Siberian Mathematical Journal, *Vol.* 51, *No.* 4, *pp.* 610–615, 2010

STRONG REALITY OF FINITE SIMPLE GROUPS

E. P. Vdovin and A. A. Gal′t

UDC 512.542

Abstract: The classification of finite simple strongly real groups is complete. It is easy to see that strong reality for every nonabelian finite simple group is equivalent to the fact that each element can be written as a product of two involutions. We thus obtain a solution to Problem 14.82 of the Kourovka Notebook from the classification of finite simple strongly real groups.

Keywords: finite group of Lie type, strongly real element, conjugacy class, involution

Introduction

In this article we solve Problem 14.82 from the Kourovka Notebook [1].

Problem 1 [1, 14.82]. Find all finite simple groups whose every element is a product of two involutions.

Since each involution of a nonabelian finite simple group lies in an elementary abelian subgroup of order 4; i.e., for every involution t there exists an involution $s \neq t$ commuting with t, Problem 14.82 is equivalent to that of the classification of finite simple strongly real groups. Recall that an element x of G is called *real* (*strongly real*), if x and x^{-1} are conjugate in G (respectively, are conjugate by an involution in G). A group G is called *real* (*strongly real*), if all elements of G are real (strongly real). Thus, if the order of x is not equal to 1 or 2 then x can be written as a product of two involutions s and t if and only if x is strongly real. Indeed, if t is an involution inverting x and $|x| > 2$ then t and tx are involutions and $x = t \cdot tx$. Conversely, if there exist involutions s and t with $x = st$ then $x^t = ts = x^{-1}$; i.e., x is strongly real. The fact that in finite simple groups each element of order at most 2 can be written as a product of two involutions follows from the Feit–Thompson Odd Order Theorem and the note above.

The problem of reality and strong reality of finite simple groups and the groups in some sense close to simple was studied by many authors, see [2–13]. In particular, the classification of finite simple real groups is obtained in [2]. Thus, it suffices to check what finite simple real groups are strongly real in order to solve Problem 14.82. All strongly real alternating and sporadic groups are found respectively in [3, 4]. It is proven in [5–7] that the symplectic groups $\mathrm{PSp}_{2n}(q)$ are strongly real if and only if $q \not\equiv 3 \pmod 4$. The strong reality of $\Omega^{\varepsilon}_{4n}(q)$ for q even is proven in [8]. The strong reality of $\mathrm{P}\Omega^{-}_{4n}(q)$ for q odd is proven in [9]. Moreover, [10, Theorem 8.5] implies that if q is odd then $\mathrm{P}\Omega^{+}_{4n}(q)$ and $\Omega_{2n+1}(q)$, together with $\mathrm{P}\Omega^{-}_{4n}(q)$, are strongly real if $q \equiv 1 \pmod 4$, while $\Omega_9(q)$ and $\mathrm{P}\Omega^{+}_{8}(q)$ are also strongly real if $q \equiv 3 \pmod 4$. In the present paper the following is proven.

Theorem 1 (Main Theorem). *$G = {}^3D_4(q)$ is strongly real.*

The theorem, together with [2–10], implies the following theorems.

Theorem 2. *Each finite simple real group is strongly real.*

The authors were supported by the Russian Foundation for Basic Research (Grants 08–01–00322, 10–01–00391, and 10–01–90007), the Russian Federal Agency for Education (Grant 2.1.1.419), and the Federal Target Program (State Contract 02.740.11.0429). The first author gratefully acknowledges the support from the Deligne 2004 Balzan Prize in Mathematics and the Lavrent′ev Young Scientists Competition of the Russian Academy of Sciences (Resolution No. 43 of 04.02.2010).

Novosibirsk. Translated from *Sibirskiĭ Matematicheskiĭ Zhurnal*, Vol. 51, No. 4, pp. 769–777, July–August, 2010. Original article submitted May 25, 2010.

Theorem 3. *Every element of a finite simple group G can be written as a product of two involutions if and only if G is isomorphic to one of the following groups:*

(1) $\mathrm{PSp}_{2n}(q)$ *for* $q \not\equiv 3 \pmod 4$, $n \geq 1$;
(2) $\Omega_{2n+1}(q)$ *for* $q \equiv 1 \pmod 4$, $n \geq 3$;
(3) $\Omega_9(q)$ *for* $q \equiv 3 \pmod 4$;
(4) $\mathrm{P}\Omega^-_{4n}(q)$ *for* $n \geq 2$;
(5) $\mathrm{P}\Omega^+_{4n}(q)$ *for* $q \not\equiv 3 \pmod 4$, $n \geq 3$;
(6) $\mathrm{P}\Omega^+_8(q)$;
(7) ${}^3D_4(q)$;
(8) A_{10}, A_{14}, J_1, J_2.

