Algebra and Logic, Vol. 39, No. 5, 2000, p. 301-312

LARGE NILPOTENT SUBGROUPS OF FINITE SIMPLE GROUPS

E. P. Vdovin* [1]

UDC 512.542.5
20D05, 20D25, 20E32

Orders and the structure of large nilpotent subgroups in all finite simple groups are determined. In particular, it is proved that if G is a finite simple non-Abelian group, and N is some of its nilpotent subgroups, then $|N|^2 < |G|$.

INTRODUCTION

In the present article, we study into the structure and orders of large nilpotent subgroups in finite simple groups and in finite groups that are close to simple, by which are meant finite groups of Lie type and symmetric groups. Values for orders of large nilpotent subgroups of finite simple and close to simple groups are given below, in Tables 1 and 3. In particular, it is proved that if G is some finite simple non-Abelian group, and N is its nilpotent subgroup, then $|N|^2 < |G|$ (Thm. 2.2).

The main tool for dealing with nilpotent subgroups in finite groups of Lie type is the structure of centralizers of semisimple elements, outlined in [1, 2]. Furthermore, in many finite simple groups, a large nilpotent subgroup coincides with a Sylow subgroup. We therefore need additional data on how Sylow subgroups of finite simple groups are structured.

The structure of Sylow subgroups in symmetric and alternating groups has been known for a rather long period of time, and for finite Chevalley groups, it has been studied by a number of authors; see, e.g., [3-5]. In [6], Kabanov and Kondratiev pointed out the structure and orders for Sylow 2-subgroups in all finite simple groups except sporadic. In [7], Zenkov and Mazurov proved that for any prime p, every finite simple non-Abelian group contains two Sylow p-subgroups having a trivial intersection.

It is worth observing that the ways in which large solvable subgroups are structured and ordered in finite simple and close to simple groups are well known. The structure and orders for large solvable subgroups in symmetric and linear groups were dealt with in [8], and in all groups of Lie type — in [9].

The notation and definitions used in the present article can be found in [10-12]. If G is a group then writing $H \leq G$ means that H is a subgroup of G and $H \trianglelefteq G$ means that H is a normal subgroup of G. By $|G : H|$ we denote the index of H in G; $N_G(H)$ is a normalizer of H in G. If the subgroup H is normal in G then G/H denotes the factor group of G w.r.t. H. If M is a subset of G, $\langle M\rangle$ stands for a subgroup generated by the set M; $|M|$ is the cardinality of M (or the order of an element, if an element is taken in place of the set). Write $C_G(M)$ to denote the centralizer of M in G; $C_G(G) = \zeta(G)$ is the center of G. By writing $x^y = y^{-1}xy$ we mean that an element x is conjugated by an element y in G. A Fitting subgroup of G is denoted by $F(G)$, and a Frattini subgroup — by $\Phi(G)$. If x and y are two elements of G then $[x, y] = x^{-1}y^{-1}xy$ is the commutator of x and y; $[G, G] = G'$ is a derived subgroup of G. The exponent of G is denoted by $\exp(G)$. Let $A \times B$ be a direct product of groups A and B and $A * B$ be their central product.

Assume that π is some subset of the set of primes. For a finite group G, $O_\pi(G)$ then denotes a largest normal subgroup of G whose order is divisible by the numbers in π only; $O^\pi(G)$ is a normal subgroup generated by elements whose order is not divisible by the primes in π. By a large nilpotent subgroup of a finite group G we always mean a nilpotent subgroup of greatest order.

If φ is an homomorphism of G, and g is an element of G, then G^φ and g^φ are the images of G and g w.r.t. φ. If φ is some automorphism of G, then G_φ denotes the set of fixed points for φ.

[1]*Supported by RFFR grant No. 99-01-00550 and by a SO RAN grant for Young Scientists, Presidium Decree No. 83 of 03/10/2000.

