FROM THOMPSON TO BAER–SUZUKI: A SHARP CHARACTERIZATION OF THE SOLVABLE RADICAL

NIKOLAI GORDEEV, FRITZ GRUNEWALD, BORIS KUNYAVSKII, EUGENE PLOTKIN

Abstract. We prove that an element g of prime order > 3 belongs to the solvable radical $\mathfrak{R}(G)$ of a finite (or, more generally, a linear) group if and only if for every $x \in G$ the subgroup generated by g, xgx^{-1} is solvable. This theorem implies that a finite (or a linear) group G is solvable if and only if in each conjugacy class of G every two elements generate a solvable subgroup.

1. Introduction

The classical Baer–Suzuki theorem [Ba], [Su2], [AL] states that

Theorem 1.1 (Baer–Suzuki). *The nilpotent radical of a finite group G coincides with the collection of $g \in G$ satisfying the property: for every $x \in G$ the subgroup generated by g and xgx^{-1} is nilpotent.*

Within past few years a lot of efforts have been made in order to describe the solvable radical of a finite group and to establish a sharp analogue of the Baer–Suzuki theorem with respect to the solvability property (see [Fl2], [Fl3], [GGKP1], [GGKP2]). In particular, the following problem is parallel to the Baer–Suzuki result:

Problem 1.2. Let G be a finite group with the solvable radical $\mathfrak{R}(G)$. What is the minimal number k such that $g \in \mathfrak{R}(G)$ if and only if the subgroup generated by $x_1gx_1^{-1}, \dots, x_kgx_k^{-1}$ is solvable for every $x_1, \dots, x_k$ in G?

Recently (see [GGKP3]) it was proved that

Theorem 1.3. *The solvable radical of a finite group G coincides with the collection of $g \in G$ satisfying the property: for every three elements $a, b, c \in G$ the subgroup generated by the conjugates $g, aga^{-1}, bgb^{-1}, cgc^{-1}$ is solvable.*

Theorem 1.3 is sharp: in the symmetric groups S_n $(n \geq 5)$ every triple of transpositions generates a solvable subgroup.

However, as mentioned by Flavell [Fl2], one can expect a precise analogue of the Baer–Suzuki theorem to hold for the elements of prime order greater than 3 in $\mathfrak{R}(G)$. Our main result confirms this expectation:

Theorem 1.4. *Let G be a finite group. An element g of prime order $\ell > 3$ belongs to $\mathfrak{R}(G)$ if and only if for every $x \in G$ the subgroup $H = \langle g, xgx^{-1}\rangle$ is solvable.*

Theorem 1.4 together with Burnside's $p^\alpha q^\beta$-theorem implies

Corollary 1.5. *A finite group G is solvable if and only if in each conjugacy class of G every two elements generate a solvable subgroup.*

Remark 1.6. A standard argument (cf. [GKPS, Theorem 4.1], [GGKP3, Theorem 1.4]) shows that Theorem 1.4 and Corollary 1.5 remain true for the linear groups (not necessarily finite).

Remark 1.7. Corollary 1.5 can be viewed as an extension of a theorem of J. Thompson [Th], [Fl1] which states that a finite group G is solvable if and only if every two-generated subgroup of G is solvable.

Remark 1.8. The proof of Theorem 1.4 uses the classification of finite simple groups (CFSG). The proof of Corollary 1.5 can be obtained without classification using the above mentioned J. Thompson's characterization of the minimal non-solvable groups. Flavell managed to prove, without CFSG, an analogue of Theorem 1.3 for $k = 10$ [Fl2] and Theorem 1.3 under the additional assumption that $g \in G$ is of prime order $\ell > 3$.

Remark 1.9. R. Guralnick informed us that Theorems 1.4 and 1.3 were independently proved in forthcoming works by Guest, Guralnick, and Flavell [Gu], [FGG]. Flavell [FGG] reduced k in Problem 1.2 to 7 with a proof which does not rely on CFSG.

Remark 1.10. The problem of explicit description of the solvable radical of a finite group in terms of quasi-Engel sequences (see [BBGKP], [GPS]) is still open: there is no explicit analogue of Baer's theorem on characterizing the nilpotent radical as the collection of Engel elements. However, a recent result by J. S. Wilson [Wi], stating the existence of a countable set of words in two variables (in spirit of [BW]) which can be used to describe the solvable radical, gives much hope for such a characterization.

The results of the present paper were announced in [GGKP4].

Notational conventions. Whenever possible, we maintain the notation of [GGKP2] which mainly follows [St1], [Ca2]. Let $G(\Phi, K)$ be a Chevalley group where Φ is a reduced irreducible root system and K is a field. Denote by $W = W(\Phi)$ the Weyl group corresponding to Φ. Denote by $\dot{w}$ a preimage of $w \in W$ in $G(\Phi, K)$. Twisted Chevalley groups and Suzuki and Ree groups are denoted by ${}^dG(\Phi, K)$, $d = 2, 3$. We call Chevalley groups (twisted, untwisted, Suzuki and Ree groups) the groups of Lie type. Chevalley groups $G(\Phi, K)$ are denoted throughout the paper mostly as groups of type $\Phi(K)$. Correspondingly, for finite fields $K = \mathbb{F}_q$, $q = p^n$, they are denoted just by $\Phi(q)$. We adopt the notation of [Ca2] for twisted Chevalley groups which means that we use the symbols ${}^2\Phi(q^2)$ but not ${}^2\Phi(q)$. For example, simple unitary groups are denoted either as ${}^2A_n(q^2)$, or as $PSU_n(q^2)$ (and not by $PSU_n(q)$), or as $PSU_n(F)$, where F is a quadratic extension of K. We use the same notation for Suzuki and Ree groups (this means that in these cases q is not integer because q^2 is an odd power of 2 or 3).

We use the standard notation $u_\alpha(t)$, $\alpha \in \Phi$, $t \in K$, for elementary unipotent elements of G. Correspondingly, split semisimple elements will be denoted by $h_\alpha(t)$, $t \in K^*$, where K^* is the multiplicative group of K.

We say that a finite group G is almost simple if it has a unique normal simple subgroup L such that $L \leq G \leq \mathrm{Aut}\,(L)$. In the classification of automorphisms we follow [GLS, p. 60], [GL, p. 78]. This means that all automorphisms of an adjoint group of Lie type are subdivided to inner-diagonal automorphisms, field automorphisms, graph automorphisms, and graph-field ones (for non-adjoint groups see [GL, p. 79]). Recall that according to [GLS, Definition 2.5.13], any field automorphism of prime order $\ell > 3$ of L is conjugate in $\mathrm{Aut}\,(L)$ to a standard one in the sense of [St1].

We use the formula $[x, y] = xyx^{-1}y^{-1}$ to denote the commutator. If H is a subgroup of G, we denote by H^a, $a \in G$, the subgroup aHa^{-1}. For the group of fixed points of an automorphism a of a group H we use the centralizer notation $C_H(a)$ (both for inner and outer automorphisms of H). The only exception is the symbol $\mathbb{G}^F$, which is traditionally used for denoting the group of fixed points of a simple algebraic group with respect to a Frobenius endomorphism (see [Ca2]).

We use below some standard language of algebraic groups ([Sp], [Hu]). Here we consider only algebraic groups defined over a finite field $\mathbb{F}_q$ and therefore sometimes we identify such groups with the groups of points over the algebraic closure $\overline{\mathbb{F}}_q$. By a Chevalley group we mean here the group of points of a reductive algebraic group which is defined and quasisplit over K. Note that all groups are quasisplit over finite fields.

2. Strategy of proof

As in [GGKP1]–[GGKP3], we reduce Theorem 1.4 to the following statement:

Theorem 2.1. *Let G be a finite almost simple group, and let $g \in G$ be of prime order > 3. Then there is $x \in G$ such that the subgroup generated by g and xgx^{-1} is not solvable.*

Although this reduction is fairly standard, we sketch its main steps below. Let $S(G)$ be the set of all elements $g \in G$ of prime order bigger than 3 such that for every $x \in G$ the subgroup $\langle g, xgx^{-1}\rangle$ is solvable.

Obviously, any element of $\mathfrak{R}(G)$ of prime order > 3 lies in $S(G)$, and we have to prove the opposite inclusion. We may assume that G is semisimple (i.e., $\mathfrak{R}(G) = 1$), and we shall prove that G does not contain elements from $S(G)$. Assume the contrary and consider a minimal counterexample (i.e. a semisimple group G of smallest order with $S(G) \neq \emptyset$).

It is easy to see that any $g \in G$ acts as an automorphism (denoted by the same letter g) on the CR-radical V of G (see [Ro, 3.3.16]) and that $V = H_1 \times \cdots \times H_n$ where all H_i, $1 \leq i \leq n$, are isomorphic (say to H) nonabelian simple groups ([GGKP2, Section 2]). Suppose that $g \neq 1$ belongs to $S(G)$. Let us show that g cannot act on V as a non-identity element of the symmetric group S_n.

Since $g \in S(G)$, the subgroup $\Gamma = \langle g, xgx^{-1}\rangle$ is solvable for any $x \in G$. Take $x \in V$. Evidently, Γ contains the elements $[g, x] = gxg^{-1}x^{-1} = g(x)x^{-1}$ and $g^2(x)x^{-1}$. Denote by σ the element of S_n corresponding to g.

Suppose $\sigma \neq 1$. Since the order of σ is greater than 3, we may assume that there exist i and j such that $\sigma(j) = i$ and $\sigma(i) = 1$. Take $x = (x_1, \dots, x_n) \in V$ such that $x_j = b$, $x_i = a$, where a and b are generators of the simple group H and $x_k = 1$ for $k \neq i, j$, $1 \leq k \leq n$. Then the group $\langle g(x)x^{-1}, g^2(x)x^{-1} \rangle$ is not solvable since $(g(x)x^{-1})_1 = a$ and $(g^2(x)x^{-1})_1 = b$ and these elements generate a simple group H. Contradiction with the assumption that Γ is solvable.

So we may assume that an element $g \in S(G)$ acts as an automorphism $\tilde{g}$ of the simple group H. Then we consider the extension of H by $\tilde{g}$. Denote this almost simple group by G_1. By Theorem 2.1, G_1 contains no elements from $S(G)$. Contradiction with the choice of $\tilde{g}$.

So the rest of the paper is devoted to the proof of Theorem 2.1. We refer to the property stated in Theorem 2.1 as Property **(NS)** (for "non-solvable"):

(NS) For every $g \in G$ of prime order > 3 there is $x \in G$ such that the subgroup generated by g and xgx^{-1} is not solvable.

We use CFSG to prove, by case-by-case analysis, that every almost simple group satisfies **(NS)**. Section 3 deals with alternating and sporadic groups. In Section 4 we consider groups of Lie type of rank 1. In Section 5 the general case is treated. Finally, the exceptional case ${}^2F_4$ is treated separately in Section 6.