Theorem 3 gives a complete solution to Problem 14.82 from the Kourovka Notebook.

1. Preliminary Results

Our notation for finite groups agrees with that of [14]. The notation and basic facts for finite groups of Lie type and linear algebraic groups can be found in [15]. A finite group G is said to be a *central product* of subgroups A and B (which is denoted by $A \circ B$) if $G = AB$ and the derived subgroup $[A, B]$ is trivial. The order of a group G and the order of an element $g \in G$ we denote by $|G|$ and $|g|$. If X is a subset of G and H is a subgroup of G then the centralizer of X in G and the normalizer of H in G are denoted by $C_G(X)$ and $N_G(H)$, respectively. Given a subset X of G, by $\langle X \rangle$ we denote the subgroup that is generated by X. A finite field of order q we denote by $\mathbb{F}_q$, while p always stands for its characteristic; i.e., $q = p^\alpha$ for some positive integer α. By e we denote the identity element of a group, while 1 stands for the unit of a field.

Let $\overline{G}$ be a simple connected algebraic group over the algebraic closure $\overline{\mathbb{F}}_p$ of a finite field $\mathbb{F}_p$. A surjective endomorphism σ of $\overline{G}$ is called a *Steinberg endomorphism* (see [15, Definition 1.15.1]), if the set of σ-stable points $\overline{G}_\sigma$ is finite. The group $O^{p'}(\overline{G}_\sigma)$ is known to be finite and of Lie type, and each finite group of Lie type can be obtained in this way (notice that given a finite group of Lie type a corresponding algebraic group and a Steinberg map are not uniquely determined in general). More detailed definitions and related results can be found in [15, Sections 1.5 and 2.2]. If $\overline{G}$ is simply connected then $\overline{G}_\sigma = O^{p'}(\overline{G}_\sigma)$ by [15, Theorem 2.2.6(f)]. Moreover, [16, Proposition 2.10] implies that the centralizer of every semisimple element is a reductive subgroup of maximal rank in $\overline{G}$.

If G is isomorphic to ${}^3D_4(q)$ then the corresponding algebraic group $\overline{G}$ can be chosen simply connected. We always assume that $\overline{G}$ is simply connected in this case, i.e., for every $G = {}^3D_4(q)$ a simply connected connected simple linear algebraic group $\overline{G} = D_4(\overline{\mathbb{F}}_q)$, where $\overline{\mathbb{F}}_q$ is the algebraic closure of $\mathbb{F}_q$, and a Steinberg endomorphism σ are chosen so that $G = \overline{G}_\sigma$. In particular, the centralizer of every semisimple element in $\overline{G}$ is connected. If $\overline{T}$ is a σ-stable maximal torus of $\overline{G}$ then $T = \overline{T} \cap G$ is called a *maximal torus* of a finite group of Lie type G. If $\overline{R} \leq \overline{S}$ are σ-stable subgroups of $\overline{G}$, $R = \overline{R} \cap G$, and $S = \overline{S} \cap G$; then $N_{\overline{S}}(\overline{R}) \cap G$ is denoted by $N(S, R)$. Notice that $N(S, R) \leq N_S(R)$, but the equality is not true in general. For every $x \in G$ there exist unique elements $s, u \in G$ such that $x = su = us$, s is semisimple, and u is unipotent. Furthermore, s is the p'-part of x, while u is the p-part of x. This is called the *Jordan decomposition* of x.

By [9, Lemma 10], all semisimple elements of ${}^3D_4(q)$ are strongly real. Moreover, the conjugating involution found in the proof of [9, Lemma 10] satisfies the following:

Lemma 1. *For every maximal torus T of ${}^3D_4(q)$ there exists an involution $x \in N(G, T)$ such that $t^x = t^{-1}$ for every $t \in T$. In particular, for every $t \in T$, both xt and tx are involutions inverting every element of T.*

All statements from the next lemma are immediate from the structure of projective linear groups of degree 2.

Lemma 2. *The following hold:*

(1) $\mathrm{PSL}_2(q)$ *is strongly real if and only if* $q \not\equiv 3 \pmod 4$.