The notation that relates to finite Lie-type groups is borrowed from [11]. By a Chevalley group, unless specified otherwise, we mean both a universal Chevalley group and any one of its factor groups w.r.t. a subgroup in the center. In dealing with Chevalley groups, we assume that $GF(q)$ stands for a field of order q, p for its characteristic, and $GF(q)^*$ for a multiplicative group of $GF(q)$. The Chevalley group corresponding to a root system Φ over $GF(q)$ is denoted by $\Phi(q)$. A Weyl group corresponding to the root system Φ is denoted by $W(\Phi)$. For twisted groups, we write ${}^2A_n(q^2)$, ${}^2D_n(q^2)$, ${}^2E_n(q^2)$, ${}^3D_4(q^3)$, ${}^2B_2(q)$, ${}^2G_2(q)$, and ${}^2F_2(q)$. Let Φ^+ be a set of positive roots in Φ and $\Delta = \{r_1, \ldots, r_k\}$ be the set of fundamental roots, where the numbering is chosen as in [11, (3.4)]. An element x of the Chevalley group $\Phi(q)$ is said to be semisimple if its order is coprime to p. And we say that it is unipotent if its order is the power of p. Likewise, a semisimple subgroup of $\Phi(q)$ is defined as one whose order is coprime to p (a p'-subgroup). And a unipotent subgroup of $\Phi(q)$ is one whose order is the power of p. An extended Dynkin diagram of the Chevalley group G is a diagram that obtains from the initial Dynkin diagram by adding the root $-r_0$ (here, r_0 is the root of maximal weight) and then adjoining that root to other vertices in the common way.

1. AUXILIARY RESULTS FOR ALGEBRAIC GROUPS

Under this section, we give the necessary data on the structure of linear algebraic groups (for brevity, the word "linear" will be dropped), and obtain some auxiliary statements which will be made use of in evaluating orders of nilpotent subgroups. For the basic definitions and results on the structure and properties of algebraic groups, we ask the reader to consult [12]. If G is an algebraic group, then G^0 denotes a connected component in G. An algebraic group is said to be semisimple if its radical is trivial. And we say that it is reductive if its unipotent radical is trivial (in either case, the algebraic group is not assumed connected). It is well known that a connected, semisimple, algebraic group is a central product of connected, simple, algebraic groups, and that a connected, reductive, algebraic group G is the product of a torus S and a semisimple group M; moreover, $S = \zeta(G)^0$, $M = [R, R]$, and the group $S \cap M$ is finite; see, e.g., [12].

Let G be a connected, reductive, algebraic group, T be its maximal torus (by a torus we always mean a connected diagonable group), and B be a Borel subgroup containing T. There then exists a Borel subgroup B^- such that $B \cap B^- = T$. Let Φ be a root system w.r.t. T, $\varphi : N_G(T) \to N_G(T)/T = W$ be the canonical homomorphism onto the Weyl group W of G, and X_α be root subgroups w.r.t. T (one-dimensional, T-invariant, unipotent subgroups of B and B^-). The action of the Weyl group W on the root system Φ is defined as follows (see [12, 24.1]). For every element w in W, we take its certain representative n_w in G. The Weyl group acts then on the roots in Φ by the rule $\alpha^w(t) = \alpha(t^{n_w})$ for all $\alpha \in \Phi$, $t \in T$. And the Weyl group acts on the weights of the representation π for G similarly. It is well known that $B = TU$, where $U = \langle X_\alpha : \alpha \in \Phi^+\rangle$ is a maximal unipotent subgroup of G, and $B^- = TU^-$, where $U^- = \langle X_\alpha : \alpha \in \Phi^-\rangle$. If the order is induced on the positive roots of Φ, then every element of U is uniquely represented as a product of elements in the root subgroups X_α (respecting the given order).

Let G be a connected reductive group. For every element w of W, we fix its representative n_w in G. Then every element of G is uniquely representable as un_wtv, where $v \in U$, $t \in T$, and $u \in U \cap n_wU^-n_w^{-1}$; see, e.g. [12, Thm. 28.3]. Such a representation of G's elements is called the Bruhat decomposition. Furthermore, in any connected reductive group, every semisimple element is contained in some maximal torus and every unipotent element is contained in some maximal (and connected) unipotent subgroup.

