $\mathrm{GU}_{d-1}(3) \times \mathrm{GU}_1(3)$ . In particular, there exists an  $x^3$  invariant, nondegenerate subspace  $U$  of  $V$  of dimension  $d - 2$  or  $d - 1$ . Moreover, as in the linear case we can take  $h \in C_G(x^3)$  such that  $h(a) \in U$ , and so we may assume that  $x^4$  acts a unitary transvection on  $U$ . Similarly, when  $d$  is odd, there is only one class of graph involutions and [Lie87] and [LS91] show that  $x^3$  normalizes a subgroup of type  $\mathrm{GU}_{d-1}(3)$ ; thus we may assume that  $x$  normalizes this subgroup and has order 6 on it. Therefore, it suffices to check the cases  $G_0 = \mathrm{PSU}_4(3)$  and  $G_0 = \mathrm{PSU}_3(3)$  in MAGMA.

Next, suppose that  $G_0 \cong \mathrm{PSU}_d(2)$ ,  $x^3$  is an involutory graph automorphism, and  $x^4$  is a pseudoreflection. If  $d$  is even, then there are two classes of graph involutions, with centralizers of type  $\mathrm{Sp}_d(2)$

and  $C_{\mathrm{Sp}_d(2)}(t)$  where  $t$  is a transvection in  $\mathrm{Sp}_d(2)$ . In both cases  $C_{\mathrm{GU}_d(2)}(x^3) \leq \mathrm{Sp}_d(2)$  and the pseudoreflexion  $y = x^4$  is contained in  $C_{\mathrm{GU}_d(2)}(x^3)$  and therefore satisfies  $y^T J y = J$  for some invertible symmetric matrix  $J$ . However this implies that  $y$  is conjugate to its inverse, which is impossible for such a pseudoreflexion. If  $d$  is odd, then there is one class of graph involutions, and we may therefore assume that  $x^3$  acts as a standard field automorphism on matrix entries, with centralizer of type  $O_d^+(2)$  (see [AS76, 19.9]). The same argument as for the  $d$  odd case implies that the pseudoreflexion  $y = x^4$  is conjugate to its inverse, which again is a contradiction.  $\square$

This completes the proof of Theorem 1.4.

## Acknowledgments

The author would like to thank Frank Lübeck for providing information on the unipotent conjugacy classes of  ${}^2E_6(3)$  and the referees for their careful reading of the paper and for many helpful comments.

## References

- [ABN+] Rachel Abbott, John N. Bray, Simon Nickerson, Steve Linton, Simon P. Norton, Richard Parker, Ibrahim Suleiman, Jonathan Tripp, Peter Walsh, Robert A. Wilson, A *www-ATLAS* of finite group representations.
- [AG84] M. Aschbacher, R. Guralnick, Some applications of the first cohomology group, *J. Algebra* 90 (2) (1984) 446–460, MR 760022 (86m:20060).
- [AS76] Michael Aschbacher, Gary M. Seitz, Involutions in Chevalley groups over fields of even order, *Nagoya Math. J.* 63 (1976) 1–91, MR 0422401 (54 #10391).
- [BCP97] Wieb Bosma, John Cannon, Catherine Playoust, The Magma algebra system. I. The user language, in: *Computational Algebra and Number Theory*, London, 1993, *J. Symbolic Comput.* 24 (3–4) (1997) 235–265, MR 1484478.
- [Bur07] Timothy C. Burness, Fixed point ratios in actions in finite classical groups. II, *J. Algebra* 309 (1) (2007) 80–138, MR 2301234 (2008a:20003).
- [FGG10] Paul Flavell, Simon Guest, Robert Guralnick, Characterizations of the solvable radical, *Proc. Amer. Math. Soc.* 138 (4) (2010) 1161–1170, MR 2578510 (2011d:20030).
- [GAP08] The GAP Group, GAP – Groups, Algorithms, and Programming, Version 4.4.12, 2008.
- [GGKP10] Nikolai Gordeev, Fritz Grunewald, Boris Kunyavskii, Eugene Plotkin, From Thompson to Baer–Suzuki: a sharp characterization of the solvable radical, *J. Algebra* 323 (10) (2010) 2888–2904, MR 2609180 (2011d:20031).
- [GHL+96] Meinolf Geck, Gerhard Hiss, Frank Lübeck, Gunter Malle, Götz Pfeiffer, CHEVIE – a system for computing and processing generic character tables, in: *Computational Methods in Lie Theory*, Essen, 1994, *Appl. Algebra Engrg. Comm. Comput.* 7 (3) (1996) 175–210, MR 1486215 (99m:20017).
- [GL83] Daniel Gorenstein, Richard Lyons, The local structure of finite groups of characteristic 2 type, *Mem. Amer. Math. Soc.* 42 (276) (1983), vii+731, MR 690900 (84g:20025).
- [GLS98] Daniel Gorenstein, Richard Lyons, Ronald Solomon, The Classification of the Finite Simple Groups, Number 3, *Math. Surveys Monogr.*, vol. 40, American Mathematical Society, Providence, RI, 1998, Part I, Chapter A: Almost simple  $K$ -groups, MR 1490581 (98j:20011).
- [GPPS99] Robert Guralnick, Tim Penttilä, Cheryl E. Praeger, Jan Saxl, Linear groups with orders having certain large prime divisors, *Proc. Lond. Math. Soc.* (3) 78 (1) (1999) 167–214, MR 1658168 (99m:20113).
- [GS03] Robert M. Guralnick, Jan Saxl, Generation of finite almost simple groups by conjugates, *J. Algebra* 268 (2) (2003) 519–571, MR 2009321 (2005f:20057).
- [Gue10] Simon Guest, A solvable version of the Baer–Suzuki theorem, *Trans. Amer. Math. Soc.* 362 (11) (2010) 5909–5946, MR 2661502 (2011h:20040).
- [KL90] Peter Kleidman, Martin Liebeck, *The Subgroup Structure of the Finite Classical Groups*, London Math. Soc. Lecture Note Ser., vol. 129, Cambridge University Press, Cambridge, 1990, MR 1057341 (91g:20001).
- [Kle88a] Peter B. Kleidman, The maximal subgroups of the Chevalley groups  $G_2(q)$  with  $q$  odd, the Ree groups  ${}^2G_2(q)$ , and their automorphism groups, *J. Algebra* 117 (1) (1988) 30–71, MR 955589 (89j:20055).
- [Kle88b] Peter B. Kleidman, The maximal subgroups of the Steinberg triality groups  ${}^3D_4(q)$  and of their automorphism groups, *J. Algebra* 115 (1) (1988) 182–199, MR 937609 (89f:20024).
- [Law95] R. Lawther, Jordan block sizes of unipotent elements in exceptional algebraic groups, *Comm. Algebra* 23 (11) (1995) 4125–4156, MR 1351124 (96h:20084).
- [Law98] R. Lawther, Correction to: “Jordan block sizes of unipotent elements in exceptional algebraic groups” [*Comm. Algebra* 23 (1995), no. 11, 4125–4156; MR 1351124 (96h:20084)], *Comm. Algebra* 26 (8) (1998) 2709, MR 1627924 (99f:20073).
- [Lie87] Martin W. Liebeck, The classification of finite simple Moufang loops, *Math. Proc. Cambridge Philos. Soc.* 102 (1) (1987) 33–47, MR 886433 (88g:20146).
- [LS91] Martin W. Liebeck, Jan Saxl, Minimal degrees of primitive permutation groups, with an application to monodromy groups of covers of Riemann surfaces, *Proc. Lond. Math. Soc.* (3) 63 (2) (1991) 266–314, MR 1114511 (92f:20003).