(2) $\mathrm{PGL}_2(q)$ *is strongly real.*

(3) *If* q *is odd,* u *is a nonidentity unipotent element of* $\mathrm{PGL}_2(q)$*, and* $t \in \mathrm{PGL}_2(q)$ *is chosen so that* $u^t = u^k$ *for some* $k \in \mathbb{N}$*; then* t *lies in a Cartan subgroup (which is cyclic of order* $q-1$*) of* $\mathrm{PGL}_2(q)$ *normalizing a unique maximal unipotent subgroup of* $\mathrm{PGL}_2(q)$ *containing* u.

2. Proof of the Main Theorem

Let $G = {}^3D_4(q)$ and $g \in G$. If g is semisimple then by [9, Lemma 10] it is strongly real. If g is unipotent and q is even then [12, Theorem 1] implies that g is strongly real. Assume that g is unipotent, q is odd, and $C_G(g)$ does not contain nonidentical semisimple elements; i.e., $C_G(g)$ is a p-group. By [2, Lemma 5.9] there is $x \in G$ such that $g^x = g^{-1}$. Clearly we may assume that $|x| = 2^k$ for some $k \in \mathbb{N}$. Then $x^2 \in C_G(g)$ and $|x^2|$ is a power of 2. Therefore, x^2 is semisimple, whence $x^2 = e$. If g is unipotent, q is odd, and $C_G(g)$ contains a nonidentical semisimple element s; then we consider $g_1 = sg$. The decomposition sg is the Jordan decomposition of g_1. If we show the existence of an involution x inverting g_1 then the uniqueness of the Jordan decomposition implies $s^x = s^{-1}$ and $g^x = g^{-1}$. Thus we may assume that g has a "mixed order"; i.e., in the Jordan decomposition $g = su$ both s and u are nonidentical.

Assume that $C = C_G(s)$. Then $u \in C$. Moreover, $\overline{C} = C_{\overline{G}}(s)$ is a connected reductive subgroup of maximal rank of $\overline{G}$ and $C = \overline{C}_\sigma$. Clearly, every maximal torus T of G, which contains s, is included in C. The structure of the centralizers of semisimple elements is given in [17, Proposition 2.2]. Tables 2.2a and 2.2b from [17] are the main technical instrument in the forthcoming arguments. If q is even then up to conjugation in G there exist 8 centralizers of order divisible by p of nonidentical semisimple elements. If q is odd then there exist 9 centralizers of this sort. We consider each centralizer separately. Note that $\overline{C} = \overline{M} \circ \overline{S}$, where $\overline{M} = [\overline{C}, \overline{C}]$ is connected and semisimple, while $\overline{S} = Z(\overline{C})^0$ is a torus. Furthermore, C possesses a normal subgroup $M \circ S$, where $S = \overline{S}_\sigma \le Z(C)$ and $M = \overline{M}_\sigma = O^{p'}(C)$, and the structure of M ($= M_\sigma$ in the notation of [17]) and S ($= S_\sigma$ in the notation of [17]) is given in [17, Tables 2.2a and 2.2b], where the structure or the order of $C/(M \circ S)$ is also given. The indices of elements below are chosen as in [17, Tables 2.2a and 2.2b]. Moreover, the subgroups and factor groups of C are isomorphic to classical groups in a natural way, and we identify the subgroups and the factor groups of C with the corresponding classical groups.