Let G be a simple, connected, algebraic group, π be its rational faithful representation, and Γ_π be a lattice generated by weights of π. Denote by Γ_{ad} a lattice generated by roots of Φ, and by Γ_{sc} a lattice generated by the fundamental roots. Clearly, $\Gamma_{ad} \leq \Gamma_\pi \leq \Gamma_{sc}$.

For a root system of a given type, we know, there exist several distinct simple algebraic groups, which are called isogenies. They differ by the structure of a group Γ_π and by the order of a finite center. If it is the case that the lattice Γ_π coincides with Γ_{sc}, G is said to be one-connected and is denoted by G_{sc}. If Γ_π coincides with Γ_{ad}, G is said to be of an adjoint type and is denoted by G_{ad}. Every group with root system of a given type is obtained from G_{sc}, to appear as a factor group w.r.t. a subgroup in the center. The center of G_{ad} is trivial and G_{ad} is trivial as an abstract group.

Let c_i be a coefficient with which the fundamental root r_i enters the decomposition of the root r_0. Prime numbers that divide the coefficients c_i are called *bad* primes.

We proceed to recall a number of fundamental results concerning the structure of algebraic groups.

LEMMA 1.1 [12, Thm. 15.3]. Let G be an algebraic group. For any $x \in G$, there then exist elements $s, u \in G$ such that $x = su = us$, s is semisimple (we call s a semisimple part of x and denote it hereafter by x_s), u is unipotent (we call u a unipotent part of x and denote it hereafter by x_u), and such s and u are unique. (The representation of an element x as $x_s x_u$ is called the Jordan decomposition.)

LEMMA 1.2 [12, Thms. 21.3, 21.2]. Let G be a connected algebraic group. Then the Borel subgroups of G are all conjugate. Moreover, maximal tori and maximal connected unipotent subgroups are exactly maximal tori and maximal connected unipotent subgroups of the Borel groups. Again, all maximal tori and all maximal connected unipotent groups are conjugate, and every semisimple (unipotent) element lies in a certain maximal torus (maximal connected unipotent subgroup).

Now we recall how finite Lie-type groups are related to simple algebraic ones. Let G be a simple algebraic group defined over an algebraically closed field of characteristic $p > 0$ and σ be an endomorphism of G such that its set of fixed points, G_σ, is finite. The endomorphism σ with this property will further be called a Frobenius automorphism, though it may fail to coincide with the classical Frobenius automorphism. It is worth mentioning that σ is an automorphism if G is treated as an abstract group, and that σ is an endomorphism if G is treated as an algebraic one. Generally, σ has the form $q\sigma_0$, where $q = p^\alpha$ is raising to the qth power and σ_0 is a graph automorphism of orders 1, 2, or 3. It follows that $O^{p'}(G_\sigma)$ is a Lie-type group over a finite field of characteristic p, and, note, every (normal or twisted) Lie-type group can be obtained similarly.

Let T be a maximal σ-invariant torus of the connected, simple, algebraic group G. In what follows, by a *maximal torus* of G_σ [resp., $O^{p'}(G_\sigma)$] we mean a group T_σ [resp., $T_\sigma \cap O^{p'}(G_\sigma)$].

Below we prove an auxiliary result which will be made use of in dealing with nilpotent subgroups of finite Chevalley groups.

LEMMA 1.3. Let G be a connected, reductive, linear, algebraic group over an algebraically closed field of characteristic p and R be its reductive (not necessarily connected) subgroup of maximal rank; moreover, $(|R : R^0|, p) = 1$, $s \in R^0$ is some semisimple element, and T is an arbitrary maximal torus in R^0 containing s. Then the group $C_R(s)$ is reductive (though not necessarily connected). It is generated by the maximal torus T, together with those root subgroups U_α for which $\alpha(s) = 1$, and by those representatives of elements of the Weyl group $n_w \in N_R(T)$ that commute with s. The connected component $C_R(s)^0$ is generated by T and by those U_α for which $\alpha(s) = 1$. In particular, the group $C_R(s)/C_R(s)^0$ is isomorphic to some section of the Weyl group for G. Moreover, all unipotent elements of $C_R(s)$ lie in $C_R(s)^0$.