3. Alternating, symmetric, and sporadic groups

Let G be an almost simple group, $L \leq G \leq \operatorname{Aut} L$.

Lemma 3.1. *Let $L = A_n$, $n \geq 5$, be the alternating group on n letters. Then G satisfies* (**NS**).

Proof. Clearly it is enough to consider the alternating groups: as $\operatorname{Aut}(A_n) = S_n$ for $n \neq 6$ and $[\operatorname{Aut}(A_6) : A_6] = 4$, any element of odd order in $\operatorname{Aut}(A_n)$ lies in A_n. So let $G = A_n$, $n \geq 5$. For $n = 5$ the proof is straightforward, so we may proceed by induction. We may thus assume that g acts without fixed points, so $n = k\ell$, where ℓ stands for the order of g, and g is a product of k disjoint cycles of length ℓ. If $k = 1$, we can conjugate $g = (12\dots\ell)$ by a 3-cycle $z = (123)$ to see that $\langle g, zgz^{-1} \rangle = A_\ell$. For $k > 1$, we conjugate g by a product of k 3-cycles. ∎

Lemma 3.2. *Let L be a sporadic simple group. Then G satisfies* (**NS**).

Proof. As the group of outer automorphisms of any sporadic group is of order at most 2, it is enough to treat the case where G is a simple sporadic group. Here the proof goes, word for word, as in [GGKP1, Prop. 9.1]. Namely, case-by-case analysis shows that any element $g \in G$ of prime order $\ell > 3$ is either contained in a smaller simple subgroup of G, or its normalizer is a maximal subgroup of G. In the latter case it is enough to conjugate g by an element x not belonging to $N_G(\langle g\rangle)$ to ensure that $\langle g, xgx^{-1}\rangle = G$. □

4. Groups of Lie rank 1

In this case our proof combines arguments of several different types. In the cases $L = PSL_2(q)$ and $L = PSU_3(q)$ we use the analysis of [GS] with appropriate modifications whenever needed. The case of inner automorphisms of Suzuki and Ree groups is treated in the same spirit as in [GGKP1] (see Proposition 4.6). The case of field automorphisms of Ree groups can be reduced to the PSL_2-case. Finally, in the case of field automorphisms of Suzuki groups we apply a counting argument similar to [GS].

Before starting the proof, let us make some preparations. The following fact is well known.

Proposition 4.1. *Let G be a finite almost simple group of Lie type, and let $g \in G$ be an element of prime order $\ell > 3$. Then g is either an inner-diagonal or a field automorphism of L.*

Proof. See [GL, p. 82, 7-3] and [LLS, Proposition 1.1]. □

Proposition 4.2. *Let L be one of the following groups: ${}^2A_2(9)$, ${}^2G_2(3)$, $A_2(2)$, $A_2(3)$, $B_2(2)$, $B_2(3)$, $G_2(2)$, $G_2(3)$, ${}^2A_3(9)$, ${}^2A_4(9)$, ${}^3D_4(8)$, ${}^3D_4(27)$, ${}^2F_4(2)$. Then G satisfies* (**NS**).

Proof. We use [GGKP2, Table 1] and straightforward MAGMA computations with outer automorphisms of L. □

Remark 4.3. If a group L from the above list is not simple, the computations have been made for its derived subgroup L' which is simple.

So from now on we can exclude the groups listed in Proposition 4.2 from the further considerations.

Recall now, for the reader's convenience, a theorem of Gow [Gow] which is essential in our argument.

Let L be a finite simple group of Lie type, and let $z \neq 1$ be a semisimple element in L. Let C be a conjugacy class of L consisting of regular semisimple elements. Then there exist $g \in C$ and $x \in L$ such that $z = [g, x]$.

Theorem 4.4. *Suppose that the Lie rank of L is 1. Then G satisfies* (**NS**).

Proof. Let $g \in G$ be of prime order > 3. We shall check that there is $x \in L$ such that the subgroup of G generated by g and xgx^{-1} is not solvable.

Proposition 4.5. *If $L = PSL_2(q)$, $q \geq 4$, or $L = PSU_3(q^2)$, $q > 2$, then G satisfies* (**NS**).

Proof. In the case $L = PSL_2(q)$ the result follows from [GS, Lemma 3.1]. If $L = PSU_3(q^2)$, $q > 2$, the result follows from the proof of [GS, Lemma 3.3] with the single exception when g is a field automorphism. In the latter case we can take g to be standard. The order of g is a prime number bigger than 3, and we may thus assume that $q \neq 2, 3$ and that g normalizes but does not centralize a subgroup of type A_1 generated by a self-conjugate root of A_2. The result follows from [GS, Lemma 3.1]. □

Let L be a Suzuki group ${}^2B_2(q^2)$ or a Ree group ${}^2G_2(q^2)$ where q^2 is an odd power of 2, in the Suzuki case, or of 3, in the Ree case (see, e.g., [Su1], [Kl2], [LN]). Then $L = \mathbb{G}^F$ where $\mathbb{G}$ is the corresponding simple algebraic group (of type B_2 or G_2) defined over the field $\mathbb{F}_2$ or $\mathbb{F}_3$, and F is the appropriate Frobenius endomorphism of $\mathbb{G}$ ([SS], [Hu2, 1.3, 20.1]). There exists an F-stable Borel subgroup $\mathbb{B} \leq \mathbb{G}$. The group $\mathbb{B}^F$ will be called below a Borel subgroup of L. We fix one of such subgroups B. Every Borel subgroup of L is of the form B^a for some $a \in L$. We will denote by T a maximal subgroup of semisimple elements of a Borel subgroup B^a. Note that T is the subgroup of F-fixed elements of an F-stable torus of $\mathbb{G}$ contained in an F-stable Borel subgroup of $\mathbb{G}$. Hence we will call such a group T a *quasisplit torus* of L. Furthermore, we denote by $\mathfrak{T}$ any group of F-fixed elements of an F-stable torus of $\mathbb{G}$ which is not contained in any F-stable Borel subgroup of $\mathbb{G}$. We call such a group a *nonsplit torus* of L. Note that $\mathfrak{T} \cap B^a = 1$ for every $a \in L$. Recall that all maximal tori in Suzuki–Ree groups are cyclic (see [Su1], [V]).

For Suzuki and Ree groups, we consider the cases of inner and outer automorphisms separately. Since all diagonal automorphisms are inner in Suzuki–Ree groups [CCNPW], the case of inner-diagonal automorphisms is reduced to the case of inner ones. We start with the case where g is an inner automorphism.

Proposition 4.6. *If L is a Suzuki group ${}^2B_2(q^2)$, $q^2 = 2^{2m+1}$, $m \geq 1$, or a Ree group ${}^2G_2(q^2)$, $q^2 = 3^{2m+1}$, $m \geq 1$, and $g \in L$ is of prime order > 3, then there exists $x \in L$ such that the group $\langle g, xgx^{-1}\rangle$ is not solvable.*

Proof. As the order of g is greater than 3, it cannot be unipotent, so we may and shall assume that g is semisimple. We argue as in [GGKP1, Section 4]. Note that all tori in the Suzuki and Ree groups are cyclic, and all semisimple elements of order greater than 3 are regular [Su1], [Kl2], [LN]. By Gow's theorem, for every semisimple element $z' \in L$ we can find $x, y \in L$ such that $z = yz'y^{-1} = [g, x]$. Consider two cases:

- g is a generator of some maximal quasisplit torus;
- g is not a generator of any maximal quasisplit torus.

In the first case, choose x so that $z = [g, x]$ would be a generator of a nonsplit torus. In the second case, choose x so that $z = [g, x]$ would be a generator of some quasisplit torus.

Note that in both cases $g \notin \langle z\rangle$.

With such a choice of x, let $H = \langle g, xgx^{-1}\rangle$. By construction, we have $T \leq H$ for some quasisplit torus T.

First note that H is not contained in $N_L(T)$. Indeed, g and z cannot both normalize T since they are of prime order > 3 and one of them does not belong to T, whereas the order of $N_L(T)/T$ is 2.

Furthermore, H is not contained in any Borel subgroup. Indeed, if both g and xgx^{-1} belong to a Borel subgroup $B' = T'U'$ (where T' is a fixed maximal quasisplit torus and U' is the subgroup of unipotent elements), then we are in the second case. Consider the cyclic group B'/U'. Let $\bar{g}$ and $\overline{xgx^{-1}} = \bar{g}_1$ be the corresponding images. Then $\bar{g}$

and $\bar{g}_1$ are of the same order, $\langle \bar{g} \rangle \neq T'$, $\langle \bar{g}_1 \rangle \neq T'$, but $\langle \bar{g}^{-1}\bar{g}_1 \rangle \cong T'$. Contradiction.

The Suzuki groups have no maximal subgroups other than $N_L(T)$, $N_L(\mathfrak{T})$, B, and Suzuki groups over smaller fields [Su1]. The subgroup H is not contained in a subgroup of the latter type since H contains a maximal torus of L. Furthermore, H is not contained in $N_L(\mathfrak{T})$ since it contains a quasisplit torus. So we conclude that $H = L$. Using similar arguments and the list of the maximal subgroups of Ree groups [Kl2], [LN], one can show that H lies in a maximal subgroup of a Ree group only in two cases: either $q^2 = 3$ (which is excluded by Proposition 4.2), or $H < PSL_2(q^2)$. In the latter case we use Proposition 4.5 to conclude that $H = PSL_2(q^2)$. □

It remains to consider the case of outer automorphisms of prime order of Suzuki and Ree groups. Any such automorphism is a field automorphism (see Proposition 4.1) which is assumed to be standard.

We start with the simpler case of Ree groups.

Proposition 4.7. *Let L be a Ree group ${}^2G_2(q^2)$, $q^2 = 3^{2m+1}$, $m \geq 1$, and let g be a field automorphism of L of prime order $\ell > 3$. Then there exists $x \in L$ such that $\langle g, xgx^{-1} \rangle$ is not solvable.*

Proof. The group L contains a subgroup isomorphic to $PSL_2(K)$, $K = \mathbb{F}_{q^2}$. This subgroup is generated by the elementary unipotent elements of L of type $u_A(t), u_{-A}(t)$, $t \in K$, where $u_A(t) = u_{a+b}(t^{\vartheta})u_{3a+b}(t)$, $\vartheta\colon K \to K$, $3\vartheta^2 = 1$, and a, b are the short and long simple roots of G_2, respectively (see [LN]).