Let s be such that its centralizer is conjugate to the centralizer of s_2 (hence s is an involution and this case can occur only if q is odd). Then $M \simeq \mathrm{SL}_2(q^3) \circ \mathrm{SL}_2(q)$ and $|Z(M)| = 2$ and $S = \{e\}$. Moreover, $|C : M| = 2$ and, by [18, Theorem 2], $C/\mathrm{SL}_2(q) \simeq \mathrm{PGL}_2(q^3)$ and $C/\mathrm{SL}_2(q^3) \simeq \mathrm{PGL}_2(q)$. We write u as $u_1 \cdot u_2$, where $u_1 \in \mathrm{SL}_2(q^3)$, $u_2 \in \mathrm{SL}_2(q)$, and let v_1 and v_2 be the images of u_1 and u_2 in $C/\mathrm{SL}_2(q)$ and $C/\mathrm{SL}_2(q^3)$, respectively. Assume first that $q \equiv 1 \pmod 4$. Then $\mathrm{PSL}_2(q)$ and $\mathrm{PSL}_2(q^3)$ are strongly real. Therefore, there exist involutions $t_1 \in \mathrm{PSL}_2(q^3)$ and $t_2 \in \mathrm{PSL}_2(q)$ such that $v_1^{t_1} = v_1^{-1}$ and $v_2^{t_2} = v_2^{-1}$. Let z_1 and z_2 belong to the preimages of t_1 and t_2 in $\mathrm{SL}_2(q^3)$ and $\mathrm{SL}_2(q)$, respectively. Then $|z_1| = 4 = |z_2|$ and $z_1^2 \in Z(\mathrm{SL}_2(q^3))$, $z_2^2 \in Z(\mathrm{SL}_2(q))$. It follows that $z_1^2 = z_2^2$ in M, whence $(z_1 z_2)^2 = e$. Thus, $z_1 z_2$ is an inverting involution for u. Assume now that $q \equiv 3 \pmod 4$. In this case there exist involutions $t_1 \in \mathrm{PGL}_2(q^3) \setminus \mathrm{PSL}_2(q^3)$ and $t_2 \in \mathrm{PGL}_2(q) \setminus \mathrm{PSL}_2(q)$ such that $v_1^{t_1} = v_1^{-1}$ and $v_2^{t_2} = v_2^{-1}$. Furthermore, t_1 lies in a Cartan subgroup of $\mathrm{PGL}_2(q^3)$, i.e., in a maximal torus of $\mathrm{PGL}_2(q^3)$ of order $q^3 - 1$, while t_2 lies in a Cartan subgroup of $\mathrm{PGL}_2(q)$, i.e., in a maximal torus of $\mathrm{PGL}_2(q)$ of order $q - 1$. Let T be a maximal torus of C such that its images under the natural homomorphisms $C \to C/\mathrm{SL}_2(q)$ and $C/\mathrm{SL}_2(q^3)$ contain elements t_1 and t_2, respectively. Then $|T| = (q^3 - 1)(q - 1)$ and, by [17, Table 1.1], $T \simeq \mathbb{Z}_{q^3-1} \times \mathbb{Z}_{q-1}$. In particular, T does not contain elements of order 4. Let z be a preimage of t_1 in T. We may assume that z is a 2-element; hence, $z^2 = e$. Moreover, since t_1 does not lie in $\mathrm{PSL}_2(q^3)$, we see that z does not lie in M. Consider a natural homomorphism $\widetilde{\ } : C \to C/\mathrm{SL}_2(q^3)$. Since $z \notin M$, we obtain $\tilde{z} \notin \mathrm{PSL}_2(q)$, and so $t_2 \mathrm{PSL}_2(q) = \tilde{z}\,\mathrm{PSL}_2(q)$. Moreover, $t_2, \tilde{z} \in \widetilde{T} \simeq \mathbb{Z}_{q-1}$; hence, $t_2 = \tilde{z}$. Thus, z lies in the preimage of t_2 as well. We find that z is an inverting involution for u.