- [LS03] Martin W. Liebeck, Gary M. Seitz, A survey of maximal subgroups of exceptional groups of Lie type, in: Groups, Combinatorics & Geometry, Durham, 2001, World Sci. Publ., River Edge, NJ, 2003, pp. 139–146, MR 1994964 (2004f:20089).
- [LSar] Martin Liebeck, Gary M. Seitz, Unipotent and Nilpotent Classes in Simple Algebraic Groups and Lie Algebras, Math. Surveys Monogr., Amer. Math. Soc., 2012.
- [Mal91] Gunter Malle, The maximal subgroups of  ${}^2F_4(q^2)$ , J. Algebra 139 (1) (1991) 52–69, MR 1106340 (92d:20068).
- [Miz77] Kenzo Mizuno, The conjugate classes of Chevalley groups of type  $E_6$ , J. Fac. Sci. Univ. Tokyo Sect. IA Math. 24 (3) (1977) 525–563, MR 0486170 (58 #5951).
- [Miz80] Kenzo Mizuno, The conjugate classes of unipotent elements of the Chevalley groups  $E_7$  and  $E_8$ , Tokyo J. Math. 3 (2) (1980) 391–461, MR 605099 (82m:20046).
- [MSW94] Gunter Malle, Jan Saxl, Thomas Weigel, Generation of classical groups, Geom. Dedicata 49 (1) (1994) 85–116, MR 1261575 (95c:20068).
- [NW02] Simon P. Norton, Robert A. Wilson, Anatomy of the Monster. II, Proc. Lond. Math. Soc. (3) 84 (3) (2002) 581–598, MR 1888424 (2003b:20023).
- [Sho74] Toshiaki Shoji, The conjugacy classes of Chevalley groups of type  $(F_4)$  over finite fields of characteristic  $p \neq 2$ , J. Fac. Sci. Univ. Tokyo Sect. IA Math. 21 (1974) 1–17, MR 0357641 (50 #10109).
- [Spa82] N. Spaltenstein, Caractères unipotents de  ${}^3D_4(\mathbb{F}_q)$ , Comment. Math. Helv. 57 (4) (1982) 676–691, MR 694610 (84k:20018).
- [Ste68] Robert Steinberg, Lectures on Chevalley Groups, Yale University, New Haven, CT, 1968, notes prepared by John Faulkner and Robert Wilson, MR 0466335 (57 #6215).
- [Suz62] Michio Suzuki, On a class of doubly transitive groups, Ann. of Math. (2) 75 (1962) 105–145, MR 0136646 (25 #112).
- [Tho68] John G. Thompson, Nonsolvable finite groups all of whose local subgroups are solvable, Bull. Amer. Math. Soc. 74 (1968) 383–437, MR 0230809 (37 #6367).
- [Wal63] G.E. Wall, On the conjugacy classes in the unitary, symplectic and orthogonal groups, J. Aust. Math. Soc. 3 (1963) 1–62, MR 0150210 (27 #212).
- [War66] Harold N. Ward, On Ree's series of simple groups, Trans. Amer. Math. Soc. 121 (1966) 62–89, MR 0197587 (33 #5752).
- [Wil99] Robert A. Wilson, The maximal subgroups of the Baby Monster. I, J. Algebra 211 (1) (1999) 1–14, MR 1656568 (2000b:20016).