Hence g normalizes and does not centralize $PSL_2(K)$. Thus the assertion of the proposition follows from Proposition 4.5. □

Proposition 4.8. *Let L be a Suzuki group ${}^2B_2(q^{2\ell})$, $q^2 = 2^{2m+1}$, $m \geq 0$, and let g be a field automorphism of L of prime order ℓ greater than 3. Then there is $x \in L$ such that the subgroup $\langle g, xgx^{-1} \rangle \cap L$ is not solvable.*

Proof. Denote by Γ the set of all $y = xgx^{-1}$, $x \in L$, such that the group $\Gamma_y := \langle g, y \rangle \cap L$ is solvable. We shall prove that $|\Gamma| < |\{aga^{-1} \mid a \in L\}|$.

Note that Γ_y is invariant under the action of g because $g \in \langle g, y \rangle$, $gLg^{-1} = L$, and $\Gamma_y = \langle g, y \rangle \cap L$.

Fix a Borel subgroup $B < L$, a maximal quasisplit torus $T < B$, and maximal nonsplit tori $\mathfrak{T}$ of L which are invariant under the action of g. It is known that either $\mathfrak{T} = \mathfrak{T}_1$ or $\mathfrak{T} = \mathfrak{T}_2$, where the orders of cyclic groups $\mathfrak{T}_1$, $\mathfrak{T}_2$ are $q^{2\ell} + \sqrt{2q^{2\ell}} + 1$ and $q^{2\ell} - \sqrt{2q^{2\ell}} + 1$ respectively (see [Su1], [SS]). Recall that every maximal subgroup of L is conjugate to B, $N_L(T)$, $N_L(\mathfrak{T})$, or is isomorphic to a Suzuki group over a smaller field.

For every $y \in \Gamma$ the group Γ_y lies in some maximal subgroup of L. So $\Gamma_y < H^a$ where $a \in L$ and H is of one of the above types.

The case when H is a Suzuki group over a smaller field can be excluded because the essential case $\Gamma_y = H = Sz(q'^2)$, $q'^2|q^2$, cannot occur. Indeed, $Sz(q^2)$ is solvable if and only if $q^2 = 2$.

Lemma 4.9. *With the above notation, we have $\Gamma_y \neq Sz(2)$.*

Proof. Assume the contrary. We have $\Gamma_y = Sz(2) = \langle a\rangle \rtimes \langle b\rangle$, $a^5 = 1$, $b^4 = 1$, $bab^{-1} = a^2$. Note that Γ_y is a normal subgroup in $\langle g,\, y\rangle$, the subgroup $\langle a\rangle$ coincides with the derived subgroup of $\Gamma_y = Sz(2)$, and it is a characteristic subgroup in $\Gamma_y = Sz(2)$. Since the order ℓ of g is prime > 3, we conclude that $gag^{-1} = a$, $yay^{-1} = a$, and hence $\gamma a\gamma^{-1} = a$ for every $\gamma \in \langle g, y\rangle$. Since $bab^{-1} = a^2$, we have $b \notin \langle g, y\rangle$. Contradiction. $\square$

Lemma 4.10. *Suppose that Γ_y is contained in $N_L(T^a)$ or in $N_L(\mathfrak{T}^a)$ where $a \in L$. Then Γ_y is contained in T^a (and thus in B^a) or in $\mathfrak{T}^{\mathfrak{a}}$, respectively.*

To prove Lemma 4.10, we need two more auxiliary assertions.

Sublemma 4.11. *Suppose that $\Gamma_y \leq N_L(T^a)$ (respectively, $\Gamma_y \leq N_L(\mathfrak{T}^a)$). Then $T_y := \Gamma_y \cap T^a$ (respectively, $\mathfrak{T}_y := \Gamma_y \cap \mathfrak{T}^a$) is g-invariant.*

Proof. Let $\Gamma_y \leq N_L(T^a)$. Denote by Γ_y^2 the subgroup of Γ_y generated by the squares of the elements of Γ_y. It is clear that Γ_y^2 is invariant under g. Since $|N_L(T)/T| = 2$, all elements of Γ_y^2 belong to T, so Γ_y^2 lies in T_y. However, all elements of T are of odd order, therefore $\Gamma_y^2 = T_y$. Hence T_y is invariant under g. In order to get the statement for $\mathfrak{T}_y$, we repeat the above argument with Γ_y^2 replaced by Γ_y^4. $\square$

Sublemma 4.12. *Suppose that Γ_y is contained in $N_L(T^a)$ or in $N_L(\mathfrak{T}^a)$. Then for any integer r the element $[g^{-r}, x]$ belongs to T_y or to $\mathfrak{T}_y$, respectively.*

Proof. If $\ell | r$, the assertion is satisfied for trivial reasons, so assume that r is prime to ℓ. Let $\Gamma_y \leq N_L(T^a)$. Then $z := g^{-r}xg^rx \in N_L(T^a)$. Assume $z \in \Gamma_y \setminus T_y$. Then $g^{-r}(x) = g^{-r}xg^r = zx$. Furthermore, g^{-r} can act only trivially on Γ_y/T_y since for r prime to ℓ the order of g^{-r} is $\ell > 3$ whereas the order of Γ_y/T_y is ≤ 4. Hence $g^{-r}(z)z^{-1} \in T_y$. Thus $x = (g^{-r})^\ell(x) = z^\ell xt$ with $t \in T_y$, so $z^\ell \in T_y$. But $z \in N_L(T^a)\setminus T^a$ and $|N_L(T^a)/T^a| = 2$, therefore $z^\ell \notin T^a$. Contradiction. Hence $z \in T_y$. The same proof can be given for the case $\Gamma_y \leq N_L(\mathfrak{T}^a)$. $\square$

We are now ready to prove Lemma 4.10.

Let $a = g$, $b = xgx^{-1}$. Then any word $w = \cdots a^k b^m a^n \cdots$ can be written as $\cdots a^{k+m}(a^{-m}b^m)a^n \cdots = \cdots g^u[g^{-m}, x]g^v \cdots$, where the commutator in the middle belongs to T_y in view of Sublemma 4.12. Therefore $w = g^{u_1}z_1g^{u_2}z_2 \cdots$, where $z_1, z_2 \in T_y$. Since $w \in L$, the sum $u_1 + u_2 + \cdots$ is divisible by ℓ, so

$$w = (g^{u_1}z_1g^{-u_1})(g^{u_1+u_2}z_2g^{-u_1-u_2})(g^{u_1+u_2+u_3}\cdots) = \prod(g^{v_i}z_ig^{-v_i}).$$

By Sublemma 4.11, the latter element must belong to T_y.

The case $\Gamma_y \leq N(\mathfrak{T}^a)$ is treated in exactly the same way. $\square$

We thus may and shall assume that $\Gamma_y \leq H^a$ where $H = B$ or $H = \mathfrak{T}$.

We are now able to estimate the number of elements $y = xgx^{-1}$, $x \in L$, such that the group $\Gamma_y = \langle g, y\rangle \cap L$ is solvable.

Denote $\mathcal{A}_H := \{H^a |\ gH^ag^{-1} = H^a,\ a \in L\}$.

Denote $L_1 = \langle L, g\rangle$. Note that $\langle g, y\rangle \neq L_1$ because the group $\langle g, y\rangle$ is solvable. Hence $\langle g, y\rangle$ is contained in a proper maximal subgroup M of L_1. By [Kl1], M is conjugate to a subgroup of the form $N_{L_1}(H^a) = \langle H^a, g\rangle$ where H^a is a maximal subgroup in L invariant under g.

So we may assume that $\langle g, y\rangle$ lies in a semidirect product $H^a \rtimes \langle g\rangle$ and Γ_y lies in some H^a such that $gH^ag^{-1} = H^a$. We have $yH^ay^{-1} = H^a$ because H^a is normal in M. The equality $yH^ay^{-1} = H^a$ can be rewritten as $g(x^{-1}H^ax)g^{-1} = x^{-1}H^ax$, or, in other words, as

$x^{-1}H^a x \in \mathcal{A}_H$. Hence it is enough to estimate, for each H, the number of elements in the set

$$S_H := \{s \in L : sH^a s^{-1} = H^{a'} \text{ for some } H^a, H^{a'} \in \mathcal{A}_H\}.$$

Lemma 4.13.

$$|S_B| \leq q^{6\ell+9}.$$

Proof. First recall that we denote $L = {}^2B_2(q^{2\ell})$. We have $C_L(g) = {}^2B_2(q^2)$. The orders of the above groups are $q^{4\ell}(q^{2\ell}-1)(q^{4\ell}+1)$ and $q^4(q^2-1)(q^4+1)$, respectively.

We have $H = B = TU$ where U is the maximal unipotent subgroup of B. Denote by $C_U(g)$ the centralizer of g in U. By the definition of S_H we have $S_B \supseteq B$ (because $B \in \mathcal{A}_B$). Furthermore, let $s \notin B$ and suppose that sBs^{-1} is g-invariant. The Bruhat decomposition of L contains only two cells, hence we can represent s in the form $s = u\dot{w}b$ with $u \in U$, $b \in B$, and w the non-identity element of the Weyl group. The condition $g(sBs^{-1})g^{-1} = sBs^{-1}$ can be rewritten as $u^{-1}guB^{-}u^{-1}g^{-1}u = B^{-}$ where B^{-} stands for the Borel subgroup opposite to B. This subgroup is invariant under g, so applying g^{-1} to the last equality we conclude that $v := g^{-1}(u^{-1})u$ normalizes B^{-} and hence belongs to B^{-}. On the other hand, v is a product of two elements from U and thus belongs to U. As $B^{-} \cap U = 1$, we conclude that $v = 1$, i.e., u belongs to the centralizer $C_U(g)$. Thus the set of $s \notin B$ such that sBs^{-1} is g-invariant is in one-to-one correspondence with the set of pairs $\{(b,u)\}$ with $b \in B$ and $u \in C_U(g)$. The number of such pairs equals $|B| \cdot |C_U(g)|$. Hence the number of $s \in L$ such that sBs^{-1} is g-invariant equals $|B|(1+|C_U(g)|) = q^{4\ell}(q^{2\ell}-1)(q^4+1)$.

This calculation should be repeated for every $B^a = aBa^{-1}$ such that $g(aBa^{-1})g^{-1} = aBa^{-1}$, i.e., for each $B^a \in \mathcal{A}_B$. Let us write the last condition in the form $a^{-1}gaBa^{-1}g^{-1}a = B$ and use the Bruhat decomposition $a = uwb$ for a, as in the above paragraph. The same computation shows that the number of such groups B^a equals $|C_U(g)| = q^4$. Thus we conclude that

$$|S_B| \leq q^{4\ell}(q^{2\ell}-1)(q^4+1)q^4 \leq q^{6\ell+9}.$$

□

In order to treat the case of nonsplit tori in a similar way we need the following

Remark 4.14. If $\mathfrak{T}_1$ and $\mathfrak{T}_2$ are nonconjugate nonsplit tori in $Sz(q^{2\ell})$, then they are cyclic groups of orders $q^{2\ell}+\sqrt{2q^{2\ell}}+1$ and $q^{2\ell}-\sqrt{2q^{2\ell}}+1$, respectively. These are odd numbers whose difference is $2\sqrt{2q^{2\ell}}$ which is a power of 2, hence they are coprime.