Let s be such that its centralizer is conjugate either to the centralizer of s_5 or to the centralizer of s_{10}. Then $|C : (M \circ S)| = (2, q-1)$, $M \simeq \mathrm{SL}_2(q)$, and $S \simeq \mathbb{Z}_{q^3-\varepsilon}$, where $\varepsilon = 1$ if $C_G(s)$ is conjugate to $C_G(s_5)$ and $\varepsilon = -1$ if $C_G(s)$ is conjugate to $C_G(s_{10})$. Moreover, $C/S \simeq \mathrm{PGL}_2(q)$. We choose a maximal torus T of C so that $T \cap M$ is a Cartan subgroup of M. Since $M \simeq \mathrm{SL}_2(q)$, we use matrices from $\mathrm{SL}_2(q)$ to write elements of M, assuming that $T \cap M$ is the group of diagonal matrices. By Lemma 1, there exists an involution $x \in N(G,T)$ inverting each $t \in T$. In particular, x inverts s so x normalizes $C_{\overline{G}}(s)$, i.e., $x \in N(G,C)$. Therefore, x normalizes $\overline{S}$, and so it normalizes S. Put $C_0 = \langle C, x\rangle$ and let $\widetilde{\ } : C_0 \to C_0/S$ be the natural homomorphism. Since $M = O^{p'}(C)$ is characteristic in C, x induces an automorphism of M of order 2. By [19, Lemma 2.3], $N(G,C)$ does not induce field automorphisms on M. Moreover, $x \notin \widehat{M}$, where $\widehat{M}$ is a group of inner-diagonal automorphisms of M, since $C/S \simeq \mathrm{PGL}_2(q) \simeq \widehat{M}$. So $C_0/S = \widetilde{C}_0 \simeq \mathrm{PGL}_2(q) \times \mathbb{Z}_2$. The elements of $\widetilde{C}$ are written below as projective images of matrices from $\mathrm{GL}_2(q)$. Up to conjugation in $\widetilde{C}_0$, we may assume that $\tilde{u} = \begin{bmatrix} 1 & \alpha \\ 0 & 1 \end{bmatrix}$ for some $\alpha \in \mathbb{F}_q$. Let $\overline{T} \in \overline{G}$ be such that $T = \overline{T}_\sigma$. Then x normalizes $\overline{T}$. So, acting by conjugation, x leaves invariant the set of maximal unipotent subgroups of $\overline{M}$ that are normalized by $\overline{T} \cap \overline{M}$. Furthermore, since x is stable under σ; therefore, x normalizes the subgroups of σ-stable points of these unipotent subgroups. Since $\overline{M} = [\overline{C}, \overline{C}] \simeq \mathrm{SL}_2(\overline{\mathbb{F}}_q)$, there exist exactly two maximal unipotent subgroups of $\overline{M}$ that are normalized by $\overline{T}$: one of them consists of upper-triangular matrices and the other consists of lower-triangular matrices. So x either leaves these subgroups invariant or interchanges these subgroups. Thus, either $\tilde{u}^{\tilde{x}} = \begin{bmatrix} 1 & \beta \\ 0 & 1 \end{bmatrix}$ or $\tilde{u}^{\tilde{x}} = \begin{bmatrix} 1 & 0 \\ \beta & 1 \end{bmatrix}$ for some $\beta \in \mathbb{F}_q$. Going back to the elements u and x in C_0 and using the fact that p is coprime to $|S|$, we derive that $u = \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix}$ and either $u^x = \begin{pmatrix} 1 & \beta \\ 0 & 1 \end{pmatrix}$ or $u^x = \begin{pmatrix} 1 & 0 \\ \beta & 1 \end{pmatrix}$.

Let $u^x = \begin{pmatrix} 1 & \beta \\ 0 & 1 \end{pmatrix}$. Then there exists $\tilde{t} \in \mathrm{PGL}_2(q) \cap \widetilde{T}$ such that $\begin{bmatrix} 1 & \beta \\ 0 & 1 \end{bmatrix}^{\tilde{t}} = \begin{bmatrix} 1 & -\alpha \\ 0 & 1 \end{bmatrix}$. Therefore, $u^{xt} = \begin{pmatrix} 1 & -\alpha \\ 0 & 1 \end{pmatrix} = u^{-1}$ and $(xt)^2 = t^x t = t^{-1}t = e$.