Proof. Fix a Borel subgroup B of the group R^0 containing T. All the generators mentioned in the lemma lie in $C_R(s)$. We prove that $C_R(x)$ is generated by the elements specified. First we claim that the group R (which is not necessarily connected) admits the Bruhat decomposition. Let x be an arbitrary element of R. Then B^x is some Borel subgroup of R^0. By virtue of Lemma 1.2, there exists an element $s \in R^0$ such that $B^x = B^s$. The element xs^{-1} normalizes B. The torus $T^{xs^{-1}}$ is maximal in B. Since all maximal tori in B are conjugate (cf. Lemma 1.2), there exists an element g of B such that $T^{xs^{-1}} = T^g$. We can therefore assume that xs^{-1} normalizes T. Then $xs^{-1} = n_w t$ for some $n_w \in N_R(T)$, $t \in T$. Since t normalizes B and xs^{-1} normalizes B, the element n_w, too, normalizes B, and hence also U, a maximal (connected) unipotent subgroup of B. For s lies in R^0, its Bruhat decomposition exists, that is, s is representable as $u_1 n_{w_1} t_1 v_1$, where $u_1 \in U \cap n_{w_1} U^- n_{w_1}^{-1}$, $n_{w_1} \in N_{R^0}(T)$, $t \in T$, and $v_1 \in U$. Note that x is representable as $x = n_w t u_1 n_{w_1} t_1 v_1$. Since the elements t and n_w normalize U, we can write x in the form $x = u_2 n_{w_2} t_2 v_2$, where $u_2 \in U \cap n_{w_2} U^- n_{w_2}^{-1}$, $n_{w_2} \in N_R(T)$, $t_2 \in T$, and $v_2 \in U$. And this decomposition is unique, for it coincides with the Bruhat decomposition of x in G.

If $x \in C_R(s)$, using the Bruhat decomposition, we can write $x = u n_w t v$, where $v \in U$, $t \in T$, and

$u \in U \cap n_w U^- n_w^{-1}$. Since s normalizes U, $N(T)$, and U^- and commutes with x, the decomposition being unique implies that each of the u, n_w, and v commutes with s. Moreover, since s normalizes every root subgroup U_α, the uniqueness of the decomposition of U into a product of root subgroups U_α $(\alpha > 0)$ implies that $\alpha(s) = 1$ whenever u or v contains a non-trivial factor of U_α. In this way x lies in the group generated by T and by those U_α and n_w that permute with s.

Because T and all U_α with $\alpha(s) = 1$ are connected, the subgroup H generated by these is closed, connected, and normal in $C_R(s)$. The fact that the Weyl group is finite implies $|C_R(s) : H| < \infty$. Thus $H = C_R(s)^0$.

Since roots of the group $C_R(s)$ w.r.t. T appear in pairs (i.e., if $\alpha(s) = 1$ then $-\alpha(s) = 1$), $C_R(s)$ is reductive. Indeed, if $C_R(s)$ has a non-trivial unipotent radical V, then that radical is normalized by T and hence contains some root subgroup U_α. V is normalized by the root group $U_{-\alpha}$, which yields a non-unipotent element in V, a contradiction.

Because $(|R : R^0|, p) = 1$, all unipotent elements of the group R lie in R^0, and so all unipotent elements of $C_R(s)$ belong to $C_{R^0}(s)$. It is well known that, for a connected reductive group R^0, every unipotent element of $C_{R^0}(s)$ lies in $C_{R^0}(s)^0$; see, e.g., [13, Thm. 2.2].

Let $x \in G$ be a semisimple element. By the previous lemma, $C_G^0(x)$ is then a connected reductive subgroup of maximal rank and $[C_G^0(x), C_G^0(x)]$ is a semisimple group whose root system is an additively closed subsystem of the root system for G. Below, such subgroups are said to be *subsystem.* In the present article we are dealing with finite groups, so of specific interest to us are elements of prime order $r\,(\neq p)$.

LEMMA 1.4 [14, 14.1]. Let G be a simple, connected, algebraic group and let $x \in G$ be of prime order $r\,(\neq p)$. Assume that $C' = [C_G^0(x), C_G^0(x)]$ is a subsystem subgroup. If Δ is Dynkin's diagram of the root system for C', then one of the following statements holds:

(1) Δ obtains by dropping vertices from Dynkin's diagram for G;

(2) Δ obtains from an extended Dynkin diagram for G by dropping one vertex r_i, where $r = c_i$ is the coefficient of a root r_i in the decomposiiton of the longest root r_0.