Lemma 4.15. *Let $\mathfrak{T}$ be a nonsplit g-stable torus of $L = Sz(q^{2\ell})$. Then the first cohomology group $H^1(\langle g\rangle, \mathfrak{T})$ is trivial.*

Proof. It is enough to prove that $H^1(\langle g\rangle, \mathfrak{T}_\ell) = 1$ where $\mathfrak{T}_\ell$ is a Sylow ℓ-subgroup of $\mathfrak{T}$.

Let us first prove that if $\mathfrak{T}_\ell \neq 1$, then g does not centralize $\mathfrak{T}_\ell$. Assume the contrary. Then $\mathfrak{T}_\ell$ is contained in $Sz(q^2)$. The order of $\mathfrak{T}$ is either $N^- = q^{2\ell} - \sqrt{2q^{2\ell}} + 1$, or $N^+ = q^{2\ell} + \sqrt{2q^{2\ell}} + 1$. Note that N^+ and N^- cannot be both divisible by ℓ (see Remark 4.14). As $\mathfrak{T}_\ell < Sz(q^2)$, we have $q^4 + 1 \equiv 0 \pmod{\ell}$ (because the order of $\mathfrak{T}_\ell$ divides both $|Sz(q^2)| = q^4(q^2-1)(q^4+1)$ and $N^+N^- = q^{4\ell}+1$) and ℓ does not divide $(q^{4\ell}+1)/(q^4+1)$. On the other hand, $q^4+1 \equiv 0 \pmod{\ell}$ implies $(q^{4\ell}+1)/(q^4+1) = ((q^4)^{\ell-1} - (q^4)^{\ell-2} + \cdots + 1) \equiv 0 \pmod{\ell}$. Contradiction. Thus g acts nontrivially on $\mathfrak{T}_\ell$.

As $\mathfrak{T}$ is a cyclic group, we finish the proof by noting that if a cyclic group C of the order ℓ acts nontrivially on a cyclic ℓ-group M (ℓ odd), we have $H^i(C, M) = 1$ for all $i \geq 1$ [AM, Ch. II, Example 7.9]. □

We are now able to repeat for the tori $\mathfrak{T} = \mathfrak{T}_1$ and $\mathfrak{T}_2$ the computations already performed for the case of Borel subgroups.

Lemma 4.16.

$$|S_{\mathfrak{T}_1}| + |S_{\mathfrak{T}_2}| \leq q^{3\ell+24}.$$

Proof. Fix a maximal nonsplit torus $\mathfrak{T}$ invariant under g. For $s \in L$ such that $s\mathfrak{T}s^{-1} \in \mathcal{A}_{\mathfrak{T}}$, consider $z := g^{-1}s^{-1}gs$. Arguing as in the proof of Lemma 4.13, we arrive at the equality $z\mathfrak{T}z^{-1} = \mathfrak{T}$, i.e., $z \in N_L(\mathfrak{T})$. Since $g \in N_{L_1}(\mathfrak{T})$ (recall that $L_1 = \langle L, g\rangle$), we have $gz = s^{-1}gs \in N_{L_1}(\mathfrak{T})$, and therefore the group $\langle g, s^{-1}gs\rangle$ is contained in $N_{L_1}(\mathfrak{T})$, so $\langle g, s^{-1}gs\rangle \cap L$ is contained in $N_L(\mathfrak{T})$. By Lemma 4.10, this group is contained in $\mathfrak{T}$, so z defines a cocycle with values in $\mathfrak{T}$. By Lemma 4.15, $H^1(\langle g\rangle, \mathfrak{T}) = 1$, therefore $z = g^{-1}t^{-1}gt$ with $t \in \mathfrak{T}$. Therefore $g(ts^{-1}) = ts^{-1}$ whence $ts^{-1} = a \in C_L(g) = Sz(q^2)$. Thus $s = a^{-1}t$ with $a \in Sz(q^2)$, $t \in \mathfrak{T}$. Therefore the number of elements $s \in L$ such that $s\mathfrak{T}s^{-1} \in \mathcal{A}_{\mathfrak{T}}$ is bounded by $|\mathfrak{T}| \cdot |Sz(q^2)| = |\mathfrak{T}|q^4(q^2-1)(q^4+1)$.

This estimate should be repeated for each $\mathfrak{T}^\gamma \in \mathcal{A}_{\mathfrak{T}}$, i.e., for every $\mathfrak{T}^\gamma$ such that $g\mathfrak{T}^\gamma g^{-1} = \mathfrak{T}^\gamma$. We have seen above that $\mathfrak{T}^\gamma = \gamma\mathfrak{T}\gamma^{-1} \in \mathcal{A}_{\mathfrak{T}}$ if and only if $\gamma \in Sz(q^2)$. Hence the the number of groups $\mathfrak{T}^\gamma$ is bounded by $|Sz(q^2)|$.

Thus

$$\begin{aligned}|S_{\mathfrak{T}}| &\leq |\mathfrak{T}| \cdot q^4(q^2-1)(q^4+1) \cdot (q^4(q^2-1)(q^4+1)) \\ &= |\mathfrak{T}|q^8(q^2-1)^2(q^4+1)^2 \leq |\mathfrak{T}|q^{22}.\end{aligned}$$

Since there are two nonconjugate nonsplit tori $\mathfrak{T}_1$ and $\mathfrak{T}_2$, we get $|S_{\mathfrak{T}_1}| + |S_{\mathfrak{T}_2}| \leq q^{22}(|\mathfrak{T}_1| + |\mathfrak{T}_2|)$. Recall that the orders of the tori are $q^{2\ell} - \sqrt{2q^{2\ell}} + 1$ and $q^{2\ell} + \sqrt{2q^{2\ell}} + 1$, so each order is less than $q^{3\ell}$. Thus we get the needed estimate $|S_{\mathfrak{T}_1}| + |S_{\mathfrak{T}_2}| \leq 2q^{3\ell+22} \leq q^{3\ell+24}$. $\square$

We can now finish the proof of Proposition 4.8.

By Lemmas 4.13 and 4.16, the total number of all elements $s \in L$ such that $sH^a s^{-1} \in \mathcal{A}_H$ for some $H^a \in \mathcal{A}_H$ is bounded by $q^{3\ell+24} + q^{6\ell+9}$. If $\ell \geq 5$ then $6\ell + 9 \geq 3\ell + 24$, and we have $q^{3\ell+24} + q^{6\ell+9} \leq 2q^{6\ell+9} \leq q^{6\ell+11}$.

We have proved above that if the group $\langle g, xgx^{-1}\rangle$ is solvable then $\langle g, xgx^{-1}\rangle \leq \langle H^a, g\rangle$ for some g-stable maximal subgroup $H^a \leq L$. Moreover, in this case $xH^a x^{-1}$ is also g-stable. Hence if $\langle g, xgx^{-1}\rangle$ is solvable then there exists a g-stable maximal subgroup H^a such that $xH^a x^{-1}$ is also g-stable. We have just estimated the number of those x such that there is a g-stable maximal subgroup H^a for which the group $xH^a x^{-1}$ is also g-stable. This number is not more than $q^{6\ell+11}$. But

$$q^{6\ell+11} < q^{9\ell} <| L |= q^{4\ell}(q^{2\ell}-1)(q^{4\ell}+1).$$

Thus we can find $x \in L$ such that the group $\langle g, xgx^{-1}\rangle$ is nonsolvable.

Proposition 4.8 is proved. $\square$

Theorem 4.4 now follows from Propositions 4.5, 4.6, 4.7, and 4.8. $\square$

5. General case

In this section we prove the main part of Theorem 1.4 considering almost simple groups of Lie rank > 1 not of type ${}^2F_4$. The case ${}^2F_4$ will be treated separately in the last section.

Theorem 5.1. *Let L be a simple group of Lie type of Lie rank ≥ 2, $L \neq {}^2F_4(q^2)$, and let $L \leq G \leq Aut\, L$. Then G satisfies* (**NS**).

Suppose that the property **(NS)** does not hold for some group G. We may assume for G the following property (**MC** stands for "minimal counter-example"):

MC:

(a) G is a finite almost simple group which does not satisfy **(NS)**;

(b) $[G, G] = L$ is a simple group of Lie type different from ${}^2F_4$;

(c) if H is a group satisfying conditions (a) and (b), then the order of $[H, H]$ is greater than or equal to the order of L.

Throughout below $g \in G$ is an element of prime order $\ell > 3$ such that the group $\langle g, xgx^{-1}\rangle$ is solvable for every $x \in L$ (such an element exists according to hypothesis (a)).

Suppose that g induces a field automorphism of L. Then one can find a subgroup $L_1 = \langle U_{\pm\alpha}\rangle$ where $U_{\pm\alpha}$ are root subgroups which are g-stable but not centralized by g (this follows from the definition of field automorphism.) Since the order of g is a prime number ≥ 5, the group $L_2 = L_1/Z(L_1)$ is a simple group of rank one, and g induces on L_2 an automorphism of prime order ≥ 5. Then the almost simple group $G_1 = \langle g, L_2\rangle$ does not satisfy **(NS)**. This contradicts Theorem 4.4.

Thus, in view of classification of automorphisms of prime order (see Proposition 4.1), we may assume that g induces an inner-diagonal automorphism of L, and therefore we may also assume that

$$g \in G = \langle \sigma, L\rangle$$

where σ is a diagonal automorphism of L.

5.1. Recall that the group L can be represented in the form

$$L = [\mathbb{G}(K), \mathbb{G}(K)] = \mathbb{G}_{\rm sc}(K)/Z(\mathbb{G}_{\rm sc}(K))$$

where $\mathbb{G}_{\rm sc}$ is a simple, simply connected linear algebraic group defined over a finite field K and $\mathbb{G} = \mathbb{G}_{\rm ad}$ is the corresponding *adjoint* group.