Assume that $u^x = \begin{pmatrix} 1 & 0 \\ \beta & 1 \end{pmatrix}$. Then there exists $\tilde{t} \in \mathrm{PGL}_2(q) \cap \widetilde{T}$ such that $\begin{bmatrix} 1 & 0 \\ \beta & 1 \end{bmatrix}^{\tilde{t}} = \begin{bmatrix} 1 & 0 \\ \alpha & 1 \end{bmatrix}$. Therefore, $u^{xt} = \begin{pmatrix} 1 & 0 \\ \alpha & 1 \end{pmatrix} = (u)^T$, where ^{T} denotes the transposition of a matrix and $(xt)^2 = t^x t = t^{-1}t = e$. Replacing x by xt, we may assume that $u^x = \begin{pmatrix} 1 & 0 \\ \alpha & 1 \end{pmatrix} = u^T$. Since $|x| = 2$, we also derive that $(u^T)^x = u$. Set $z = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \in \mathrm{SL}_2(q) \cap N(C_0, T)$. Then $u^{xz} = u^{-1} = u^{zx}$. Since $|N(C_0,T)/T| = 4$, $N(C_0,T)/T$ is abelian. Moreover, x and z lie in $N(C_0,T)$, and their images in $N(C_0,T)/T$ are involutions; hence $N(C_0,T)/T \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$ and x normalizes $z(T \cap M)$, i.e., $z^x = zt$ for some $t \in T \cap M$. Therefore, $xzt = zx$. As we noted above, both xz and zx invert u, and so $t \in Z(M)$. If q is even then $Z(M) = \{e\}$, whence x centralizes $\langle z\rangle$. Therefore, $|xz| = 2$, and so xz is an inverting involution. Assume that q is odd. Then $|z| = 4$, $|Z(M)| = 2$, and for $t \in Z(M) \setminus \{e\}$ the identity $zt = z^{-1}$ holds. Thus either $z^x = z$ or $z^x = z^{-1}$. We show that $z^x = z^{-1}$, whence $(xz)^2 = z^x z = z^{-1}z = e$ and xz is an inverting involution. Let Q be a maximal torus of C that contains z. Note that $\tilde{x}$ and $\widetilde{Q}$ lie in $C_{\widetilde{C}_0}(\tilde{z})$ and $C_{\widetilde{C}_0}(\tilde{z}) \le N(\widetilde{C}_0, \widetilde{Q})$. Moreover, $\widetilde{C}_0 = \mathrm{PGL}_2(q) \times \langle \tilde{y}\rangle$ and $\tilde{y} \in N(\widetilde{C}_0, \widetilde{Q})$. Consider the cosets $\tilde{y}\widetilde{Q}$ and $\tilde{x}\widetilde{Q}$. Suppose that these cosets coincide. Then $\tilde{x} \in \tilde{y}\widetilde{Q}$. Since $\widetilde{Q}$ is cyclic, it contains a unique involution $\tilde{z}$. Therefore, $\tilde{y}\widetilde{Q}$ contains the two involutions $\tilde{y}$ and $\tilde{y}\tilde{z}$; hence either $\tilde{x} = \tilde{y}$ or $\tilde{x} = \tilde{y}\tilde{z}$. The first equality is impossible, since $\tilde{y}$ centralizes $\mathrm{PGL}_2(q)$; and if $\tilde{x} = \tilde{y}\tilde{z}$ then $\tilde{u}^{-1} = \tilde{u}^{\tilde{x}\tilde{z}} = \tilde{u}^{\tilde{y}\tilde{z}^2} = \tilde{u}^{\tilde{z}^2} = \tilde{u}$, which is impossible. Therefore, $\tilde{y}\widetilde{Q} \ne \tilde{x}\widetilde{Q}$. By Lemma 1, there exists an involution $x' \in N(G,Q)$ inverting each element of Q. We have

$s \in Q$, and so $x' \in C_0$ and $x, x' \in N(G,Q) \cap C_0$. Since $\tilde{y}\widetilde{Q} \neq \tilde{x}\widetilde{Q}$, $N(C_0,Q)/Q \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$, and $x, x' \notin C$, we see that $\tilde{x}'\widetilde{Q} = \tilde{x}\widetilde{Q}$ and $xQ = x'Q$. Therefore, x inverts every element of Q; in particular, $z^x = z^{-1}$.

Let s be such that its centralizer either is conjugate to the centralizer of s_3 or is conjugate to the centralizer of s_7. Then $|C : (M \circ S)| = (2, q-1)$, $M \simeq \mathrm{SL}_2(q^3)$, and $S \simeq \mathbb{Z}_{q-\varepsilon}$, where $\varepsilon = 1$ if $C_G(s)$ is conjugate to $C_G(s_3)$, and $\varepsilon = -1$ if $C_G(s)$ is conjugate to $C_G(s_7)$. Moreover, $C/S \simeq \mathrm{PGL}_2(q)$. This case can be settled by using exactly the same arguments as in the previous case.

Assume that $C_G(s)$ is conjugate to $C_G(s_4)$. Then $M \simeq \mathrm{SL}_3(q)$ and $S \simeq \mathbb{Z}_{q^2+q+1}$. Moreover, if 3 divides $q-1$ then $|C : M \circ S| = 3$ and $C/S \simeq \mathrm{PGL}_3(q)$; and if 3 does not divide $q-1$ then $C = M \times S$ and $\mathrm{SL}_3(q) \simeq \mathrm{PGL}_3(q)$. In both cases the proof is the same. Choose a maximal torus T of C so that $T \cap M$ is a Cartan subgroup of M. We identify the elements of M with matrices of $\mathrm{SL}_3(q)$ and we assume that $T \cap M$ is a subgroup of diagonal matrices under this identification. By Lemma 1, there exists $x \in N(G,T)$ such that $x^2 = e$ and $t^x = t^{-1}$ for every $t \in T$. Consider $C_0 = \langle C, x \rangle$. By [19, Lemma 2.3], $N(G,C)$ does not induce field automorphisms on M. Since x inverts each element of a Cartan subgroup $T \cap M$ of M, we see that x induces a graph automorphism on M. Let ι be the graph automorphism of $\mathrm{SL}_3(q)$ acting by $y \mapsto (y^{-1})^T$, where ^{T} denotes the transposition of a matrix. Then ι normalizes $T \cap M$ and inverts each element from $T \cap M$. Hence, multiplying x by a suitable element of $T \cap M$, we may assume that x acts on M in the same way as ι. The element u is conjugate to its Jordan form in C, and so we may assume that $u = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & \alpha \\ 0 & 0 & 1 \end{pmatrix}$, where $\alpha \in \{0, 1\}$. Let $u = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$, and set $z = \begin{pmatrix} 0 & 0 & -1 \\ 0 & -1 & 0 \\ -1 & 0 & 0 \end{pmatrix} \in \mathrm{SL}_3(q)$. We have