In particular, if r is not a bad prime for G then $\dim(\zeta^0(C_G^0(x))) \geqslant 1$.

2. LARGE NILPOTENT SUBGROUPS

Here, we study large nilpotent subgroups of finite simple groups and of close to simple groups. The section is divided into four parts. Under the first subsection, we deal with large nilpotent subgroups in symmetric and alternating groups. Under the second and third subsections, we treat finite groups of Lie type. And sporadic groups are the subject matter of the fourth. In the majority of cases, a large nilpotent group coincides with some Sylow subgroup. If G is a finite group, then $Syl_p(G)$ denotes a set of Sylow p-subgroups of G. The set of large nilpotent subgroups of a finite group G is denoted by $N(G)$, and the order of an arbitrary element of $N(G)$ — by $n(G)$.

2.1. Large Nilpotent Subgroups of Symmetric and Alternating Groups

Let G be a subgroup of S_n. Then the set $\{1, \ldots, n\}$, under the action of G, is partitioned into disjoint subsets (orbits) each of which the group G acts transitively on. First we prove the following technical lemma.

LEMMA 2.1. Let N be a nilpotent subgroup of S_n and $I_1, I_2, \ldots$ be a set of orbits of the center $\zeta(N)$ in N on a set $\{1, \ldots, n\}$. Assume that J_1 is a collection of sets I_m of order 1, J_2 is a collection of I_m of order 2, etc. Suppose that $K_1 = \bigcup\limits_{|I_m|=1} I_m$, $K_2 = \bigcup\limits_{|I_m|=2} I_m$, etc. Then the following statements hold:

(1) the group $N/\zeta(N)$ permutes sets of one order, and consequently $N \leqslant N_1 \times N_2 \times \ldots$, where $N_1 \leq S_{K_1}$, $N_2 \leq S_{K_2}$, etc.;

(2) if k_i is the number of orbits under the action of $N/\zeta(N)$ on J_i then $|\zeta(N)\cap N_i| = i^{k_i}$;

(3) if $p_1,\ldots,p_s$ are all primes by which i is divisible then the order of N_i is divisible only by $p_1,\ldots,p_s$.

Proof. Let σ be an element of the group N which translates the element i of the set I_1 into an element of some set I_k. Then $i^{\sigma\tau} = i^{\tau\sigma} \in I_k$ for any $\tau \in \zeta(N)$. Since $\zeta(N)$ acts transitively on I_1, we have $\{i^\tau : \tau \in \zeta(N)\} = I_1$; consequently, $I_1^\sigma \subseteq I_k$, that is, $|I_1| \leqslant |I_k|$. On the other hand, the element σ^{-1} translates an element of I_k into the element i of I_1; therefore, $I_k^{\sigma^{-1}} \subseteq I_1$, that is, $|I_k| \leqslant |I_1|$. Combining the inequalities obtained yields $|I_1| = |I_k|$, proving (1).

We embark on (2). We may assume that $K_i = \{1,\ldots,n\}$ and the group $N/\zeta(N)$ acts transitively on the orbits (under the action of the center $\zeta(N)$) of J_i. Let $\{I_1,\ldots,I_k\}$ be a set of all orbits of J_i under the action of $\zeta(N)$. Then the order of each such orbit equals i, and $i\cdot k = n$. Let $l \in I_1$ be some element of the orbit I_1. Consider a stabilizer $St_{\zeta(N)}(l)$ of an element l in the center $\zeta(N)$ and assume that $\tau \in St_{\zeta(N)}(l)$. Let $m \in K_i$ be an element lying in some orbit I_j. Since $N/\zeta(N)$ acts transitively on $I_1,\ldots,I_k$, there exists an element $\sigma \in N$ such that $I_j^\sigma = I_1$. Further, the group $\zeta(N)$ acts transitively on I_1, and so there exists an element $\varphi \in \zeta(N)$ such that $(m^\sigma)^\varphi = l$. It follows that $m^\tau = ((l^{\varphi^{-1}})^{\sigma^{-1}})^\tau = ((l^\tau)^{\varphi^{-1}})^{\sigma^{-1}} = m$; consequently, $\tau = \varepsilon$ and $St_{\zeta(N)}(l) = \{\varepsilon\}$. By the Lagrange theorem, $|\zeta(N)| = |\zeta(N) : St_{\zeta(N)}(l)|\cdot|St_{\zeta(N)}(l)| = i$.