Lemma 5.2. *There exists a reductive algebraic group $\mathfrak{G}$ defined over a finite field K satisfying the following conditions:*

(i) *the centre of* $\mathfrak{G}$ *is a torus and the derived group* $\mathfrak{G}'$ *is simply connected;*

(ii) $\mathfrak{G}'(K)/Z(\mathfrak{G}'(K)) \cong L$*;*

(iii) *there is* $\tau \in \mathfrak{G}(K)$ *such that* $\langle \tau, \mathfrak{G}'(K)\rangle / Z(\langle \tau, \mathfrak{G}'(K)\rangle \cong G$*.*

Proof. Let $\mathbb{H}$ be a maximal K-torus of $\mathbb{G}_{sc}$ which is quasisplit over K, i.e. is contained in a K-defined Borel subgroup. Further, let $\tilde{\mathbb{Z}} = Z(\mathbb{G}_{sc})$ be the centre of $\mathbb{G}_{sc}$ (here we regard $\tilde{\mathbb{Z}}$ as a finite algebraic subgroup of $\mathbb{G}_{sc}$ which is also defined over K [Sp]). We also identify $\tilde{\mathbb{Z}}$ with an algebraic subgroup of $\mathbb{H}$. Consider the embedding $\mathfrak{i}\colon \tilde{\mathbb{Z}} \hookrightarrow \mathbb{H} \times \mathbb{G}_{\mathrm{sc}}$ given by $\mathfrak{i}(z) = (z, z^{-1})$. The image $\mathfrak{i}(\tilde{\mathbb{Z}})$ will also be denoted by $\tilde{\mathbb{Z}}$.

Define the reductive group $\mathfrak{G} := (\mathbb{H} \times \mathbb{G}_{\mathrm{sc}})/\tilde{\mathbb{Z}}$. Then $Z(\mathfrak{G}) = \mathbb{H}$, $\mathfrak{G}' = \mathbb{G}_{\mathrm{sc}}$ (here we identify the groups $\mathbb{H}$ and $\mathbb{G}_{\mathrm{sc}}$ with their images in $\mathfrak{G}$). Thus we have (i), (ii).

Note that there exists an automorphism $\tilde{\sigma}$ of $\mathbb{G}_{\mathrm{sc}}$ which induces the given diagonal automorphism σ of L (because σ is defined by its action on the root subgroups). All such automorphisms are inner in $\mathbb{G}_{sc}$. Thus we may assume $\tilde{\sigma} \in \mathbb{G}_{\mathrm{sc}}$. Let F denote the Frobenius map naturally acting on $\mathfrak{G}$ such that $\mathbb{G}_{\mathrm{sc}}^F = \mathbb{G}_{\mathrm{sc}}(K)$, $\mathbb{H}^F = \mathbb{H}(K)$. Then $F(\tilde{\sigma})$ and $\tilde{\sigma}$ induce the same automorphism of $\mathfrak{G}$ (check this on root subgroups). Hence $F(\tilde{\sigma})\tilde{\sigma}^{-1} \in Z(\mathfrak{G}) = \mathbb{H}$. By Lang's theorem, $H^1(F, \mathbb{H}) = 1$, therefore we have $F(\tilde{\sigma})\tilde{\sigma}^{-1} = F(t^{-1})t$ for some $t \in \mathbb{H}$. Hence $\tau = \tilde{\sigma}t \in \mathfrak{G}(K)$. This gives (iii). □

Lemma 5.3. *We have* $G \leq \mathbb{G}(K)$*.*

Proof. The quotient $\mathfrak{G}/Z(\mathfrak{G})$ coincides with the adjoint group $\mathbb{G}$. Let $\theta\colon \mathfrak{G} \to \mathbb{G}$ be the natural homomorphism of algebraic groups. We have $\theta(\mathfrak{G}(K)) \leq \mathbb{G}(K)$. Lemma 5.2 implies $G = \langle \sigma, L\rangle \leq \theta(\mathfrak{G}(K)) \leq \mathbb{G}(K)$. □

Let $\mathbb{GL}_n$, $\mathbb{SL}_n$ be the algebraic groups such that $\mathbb{GL}_n(E) = GL_n(E)$, $\mathbb{SL}_n(E) = SL_n(E)$ for every field E. Further, let $K = \mathbb{F}_q$, let $\overline{K}$ be an algebraic closure of K, and let $\mathrm{Gal}(\overline{K}/K) = \langle \tau \rangle$ where $\tau(\alpha) = \alpha^q$ for every $\alpha \in \overline{K}$. Denote by σ the automorphism of $GL_n(\overline{K})$, $SL_n(\overline{K})$ given by the formula $\sigma(A) = (A^{-1})^t$. The automorphism τ of $\overline{K}$ also defines the automorphism of the matrix groups $GL_n(\overline{K})$, $SL_n(\overline{K})$

which will be denoted by the same symbol τ. For every natural number m we denote by F_m the Frobenius maps:

$$F_m = (\sigma\tau)^m \colon GL_n(\overline{K}) \to GL_n(\overline{K}),\ \ SL_n(\overline{K}) \to SL_n(\overline{K}).$$

Denote by $\mathbb{U}_n(q)$, $\mathbb{SU}_n(q)$ the quasisplit forms of $\mathbb{GL}_n$, $\mathbb{SL}_n$ defined over $K = \mathbb{F}_q$ such that

$$\mathbb{U}_n(q)(\mathbb{F}_{q^m}) = GL_n(\overline{K})^{F_m},\ \mathbb{SU}_n(q)(\mathbb{F}_{q^m}) = SL_n(\overline{K})^{F_m}.$$

Lemma 5.4. *Suppose that $L = A_{n-1}(q)$ or $L = {}^2A_{n-1}(q^2)$. Then in Lemma* 5.2 *one can take $\mathfrak{G} = \mathbb{GL}_n$ or $\mathfrak{G} = \mathbb{U}_n(q)$, respectively.*

Proof. For the case $L = A_{n-1}(q)$ the statement is obvious. Let $L = {}^2A_{n-1}(q^2)$. Then $\mathbb{G}_{sc} = \mathbb{SU}_n(q) = \mathbb{U}_n(q)'$ and the centre of $\mathbb{SU}_n(q)$ is a one-dimensional anisotropic torus over $K = \mathbb{F}_q$. Thus we have (i) and (ii). Note that the proof of Lemma 5.2 implies that (iii) holds for every reductive group $\mathfrak{G}$ satisfying (i) and (ii). □

5.2. The notation introduced in the next paragraph refers to the reductive group $\mathfrak{G}$ and the semisimple group $\mathbb{G}$ as in Section 5.1.

For the Chevalley groups $\mathfrak{G}(K)$ and $\mathbb{G}(K)$ denote $T_{\mathfrak{G}} = \mathbb{T}_{\mathfrak{G}}(K)$ and $T = \mathbb{T}(K)$ where $\mathbb{T}_{\mathfrak{G}}$ and $\mathbb{T}$ are maximal quasisplit tori of $\mathfrak{G}$ and $\mathbb{G}$. We will assume that $\tau \in T_{\mathfrak{G}}$ and $\sigma \in T$. Further, for the Chevalley group $\mathfrak{G}(K)$ (or $\mathbb{G}(K)$) there exists the root system Φ corresponding to $T_{\mathfrak{G}}$ (or T) which either coincides with the root system R of $\mathbb{G}$ or is obtained from R by twisting [Ca1]. We denote by $\mathfrak{U}_\alpha$ and U_α the root subgroups of $\mathfrak{G}(K)$ and $\mathbb{G}(K)$ corresponding to $\alpha \in \Phi$. We set $U_{\mathfrak{G}} = \langle \mathfrak{U}_\alpha \mid \alpha \in \Phi^+\rangle$, $U = \langle U_\alpha \mid \alpha \in \Phi^+\rangle$. The groups $B_{\mathfrak{G}} = T_{\mathfrak{G}}U_{\mathfrak{G}}$ and $B = TU$ (as well as all their conjugates) are called *Borel subgroups* of $\mathfrak{G}(K)$ and $\mathbb{G}(K)$. Any subgroup of $\mathfrak{G}(K)$ or $\mathbb{G}(K)$ which contains a Borel subgroup is called a parabolic subgroup.

Fix a simple root system Π generating Φ. For $\Pi' \subset \Pi$ denote $W_{\Pi'} = \langle w_\alpha \mid \alpha \in \Pi'\rangle$. Then $P_{\Pi'} = BW_{\Pi'}B$ is a standard parabolic subgroup of $\mathbb{G}(K)$. Note that every parabolic subgroup of $\mathbb{G}(K)$ is conjugate to a standard parabolic subgroup by an element of $[\mathbb{G}(K), \mathbb{G}(K)]$.

Lemma 5.5. *The element $g \in G = \langle \sigma, L\rangle \leq \mathbb{G}(K)$ does not belong to any proper parabolic subgroup of $\mathbb{G}(K)$.*

Proof. Assume to the contrary that $g \in P$ where $P \leq \mathbb{G}(K)$ is a proper parabolic subgroup of $\mathbb{G}(K)$. There exists $\gamma \in L = [\mathbb{G}(K), \mathbb{G}(K)]$

such that $\gamma P_{\Pi'}\gamma^{-1} = P$ for some $\Pi' \subset \Pi$. Since $\gamma \in L$ and since we may consider the element $g \in G = \langle \sigma, L\rangle$ up to conjugacy in G, we may assume that P is the standard parabolic subgroup $P_{\Pi'}$ for some $\Pi' \subset \Pi$.

Let us show that g is not a unipotent element. Indeed, if g is a unipotent element, then by conjugation with some appropriate element of L we can get an element $u \in U$ having a nontrivial factor u_α for some $\alpha \in \Pi$. Again we may assume $g = u = u_\alpha v,\ u_\alpha \neq 1, v \in U$, and $g \in P = P_{\Pi'}$ for $\Pi' = \{\alpha\}$. The image g_1 of g in the quotient $L_1 = P/Z(P)R_u(P)$ is an element of prime order $\ell > 3$. Hence L_1 is an almost simple group of Lie type of rank one which does not satisfy **(NS)**. This contradicts Theorem 4.4.

Let us show that $\delta g\delta^{-1} \notin T$ for every $\delta \in \mathbb{G}(K)$. Suppose $\delta g\delta^{-1} \in T$ for some $\delta \in \mathbb{G}(K)$. Then we may assume $g \in T$ (the same arguments as above). One can then find a group $G_\alpha = \langle U_{\pm\alpha}\rangle$, $\alpha \in \Pi$, which is normalized but not centralized by g. Then again we have a contradiction with Theorem 4.4.