$$u^{xz} = ((u^{-1})^T)^z = \left(\begin{pmatrix} 1 & -1 & 1 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix}^T \right)^z = \begin{pmatrix} 1 & 0 & 0 \\ -1 & 1 & 0 \\ 1 & -1 & 1 \end{pmatrix}^z = \begin{pmatrix} 1 & -1 & 1 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix} = u^{-1}.$$

Therefore, xz is a sought involution, since $(xz)^2 = z^x z = (z^{-1})^T z = e$. Let $u = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$, and set $z = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & -1 \end{pmatrix} \in \mathrm{SL}_3(q)$. We have

$$u^{xz} = ((u^{-1})^T)^z = \left(\begin{pmatrix} 1 & -1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}^T \right)^z = \begin{pmatrix} 1 & 0 & 0 \\ -1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}^z = \begin{pmatrix} 1 & -1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = u^{-1}.$$

Therefore, xz is a sought involution, since $(xz)^2 = z^x z = (z^{-1})^T z = e$.

Assume that $C_G(s)$ is conjugate to $C_G(s_9)$. Then $M \simeq \mathrm{SU}_3(q)$, $S \simeq \mathbb{Z}_{q^2-q+1}$. Moreover, if 3 divides $(q+1)$, then $|C : M \circ S| = 3$ and $C/S \simeq \mathrm{PGU}_3(q)$; and if 3 does not divide $(q+1)$ then $C = M \times S$ and $\mathrm{SU}_3(q) \simeq \mathrm{PGU}_3(q)$. In both cases the proof is the same. Choose a maximal torus T of C so that $T \cap M$ is a Cartan subgroup of M. By Lemma 1, there exists $x \in N(G,T)$ such that $x^2 = e$ and $t^x = t^{-1}$ for every $t \in T$. Again, by [19, Lemma 2.3], $N(G,C)$ does not induce field automorphisms on M. Let $A = \begin{pmatrix} 0 & 0 & 1 \\ 0 & -1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$ and let ι be an automorphism of $\mathrm{SL}_3(q^2)$, acting by $y \mapsto A(y^{-1})^T A$, where ^{T} denotes the transposition of a matrix. Denote the automorphism of $\mathrm{SL}_3(q^2)$ that maps each element of a matrix from $\mathrm{SL}_3(q^2)$ into the power q by f. In view of [20, pp. 268–270] we may assume that $\mathrm{SU}_3(q)$ coincides with the set of $\iota \circ f$-stable points. We identify elements of M with the set of $\iota \circ f$-stable points of $\mathrm{SL}_3(q^2)$ and we assume that $T \cap M$ is a group of diagonal matrices under this identification. The restriction of ι on $\mathrm{SU}_3(q)$ we denote by the same symbol ι. Then ι normalizes $T \cap M$. So, multiplying x by a suitable element of T, we may assume that x acts on M in the same way as ι. Up to conjugation in C, each

unipotent element u of M has the form $u = \begin{pmatrix} 1 & \alpha & \beta \\ 0 & 1 & \alpha^q \\ 0 & 0 & 1 \end{pmatrix}$, where $\alpha, \beta \in F_{q^2}$ and $\beta + \beta^q = \alpha^{q+1}$. If $\alpha \neq 0$ then there exists an element $t \in T$ such that $u^t = \begin{pmatrix} 1 & 1 & \gamma \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$ for some $\gamma \in F_{q^2}$. So we may assume that $u = \begin{pmatrix} 1 & 1 & \gamma \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$ and $u^{-1} = \begin{pmatrix} 1 & -1 & \gamma' \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix}$ for some $\gamma' \in F_{q^2}$. Put $z = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix} \in \mathrm{SU}_3(q)$. Then

$$u^{xz} = (A(u^{-1})^T A)^z = \begin{pmatrix} 1 & 1 & \gamma' \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}^z = \begin{pmatrix} 1 & -1 & \gamma' \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix} = u^{-1}.$$

For $\alpha = 0$ the identity $u^{xz} = u^{-1}$ is also true. Therefore, xz is a sought involution, since $(xz)^2 = z^x z = (z^{-1})^T z = e$.