Further, $J_i = \{I_k : |I_k| = i\}$ by definition. Assume that there exists a prime $q \notin \{p_1,\ldots,p_s\}$ which divides the order of N_i. Since N_i is a nilpotent group, there exists a central element τ of order q. Because N is a direct product of groups $N_1, N_2, \ldots$, the element τ lies in $\zeta(N)$. Clause (2) implies that $|\zeta(N)\cap N_i| = i^k$, where $k \geqslant 1$. Hence τ lies in $\zeta(N)\cap N_i$, but $|\tau|$ does not divide $|\zeta(N)\cap N_i|$, a contradiction.

Note that the group N_1 specified in the lemma is trivial. Now we are in a position to explicate the structure of symmetric and alternating groups.

THEOREM 2.1. A large nilpotent subgroup in an alternating group is conjugate to one of the following groups:

(1) $\langle(1,2,3)\rangle$ if $n = 3$;

(2) $\langle(1,2,3,4,5)\rangle$ if $n = 5$;

(3) $\langle(1,2,3)\rangle \times \langle(4,5,6)\rangle$ if $n = 6$;

(4) $Syl_2(A_n)$ if $n \neq 2(2k+1)+1$ for some natural k;

(5) $Syl_2(A_{n-3}) \times \langle(n-2,n-1,n)\rangle$ if $n = 2(2k+1)+1$, $k \geqslant 1$.

A large nilpotent subgroup in a symmetric group is conjugate to one of the following:

(1) $Syl_2(S_n)$ if $n \neq 2(2k+1)+1$ for some natural k;

(2) $Syl_2(S_{n-3}) \times \langle(n-2,n-1,n)\rangle$ if $n = 2(2k+1)+1$ for some natural k.

In all groups, a large nilpotent subgroup is unique up to conjugation.

Proof. Assume that the statement of the theorem fails and that n is the minimal natural number yielding a counterexample to the hypothesis. Let P be a subgroup of S_n which is structured the same way as is the nilpotent subgroup specified in Lemma 2.1. Suppose that $N \in N(S_n)$ is a large nilpotent subgroup which is not conjugate to p.

Under the action of $\zeta(N)$, the set $\{1,\ldots,n\}$ gets partitioned into orbits. There are two cases to consider:

1. Among the orbits of the center $\zeta(N)$, there are subsets of different orders. By Lemma 2.1, therefore, $N(S_n)$ is a subgroup in the direct product of the groups $N_1 \leq S_{n_1}$ and $N_2 \leq S_{n_2}$, in which case $n_1 + n_2 = n$. Since n is the minimal natural number for which the statement of the theorem fails, the groups of $N(S_{n_1})$ and $N(S_{n_2})$ are structured in the way specified by the lemma.

Let $n_1 \neq 2(2k+1)+1$; then $|N_1| \leqslant |S|$, where $S \in Syl_2(S_{n_1})$. Depending on whether or not the number n_2 is representable as $2(2k+1)+1$, we obtain the following values: $|N_2| \leqslant 3|S_1|$ or $|N_2| \leqslant |S_2|$, where $S_1 \in Syl_2(S_{n_2-3})$ and $S_2 \in Syl_2(S_{n_2})$. For the first option, we have $|N| \leqslant |N_1|\cdot|N_2| \leqslant |Syl_2(S_{n_1})|\cdot 3|Syl_2(S_{n_2-3})| \leqslant 3|Syl_2(S_{n-3})| \leqslant |P|$, in which case the equality attains only if $N_1 \in Syl_2(S_{n_1})$ and $N_2 = S_1 \times \langle(k_1,k_2,k_3)\rangle$, that is, if $N = P$ up to conjugation. Which is impossible, for n is the minimal number delivering a counterexample. Similarly we can treat the situation where $N_2 \in Syl_2(S_{n_2})$.