Let now $g \in P = P_{\Pi'}$, $g \notin T$, $g \notin R_u(P)$. Then the image g_1 of g in $L_1 = P/Z(P)R_u(P)$ is not trivial. Further, there exists a simple component L_2 of L_1 which is an almost simple group of Lie type such that the component g_2 of g_1 in L_2 is not trivial. Obviously, $L_3 = [L_2, L_2]$ is a finite simple group of Lie type $\neq {}^2F_4(q^2)$ and $|L| > |L_3|$. Since L_2 is a simple component of $L_1 = P/Z(P)R_u(P)$, the image g_2 of g_1 can be represented in the form $g_2 = \sigma' g_3$ where $g_3 \in L_3$ and $\sigma' \in L_2$ induces a diagonal automorphism of $L_3 = [L_2, L_2]$. Then the group $G_1 = \langle \sigma', L_3\rangle$ does not satisfy **(NS)**. Hence we have a contradiction with **(MC)**. $\square$

Lemma 5.6. *The element $g \in G = \langle \sigma, L\rangle \leq \mathbb{G}(K) \leq \mathbb{G}$ is a regular semisimple element of $\mathbb{G}$.*

Proof. Since the order of g is prime and g is not unipotent, g is semisimple. Let $C_{\mathbb{G}}(g)$ be the centralizer of g in $\mathbb{G}$. This is a reductive subgroup of $\mathbb{G}$ [Ca2, Theorem 3.5.3]. Suppose that g is not regular. Then the identity component $C^0_{\mathbb{G}}(g)$ is not a torus. Since K is a finite field, there exists a K-defined Borel subgroup $\mathbb{B}_g$ of $C^0_{\mathbb{G}}(g)$. Again, the unipotent radical $R_u(\mathbb{B}_g)$ is also defined and split over K [Sp, 14.4.5]. Hence $R_u(\mathbb{B}_g)(K) \neq 1$. Since $R_u(\mathbb{B}_g)(K) \leq C_{\mathbb{G}}(g)(K) \leq \mathbb{G}(K)$, one can find a nontrivial unipotent element $u \in C_{\mathbb{G}(K)}(g)$. However, by

Lemma 5.5 the element g does not lie in any proper parabolic subgroup $P \leq \mathbb{G}(K)$, and therefore the characteristic of K does not divide the order of $C_{\mathbb{G}(K)}(g)$ [Ca2, Proposition 6.4.5]. Contradiction. □

Lemma 5.7. *The element g does not normalize any unipotent subgroup V of $\mathbb{G}(K)$.*

Proof. Assume to the contrary that $gVg^{-1} = V$ for some unipotent subgroup $V \leq \mathbb{G}$. Then V is a closed subgroup of $\mathbb{G}$ (because it is finite). The following construction is due to Borel and Tits [BT]. Consider the sequence of subgroups

$$N_1 := N_{\mathbb{G}}(V), V_1 := VR_u(N_1), \dots, N_i = N_{\mathbb{G}}(V_{i-1}), V_i := V_{i-1}R_u(N_i)$$

in $\mathbb{G}$. All groups here are defined over K. Moreover, since V is in a Borel subgroup of $\mathbb{G}$ (indeed, V belongs to a p-Sylow subgroup of G which is conjugate to $U \leq B$), the last term $N_k = P$ is a parabolic subgroup of $\mathbb{G}$ containing $N_{\mathbb{G}}(V)$, and therefore $g \in P$ (see [Hu1, 30.3]). Since $g \in \mathbb{G}(K)$ and P is a parabolic subgroup defined over K, we have $g \in P(K)$ where $P(K)$ is a parabolic subgroup of $\mathbb{G}(K)$. This is a contradiction with Lemma 5.5. □

5.3. Recall that a Coxeter element w_c of the Weyl group $W = W(\Phi)$ with respect to Π is a product (taken in any order) of the reflections w_α, $\alpha \in \Pi$, where each reflection occurs exactly once.

Let now $\mathfrak{g}$ be a preimage of g in $\mathfrak{G}(K)$, see Lemma 5.2(iii). Since g is a semisimple regular element of $\mathbb{G}$ (Lemma 5.6), the element $\mathfrak{g}$ is also semisimple and regular in $\mathfrak{G}$. By [St2, §9] (see also [GoS]), for every Coxeter element $\mathbf{w_c}$ of $\mathfrak{G}(K)$ there exists $x \in \mathfrak{G}(K)$ such that

$$x\mathfrak{g}x^{-1} = \mathbf{u}\dot{\mathbf{w}}_c$$

where $\mathbf{u} \in U_{\mathfrak{G}}$ (here $\dot{\mathbf{w}}_c$ is any preimage of $\mathbf{w}_c$). We have $x = hy$ where $h \in T_{\mathfrak{G}}$ and $y \in \mathfrak{G}'(K)$. Then

$$y\mathfrak{g}y^{-1} = \mathbf{u}'\dot{\mathbf{w}}_c$$

Thus we can put the element $\mathfrak{g}$ in the Coxeter cell $B_{\mathfrak{G}}\dot{\mathbf{w}}_c B_{\mathfrak{G}}$ by conjugation with some element from $\mathfrak{G}'(K)$. So we may assume $\mathfrak{g} \in B_{\mathfrak{G}}\dot{\mathbf{w}}_c B_{\mathfrak{G}}$. Therefore we may assume $g \in B\dot{w}_c B$ and moreover

$$g = u\dot{w}_c \tag{5.1}$$

for some $u \in U$.

In [GGKP2, Section 5], it was proved that for an element g of form (5.1) with an appropriate Coxeter element w_c, there is $x \in L$ such that $[g, x] = u \in U$. With this choice of x, put

$$H = \langle g, xgx^{-1} \rangle.$$

By our assumptions, H is a solvable group. Since $g, u \in H$, there is a Hall subgroup $H_{p\ell}$, where $p = \mathrm{char}(K)$, such that $g \in H_{p\ell}$. Let A be the maximal abelian normal subgroup of $H_{p\ell}$, and let A_p be the p-Sylow subgroup of A. Suppose that $A_p \neq 1$. Then A_p is normalized by g. This contradicts Lemma 5.7. Hence $A_p = 1$. Then $|A| = \ell^s$. Let

$$A_{[\ell]} = \{a \in A \ \mid \ a^l = 1\}, \ \ C_{A_{[\ell]}}(g) = \{a \in A_{[\ell]} \ \mid \ gag^{-1} = a\}.$$

We have $C_{A_{[\ell]}}(g) \neq 1$ since any operator of order ℓ acting on a vector space over the field $\mathbb{F}_\ell$ is unipotent and hence has a nontrivial fixed point.

We have $C_{\mathbb{G}}(g) \leq N_{\mathbb{G}}(\tilde{\mathbb{T}})$ for some maximal torus $\tilde{\mathbb{T}}$ of $\mathbb{G}$ (recall that g is a regular element of $\mathbb{G}$).

Consider the group $C_{\mathbb{G}(K)}(g)_{[\ell]}$ generated by all elements of order ℓ in $C_{\mathbb{G}(K)}(g)$. Clearly, $C_{A_{[\ell]}}(g) \leq C_{\mathbb{G}(K)}(g)_{[\ell]}$. Consider three separate cases.

Case 1. Suppose that $C_{\mathbb{G}(K)}(g)_{[\ell]} = \langle g \rangle$.

Then $C_{A_{[\ell]}}(g) = C_{\mathbb{G}(K)}(g)_{[\ell]} = \langle g \rangle$. Since $C_{A_{[\ell]}}(g) = \langle g \rangle$ and A is abelian, we have $A_{[\ell]} = C_{A_{[\ell]}}(g)$. Therefore $\langle g \rangle = A_{[\ell]}$ is an $H_{p\ell}$-invariant subgroup. Recall that $[g, x] = u \in H$ is unipotent. Hence there exists a unipotent element $v \in H_{p\ell}$. We have

$$vgv^{-1} = g^r, 1 < r < \ell$$

(indeed, g is regular and therefore $r \neq 1$, otherwise g would commute with a unipotent element). Hence $g^{r-1} = [v, g] \in [H, H]$ and therefore $g \in [H, H]$. On the other hand, the generators of the solvable group $H = \langle g, xgx^{-1} \rangle$ are not in $[H, H]$, so $g \notin [H, H]$. Contradiction.

Case 2. Suppose that $\langle g \rangle \times \langle a \rangle \leq C_{\mathbb{G}(K)}(g)_{[\ell]}$ for some $a \in \tilde{\mathbb{T}}(K)$.

Let $\mathfrak{L}(\mathbb{G})$ and $\mathfrak{L}(\tilde{\mathbb{T}})$ be the Lie algebras of $\mathbb{G}$ and $\tilde{\mathbb{T}}$, respectively. Then we have a subgroup of type $\ell \times \ell$ in $\tilde{\mathbb{T}}$ which acts by conjugation on the linear space $\overline{\mathfrak{L}} = \mathfrak{L}(\mathbb{G})/\mathfrak{L}(\tilde{\mathbb{T}})$ defined over a field of characteristic p. Since q and ℓ are coprime, by Maschke's theorem this action is diagonalizable. This implies that there exists $b \in \langle a\rangle \times \langle g\rangle$ stabilizing a nonzero vector from $\overline{\mathfrak{L}}$. Then $C_{\mathbb{G}}(b)$ is a K-defined reductive subgroup of $\mathbb{G}$ of nonzero semisimple rank because the Lie algebra of $C_{\mathbb{G}}(b)$ is not equal to the Cartan subalgebra $\mathfrak{L}(\tilde{\mathbb{T}})$ (see [Ca2, 1.14]). The identity component $C^0_{\mathbb{G}}(b)$ is also defined over K [Sp, 12.1.1]. Since K is a finite field, there exists a K-defined Borel subgroup of $C^0_{\mathbb{G}}(b)$. Hence the group $C^0_{\mathbb{G}}(b)(K)$ is not a torus (see the proof of Lemma 5.6). Further,

$$g \in \tilde{\mathbb{T}}(K) \leq C^0_{\mathbb{G}}(b)(K) \lneqq \mathbb{G}(K).$$

Note that g does not commute with unipotent elements of $C^0_{\mathbb{G}}(b)(K)$. Then there exists a subgroup $M \leq C^0_{\mathbb{G}}(b)(K)$, which is a Chevalley group over some finite extension of K, such that g normalizes M but does not centralize it and $[M,M]/Z(M)$ is a finite group of Lie type. There exists $m \in M$ such that $m \in M/Z(M)$ induces a diagonal automorphism of $[M,M]/Z(M)$ and $g \in \langle m, [M,M]/Z(M)\rangle$. The group $\langle m, [M,M]/Z(M)\rangle$ does not satisfy **(NS)** but $|[M,M]/Z(M)| < |L|$. This is a contradiction with **(MC)**.

Case 3. Suppose that $\langle g\rangle \times \langle a\rangle \leq C_{\mathbb{G}(K)}(g)_{[\ell]}$ for some $a \notin \tilde{\mathbb{T}}(K)$.