Theorem 1 and so Theorems 2 and 3 are proven.

References

1. *The Kourovka Notebook: Unsolved Problems in Group Theory*, 17th ed., Institute of Mathematics, Novosibirsk (2010).
2. *Tiep P. H. and Zalesski A. E.*, "Real conjugacy classes in algebraic groups and finite groups of Lie type," J. Group Theory, **8**, No. 3, 291–315 (2005).
3. *Bagiński C.*, "On sets of elements of the same order in the alternating group A_n," Publ. Math. Debrecen, **34**, No. 3–4, 313–315 (1987).
4. *Kolesnikov S. G. and Nuzhin Ja. N.*, "On strong reality of finite simple groups," Acta Appl. Math., **85**, No. 1–3, 195–203 (2005).
5. *Gow R.*, "Commutators in the symplectic group," Arch. Math. (Basel), **50**, No. 3, 204–209 (1988).
6. *Gow R.*, "Products of two involutions in classical groups of characteristic 2," J. Algebra, **71**, No. 2, 583–591 (1981).
7. *Ellers E. W. and Nolte W.*, "Bireflectionality of orthogonal and symplectic groups," Arch. Math., **39**, No. 1, 113–118 (1982).
8. *Rämö J.*, "Strongly real elements of orthogonal groups in even characteristic," J. Group Theory (to appear).
9. *Gal′t A. A.*, "Strongly real elements in finite simple orthogonal groups," Siberian Math. J., **51**, No. 2, 193–198 (2010).
10. *Knüppel F. and Thomsen G.*, "Involutions and commutators in orthogonal groups," J. Austral. Math. Soc., **65**, No. 1, 1–36 (1998).
11. *Tiep P. H. and Zalesski A. E.*, "Unipotent elements of finite groups of Lie type and realization fields of their complex representations," J. Algebra, **271**, No. 1, 327–390 (2004).
12. *Gazdanova M. A. and Nuzhin Ya. N.*, "On the strong reality of unipotent subgroups of Lie-type groups over a field of characteristic 2," Siberian Math. J., **47**, No. 5, 844–861 (2006).
13. *Wonenburger M. J.*, "Transformations which are products of two involutions," J. Math. Mech., **16**, 327–338 (1966).
14. *Conway J. H., Curtis R. T., Norton S. P., Parker R. A., and Wilson R. A.*, Atlas of Finite Groups, Clarendon Press, Oxford (1985).
15. *Gorenstein D., Lyons R., and Solomon R.*, The Classification of the Finite Simple Groups, Amer. Math. Soc., Providence (1998). Number 3. Part I. Chapter A. Almost Simple K-Groups (Math. Surveys Monogr.; V. 40, No. 3).
16. *Humphreys J. E.*, Conjugacy Classes in Semisimple Algebraic Groups, Amer. Math. Soc., Providence (1995) (Math. Surveys Monogr.; No. 43).
17. *Deriziotis D. I. and Michler G. O.*, "Character table and blocks of finite simple triality groups ${}^3D_4(q)$," Trans. Amer. Math. Soc., **303**, No. 1, 39–70 (1987).
18. *Vdovin E. P. and Gal′t A. A.*, "Normalizers of subsystem subgroups in finite groups of Lie type," Algebra and Logic, **47**, No. 1, 1–17 (2008).
19. *Tamburini M. C. and Vdovin E. P.*, "Carter subgroups of finite groups," J. Algebra, **255**, No. 1, 148–163 (2002).
20. *Carter R. W.*, Simple Groups of Lie Type, John Wiley and Sons, New York (1972).

E. P. Vdovin
Sobolev Institute of Mathematics, Novosibirsk, Russia
E-mail address: vdovin@math.nsc.ru

A. A. Gal′t
Novosibirsk State University, Novosibirsk, Russia
E-mail address: galt84@gmail.com