We have $aga^{-1} = g$ in $\mathbb{G}$, and thus $a \in C_{\mathbb{G}}(g) \leq N_{\mathbb{G}}(\tilde{\mathbb{T}})$. As $a \notin \tilde{\mathbb{T}}(K)$, we have $a \in N_{\mathbb{G}}(\tilde{\mathbb{T}}) \setminus \tilde{\mathbb{T}}$. Let $\mathfrak{g}, \mathfrak{a}, \mathfrak{T}$ be preimages in $\mathfrak{G}$ of $g, a, \tilde{\mathbb{T}}$, respectively. Since $\mathfrak{G}/Z(\mathfrak{G}) = \mathbb{G}$, we have

$$\mathfrak{a}\mathfrak{g}\mathfrak{a}^{-1} = \mathfrak{g}\mathfrak{c} \tag{5.2}$$

for some $\mathfrak{c} \in Z(\mathfrak{G})$. Note that $C_{\mathfrak{G}}(\mathfrak{g}) = \mathfrak{T}$ because $\mathfrak{g}$ is regular in $\mathfrak{G}$ and $\mathfrak{G}'$ is simply connected. Since $a \in N_{\mathbb{G}}(\tilde{\mathbb{T}}) \setminus \tilde{\mathbb{T}}$, we have $\mathfrak{c} \neq 1$.

Lemma 5.8. *Equality* (5.2) *cannot hold except possibly for the cases* $\mathfrak{G}' = \mathbb{SL}_\ell$ *or* $\mathfrak{G}' = \mathbb{SU}_\ell(q)$.

Proof. As $\mathfrak{a}$ is a preimage of a and $a^\ell = 1$, we have $\mathfrak{a}^\ell \in Z(\mathfrak{G})$. Hence $\mathfrak{c}^\ell = 1$. Thus ℓ is the order of $\mathfrak{c}$ (recall that $\mathfrak{c} \neq 1$). Note that ℓ divides the order of $Z(\mathfrak{G}')$ because $c = [\mathfrak{a}, \mathfrak{g}] \in Z(\mathfrak{G}')$. Since ℓ is a prime ≥ 5, we have $\mathfrak{G}' = \mathbb{SL}_n$ or $\mathbb{SU}_n(q)$ for some n.

Now we may assume $\mathfrak{G} = \mathbb{GL}_n$ or $\mathfrak{G} = \mathbb{U}_n(q)$ (Lemma 5.4).

Choose a preimage $\mathfrak{g}$ of g of ℓ-power order, say, ℓ^s. We have $\mathfrak{g}^\ell \in Z(\mathfrak{G}(K))$. We have $\mathfrak{G}(\overline{K}) = GL_n(\overline{K})$. Note that $\mathfrak{g}$ is a regular element in $GL_n(\overline{K})$. Therefore $n \leq \ell$ because all eigenvalues of $\mathfrak{g}$ are different and are of the form $\epsilon_{\ell^s}\epsilon_\ell^m$ where ϵ_{ℓ^s} and ϵ_ℓ stand for fixed roots of unity of degrees ℓ^s and ℓ, respectively. Suppose that $n < \ell$. Then the Weyl group $W(\mathbb{GL}_n)$ has no elements of order ℓ. The element a is of order ℓ and, according to the hypothesis of Case 3, belongs to $N_{\mathbb{G}}(\tilde{\mathbb{T}}) \setminus \tilde{\mathbb{T}}$. Since every element of $N_{\mathfrak{G}}(\mathfrak{T})/\mathfrak{T}$ coincides with some element of $W(GL_n)$ [Ca2, Proposition 3.3.6], we have $\mathfrak{a} \notin N_{\mathfrak{G}}(\mathfrak{T}) \setminus \mathfrak{T}$, and therefore $a \notin N_{\mathbb{G}}(\tilde{\mathbb{T}}) \setminus \tilde{\mathbb{T}}$, contradiction with the choice of a. Hence $\mathfrak{G}' = \mathbb{SL}_\ell$ or $\mathfrak{G}' = \mathbb{SU}_\ell(q)$. □

Lemma 5.9. *The case $\mathfrak{G}' = \mathbb{SL}_\ell$ cannot occur.*

Proof. We have $\mathfrak{g}^\ell \in Z(GL_\ell(K))$. As in the previous lemma, we may assume that $\mathfrak{g}^{\ell^s} = 1$ for some s. Thus $\epsilon_s = \sqrt[\ell^s]{1} \notin K$ since otherwise g would be a split semisimple element of $\mathbb{G}$ which would contradict Lemma 5.5. On the other hand, $\epsilon_{s-1} = \sqrt[\ell^{s-1}]{1} \in K$ since $\mathfrak{g}^\ell = \mathrm{diag}(\epsilon_{s-1}, \epsilon_{s-1}, \ldots, \epsilon_{s-1})$. Let ϵ be an ℓ^{th} root of unity. In $GL_\ell(\overline{K})$ one can represent $\mathfrak{g}$ by a diagonal matrix of the form $\mathrm{diag}(\epsilon_s\epsilon, \epsilon_s\epsilon^2, \ldots, \epsilon_s\epsilon^\ell)$. Clearly, $det(\mathfrak{g}) = \epsilon_{s-1}$ and the characteristic polynomial of $\mathfrak{g}$ is $x^\ell + (-1)^\ell\epsilon_{s-1}$. The matrix $\mathrm{diag}(\epsilon_s\epsilon, \epsilon_s\epsilon^2, \ldots, \epsilon_s\epsilon^\ell)$ is conjugate over $\overline{K}$ to its companion matrix

$$\mathfrak{m} = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 1 & 0 & 0 & \cdots & 0 \\ \cdots & & & & & & \\ 0 & 0 & 0 & 0 & 0 & \cdots & 1 \\ \epsilon_{s-1} & 0 & 0 & 0 & 0 & \cdots & 0 \end{pmatrix} \in GL_\ell(K).$$

Since $\mathfrak{g}$ and $\mathfrak{m}$ have the same characteristic polynomial and $\mathfrak{g}$ is a semisimple matrix, we have

$$\mathfrak{g} = y\mathfrak{m}y^{-1}$$

for some $y \in GL_\ell(K)$. Further, $y = y_1 d$ where $y_1 \in SL_\ell(K)$ and d is a diagonal matrix. Hence $\mathfrak{g}_1 = y_1^{-1}\mathfrak{g}y_1$ is a monomial matrix corresponding to an ℓ-cycle in $W(\mathbb{GL}_\ell)$. Let now g_1 be the image of $\mathfrak{g}_1$ in $PGL_n(K) = \mathbb{G}(K)$. The element g_1 is conjugate to g by an element of $PSL_n(K) = L$. Then we may assume $g_1 = g$. Let M be the image in $PGL_n(K)$ of all monomial matrices of $GL_n(K)$. Then there exists a natural epimorphism $\phi\colon M \to S_\ell$. We have $\phi(g) \in S_\ell$. Since S_ℓ satisfies condition **(NS)**, so does M. Then there exists $m \in M$ such that $\langle g, mgm^{-1}\rangle$ is not solvable which is a contradiction with the choice of g. □

Lemma 5.10. *The case $\mathfrak{G}' = \mathbb{SU}_\ell(q)$ cannot occur.*

Proof. The same arguments as in the previous lemma imply that the element $\mathfrak{g} \in \mathbb{U}_\ell(q)(K) \le GL_\ell(K)$ is conjugate in $GL_\ell(K)$ to the matrix

$$\mathfrak{m} = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 1 & 0 & 0 & \cdots & 0 \\ \cdots & & & & & & \\ 0 & 0 & 0 & 0 & 0 & \cdots & 1 \\ \epsilon_{s-1} & 0 & 0 & 0 & 0 & \cdots & 0 \end{pmatrix} \in \mathbb{U}_\ell(q)(K) = \mathfrak{G}(K)$$

for some $\epsilon_{s-1} \in \sqrt[\ell^{s-1}]{1} \in E = \mathbb{F}_{q^2}$ such that $\epsilon_{s-1}\epsilon_{s-1}^q = 1$. Then the elements $\mathfrak{g}$ and $\mathfrak{m}$ are conjugate by an element of the group $\mathbb{U}_\ell(q)(K)$ [Ca2, Proposition 3.7.3].

Note that $\mathbb{U}_\ell(q)(K) = U_\ell(E)$ is the group of unitary matrices in $GL_\ell(E)$ where $E = \mathbb{F}_{q^2}$, i.e., the matrices satisfying the condition $(\tilde{A}^{-1})^t = A$ where $\tilde{A}$ is the matrix obtained from A by replacing all the entries α_{ij} with α_{ij}^q.

Let $DU_\ell(E)$ be the set of diagonal unitary matrices over E, and let $W_\ell \le GL_n(K)$ be the group of monomial matrices with nonzero entries equal to 1. Then

$$\mathfrak{m} \in DU_\ell(E)W_\ell \le U_\ell(E).$$

Further, it is easy to see that $U_\ell(E) = DU_\ell(E)SU_\ell(E)$. Since $\mathfrak{g}$ and $\mathfrak{m}$ are conjugate by an element of $\mathbb{U}_\ell(q)(K) = U_\ell(E)$, the element $\mathfrak{g}$ is conjugate by some element of the group $SU_\ell(E)$ to some $\mathfrak{m}' \in DU_\ell(E)W_\ell$. Thus we may assume $\mathfrak{g} = \mathfrak{m}' \in DU_\ell(E)W_\ell$. Moreover, the image of $\mathfrak{g}$ in the quotient $DU_\ell(E)W_\ell/DU_\ell(E) \cong W_\ell \cong S_\ell$ is not trivial. Hence, as in the previous lemma, we have a contradiction with the choice of g. □

Theorem 5.1 is proved. □

6. Case $^2F_4$

In order to complete the proof of Theorem 2.1, it remains to consider the case of groups of type $^2F_4(q^2)$.

Theorem 6.1. *Let L be a group of type $^2F_4(q^2)$, $q^2 > 2$, and $L \le G \le Aut\, L$. Then G satisfies* **(NS)**.

Proof. Let $g \in G$. If g is a field automorphism of L, then it normalizes but does not centralize a group of rank 1, and we can use Theorem 4.4.

Thus we assume that g induces an inner-diagonal automorphism of L. Note that every inner-diagonal automorphism is an inner automorphism in the case $L = {}^2F_4(q^2)$. Hence $g \in L$. Further, one can define Borel and parabolic subgroups in ${}^2F_4(q^2)$ (see [Ca2]) because ${}^2F_4(q^2)$ has a BN-pair. One can also represent L in the form $\mathbb{G}(\overline{\mathbb{F}}_2)^F$ where $\mathbb{G}$ is the algebraic group of type F_4 defined over $\mathbb{F}_2$ and F is the Frobenius map corresponding to the group ${}^2F_4(q^2)$. We can define "tori" of L as groups of F-invariant elements of F-stable tori in $\mathbb{G}(\overline{\mathbb{F}}_2)$. Denote by T the group of F-invariant elements of an F-stable quasisplit torus. If $g \in T$, then g normalizes but does not centralize a subgroup of L which is a simple group of Lie type of rank one, and we can use Theorem 4.4. We can also use Theorem 4.4 in the case when g belongs to a parabolic subgroup of L (see the proof of Lemma 5.5). If g does not belong to any proper parabolic subgroup $P \leq G$, then the order of $C_L(g)$ is odd [Ca2, 6.4.5], and therefore (see [Gow]) we can write every semisismple element s (up to conjugacy) in the form $[g, x]$ with $x \in L$.

Among maximal tori of L one can find two tori $\mathfrak{T}_1$, $\mathfrak{T}_2$ satisfying the following conditions [Ma]:

(1) $\mathfrak{T}_1$ and $\mathfrak{T}_2$ are cyclic groups;

(2) $y\mathfrak{T}_1 y^{-1} \cap \mathfrak{T}_2 = 1$ for every $y \in L$;

(3) $N_L(\mathfrak{T}_i)$, $i = 1, 2$, is the only maximal subgroup of L containing $\mathfrak{T}_i$;

(4) the only prime divisors of $\mid N_L(\mathfrak{T}_i)/\mathfrak{T}_i \mid$ are 2 and 3.

In the notation of [Ma], one can take $\mathfrak{T}_1 = T_{10}$ and $\mathfrak{T}_2 = T_{11}$. These groups are cyclic, and their orders are $N^- = q^4 - \sqrt{2}q^3 + q^2 - \sqrt{2}q + 1$ and $N^+ = q^4 + \sqrt{2}q^3 + q^2 + \sqrt{2}q + 1$, respectively. It is easy to check condition (2) by showing that N^+ and N^- are coprime (one can see that looking at their sum and difference).

By (2), we may assume that g does not belong to a torus conjugate to one of those $\mathfrak{T}_1, \mathfrak{T}_2$, say, to $\mathfrak{T}_1$, but $[g, x]$ is a generator of $\mathfrak{T}_1$. Since $\operatorname{ord} g = \ell > 3$, condition (4) implies that $g \notin N_L(\mathfrak{T}_1)$. We have $\mathfrak{T}_1 \leq H = \langle g, xgx^{-1} \rangle \not\leq N_L(\mathfrak{T}_i)$. By [Ma], we get $H = L$, and we have property **(NS)** for the group L. $\square$

Acknowledgements. Gordeev was supported in part by RFBR grant N-08-01-00756-A. Kunyavskiĭ and Plotkin were supported in part by the Ministry of Absorption (Israel) and the Minerva Foundation through the Emmy Noether Research Institute of Mathematics. A substantial part of this work was done in MPIM (Bonn) during the visits of Kunyavskiĭ and Plotkin in 2007, the visit of Plotkin in 2008, and the visit of Gordeev in 2009. The work was discussed by all the coauthors during the international workshops hosted by the Heinrich-Heine-Universität (Düsseldorf) in 2007 and 2008. The support of these institutions is highly appreciated.

References

[AM] A. Adem, R. J. Milgram, *Cohomology of Finite Groups*, 2nd ed., Springer, Berlin et al., 2004.

[AL] J. Alperin, R. Lyons, *On conjugacy classes of p-elements*, J. Algebra **19** (1971) 536–537.

[Ba] R. Baer, *Engelsche Elemente Noetherscher Gruppen*, Math. Ann. **133** (1957) 256–270.

[BBGKP] T. Bandman, M. Borovoi, F. Grunewald, B. Kunyavskiĭ, E. Plotkin, *Engel-like characterization of radicals in finite dimensional Lie algebras and finite groups*, Manuscr. Math. **119** (2006) 365–381.

[BGGKPP] T. Bandman, G.-M. Greuel, F. Grunewald, B. Kunyavskiĭ, G. Pfister, E. Plotkin, *Identities for finite solvable groups and equations in finite simple groups*, Compositio Math. **142** (2006) 734–764.

[BT] A. Borel, J. Tits, *Éléments unipotents et sous-groupes paraboliques de groupes réductifs*, I, Invent. Math. **12** (1971) 95–104.

[BW] R. Brandl, J. S. Wilson, *Characterization of finite soluble groups by laws in a small number of variables*, J. Algebra **116** (1988) 334–341.

[BWW] J. N. Bray, J. S. Wilson, R. A. Wilson, *A characterization of finite soluble groups by laws in two variables*, Bull. London Math. Soc. **37** (2005) 179–186.

[Ca1] R. W. Carter, *Simple Groups of Lie Type*, John Wiley & Sons, London et al., 1972.

[Ca2] R. W. Carter, *Finite Groups of Lie Type. Conjugacy Classes and Complex Characters*, John Wiley & Sons, Chichester et al., 1985.

[CCNPW] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, R. A. Wilson, *Atlas of Finite Groups*, Clarendon Press, Oxford, 1985.

[Fl1] P. Flavell, *Finite groups in which every two elements generate a soluble group*, Invent. Math. **121** (1995) 279–285.

[Fl2] P. Flavell, *A weak soluble analogue of the Baer–Suzuki Theorem*, preprint, available on the homepage of the author at http://web.mat.bham.ac.uk/P.J.Flavell/research/preprints .

[Fl3] P. Flavell, *On the Fitting height of a soluble group that is generated by a conjugacy class*, J. London Math. Soc. **66** (2002) 101–113.

[FGG] P. Flavell, S. Guest, R. Guralnick, *Characterizations of the solvable radical*, submitted.

[GGKP1] N. Gordeev, F. Grunewald, B. Kunyavskiĭ, E. Plotkin, *On the number of conjugates defining the solvable radical of a finite group*, C. R. Acad. Sci. Paris, Sér. I **343** (2006) 387–392.

[GGKP2] N. Gordeev, F. Grunewald, B. Kunyavskiĭ, E. Plotkin, *A commutator description of the solvable radical of a finite group*, Groups, Geometry, and Dynamics **2** (2008) 85–120.

[GGKP3] N. Gordeev, F. Grunewald, B. Kunyavskiĭ, E. Plotkin, *A description of Baer–Suzuki type of the solvable radical of a finite group*, J. Pure Appl. Algebra **213** (2009) 250–258.

[GGKP4] N. Gordeev, F. Grunewald, B. Kunyavskiĭ, E. Plotkin, *Baer–Suzuki theorem for the solvable radical of a finite group*, C. R. Acad. Sci. Paris, Sér. I **347** (2009) 217–222.

[GoS] N. Gordeev, J. Saxl, *Products of conjugacy classes in Chevalley groups, I: Extended covering numbers*, Israel J. Math. **130** (2002) 207–248.

[GL] D. Gorenstein, R. Lyons, *The Local Structure of Finite Groups of Characteristic* 2 *Type*, Mem. Amer. Math. Soc., vol. 42, Number 276, Providence, RI, 1983.

[GLS] D. Gorenstein, R. Lyons, R. Solomon, *The Classification of the Finite Simple Groups*, Number 3, Math. Surveys and Monographs, vol. 40, no. 3, Amer. Math. Soc., Providence, RI, 1998.

[Gow] R. Gow, *Commutators in finite simple groups of Lie type*, Bull. London Math. Soc. **32** (2000) 311–315.

[Gu] S. Guest, *A solvable version of the Baer–Suzuki theorem*, Trans. Amer. Math. Soc., to appear.

[GKPS] R. Guralnick, B. Kunyavskiĭ, E. Plotkin, A. Shalev, *Thompson-like characterization of radicals in groups and Lie algebras*, J. Algebra **300** (2006) 363–375.

[GPS] R. Guralnick, E. Plotkin, A. Shalev, *Burnside-type problems reated to solvability*, Internat. J. Algebra and Computation **17** (2007) 1033–1048.

[GS] R. M. Guralnick, J. Saxl, *Generation of finite almost simple groups by conjugates*, J. Algebra **268** (2003) 519–571.

[Hu1] J. E. Humphreys, *Linear Algebraic Groups*, Springer-Verlag, Berlin–Heidelberg–New York, 1981.

[Hu2] J. E. Humphreys, *Modular Representations of Finite Groups of Lie Type*, London Math. Soc. Lecture Note Ser. **326**, Cambridge Univ. Press, 2005.

[Kl1] P. Kleidman, *The subgroup structure of some finite simple groups*, Ph.D. thesis, Univ. of Cambridge, 1987.

[Kl2] P. 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** (1988) 30–71.

[LLS] R. Lawther, M. W. Liebeck, G. Seitz, *Fixed point ratios in actions of finite exceptional groups of Lie type*, Pacific J. Math. **205** (2002) 393–464.

[LN] V. M. Levchuk, Ya. N. Nuzhin, *Structure of Ree groups*, Algebra i Logika **24** (1985), no. 1, 26–41; English transl. in Algebra and Logic **24** (1985), no. 1, 16–26.

[Ma] G. Malle, *The maximal subgroups of ${}^2F_4(q^2)$*, J. Algebra **139** (1991) 52–69.

[Ro] D. J. S. Robinson, *A Course in the Theory of Groups*, Springer-Verlag, New York, 1995.

[Sp] T. A. Springer, *Linear Algebraic Groups*, 2nd ed., Progress in Math. **9**, Birkhäuser, Boston, 1998.

[SS] T. A. Springer, R. Steinberg, *Conjugacy classes*, Seminar on Algebraic Groups and Related Finite Groups, Lecture Notes Math. **131**, Springer-Verlag, Berlin–New York, 1970, pp. 167–266.

[St1] R. Steinberg, *Lectures on Chevalley Groups*, Yale University, 1967.

[St2] R. Steinberg, *Conjugacy Classes in Algebraic Groups*, Lecture Notes Math. **366**, Springer-Verlag, Berlin–New York, 1974.

[Su1] M. Suzuki, *On a class of doubly transitive groups*, Ann. Math. **75** (1962) 105–145.

[Su2] M. Suzuki, *Finite groups in which the centralizer of any element of order 2 is 2-closed*, Ann. Math. **82** (1965) 191–212.

[Th] J. Thompson, *Non-solvable finite groups all of whose local subgroups are solvable*, Bull. Amer. Math. Soc. **74** (1968) 383–437.

[V] F. D. Veldkamp, *Roots and maximal tori in finite forms of semisimple algebraic groups*, Math. Ann. **207** (1974) 301–314.

[Wi] J. S. Wilson, *Characterization of the soluble radical by a sequence of words*, preprint, 2008.

Gordeev: Department of Mathematics, Herzen State Pedagogical University, 48 Moika Embankment, 191186, St.Petersburg, RUSSIA

E-mail address: `nickgordeev@mail.ru`

Grunewald: Mathematisches Institut der Heinrich-Heine-Universität Düsseldorf, Universitätsstr. 1, 40225 Düsseldorf, GERMANY

E-mail address: `grunewald@math.uni-duesseldorf.de`

Kunyavskii: Department of Mathematics, Bar-Ilan University, 52900 Ramat Gan, ISRAEL

E-mail address: `kunyav@macs.biu.ac.il`

Plotkin: Department of Mathematics, Bar-Ilan University, 52900 Ramat Gan, ISRAEL

E-mail address: plotkin@macs.biu.ac.il