TABLE 1

Group G	$n(G)$	Structure
A_3	3	$\langle(1,2,3)\rangle$
A_5	5	$\langle(1,2,3,4,5)\rangle$
A_6	9	$\langle(1,2,3)\rangle \times \langle(4,5,6)\rangle$
A_n, $n \neq 2(2k+1)+1$	$\frac{1}{2}2^{[n/2]+[n/2^2]+\dots}$	S, where $S \in Syl_2(A_n)$
A_n, $n = 2(2k+1)+1$	$\frac{3}{2}2^{[(n-3)/2]+[(n-3)/2^2]+\dots}$	$S \times \langle(n-2,n-1,n)\rangle$, $S \in Syl_2(A_{n-3})$
S_n, $n \neq 2(k+1)+1$	$2^{[n/2]+[n/2^2]+\dots}$	S, $S \in Syl_2(S_n)$
S_n, $n = 2(2k+1)+1$	$3 \cdot 2^{[(n-3)/2]+[(n-3)/2^2]+\dots}$	$S \times \langle(n-2,n-1,n)\rangle$, $S \in Syl_2(S_{n-3})$

Let $n_1 = 2(2k_1+1)+1$ and $n_2 = 2(2k_2+1)+1$. Then $|N(G)| \leqslant 3|S_3| \cdot 3|S_1| < |Syl_2(S_n)| = |P|$, where $S_3 \in Syl_2(S_{n_1-3})$, and we arrive at a contradiction. Thus the first case which holds that orbits may contain subset of different orders is impossible.

2. Suppose that all orbits under the action of $\zeta(N)$ are of the same order k. Let $I_1, \dots, I_{n/k}$ all be orbits of the set $\{1, \dots, n\}$ under the action of $\zeta(N)$. If the action of the group $N/\zeta(N)$ on a set of orbits $I_1, \dots, I_{n/k}$ is not transitive, N is a subgroup in the direct product of N_1 and N_2, each of which is a nilpotent subgroup of a symmetric group of lesser degree. Similarly to the first case, we can show that N is not a counterexample.

Now we let N act transitively on the orbits $I_1, \dots, I_{n/k}$. In virtue of Lemma 2.1(2), the order of $\zeta(N)$ equals k, the group $N/\zeta(N)$ can be treated as a nilpotent subgroup of $S_{n/k}$, and so $|N| \leqslant k \cdot |N_3|$, where $N_3 \in N(S_{n/k})$. It is not hard to verify that $|N| \leqslant |Syl_2(S_n)|$ except $n = k = 3$. We have thus proved the theorem for symmetric groups.

We turn to alternating groups. Let n be the minimal number for which a counterexample to the statement of the theorem exists. Let that counterexample be furnished by $N \in N(A_n)$. Write R

to denote a nilpotent subgroup of A_n which coincides with the large nilpotent group specified by the theorem. Again we have two cases to consider:

1. The action of $N/\zeta(N)$ on a set of orbits of the center $\zeta(N)$ is not transitive. Hence, either N is contained in a direct product of nilpotent groups N_1 and N_2 each of which is a nilpotent subgroup of an alternating group in a lesser dimension, or it belongs to a direct product of two nilpotent groups N_1 and N_2, of which each is a nilpotent subgroup of a symmetric group in a lesser dimension, but does not coincide with that product. Using the orders of large nilpotent subgroups in symmetric groups at hand, it is not hard to verify that N fails as a counterexample in this case, too.

2. The group $N/\zeta(N)$ acts transitively on a set of orbits. Suppose that each orbit is of order k. By Lemma 2.1, then, $|\zeta(N)| = k$ and $N/\zeta(N)$ can be treated as a nilpotent subgroup of $S_{n/k}$. It is not hard to verify that $k|N_4| \leqslant (1/2)|S| \leqslant |R|$, where $N_4 \in N(A_{n/k})$ and $S \in Syl_2(S_n)$, holds for $n \geqslant 7$.

2.2. General Structure of Nilpotent Subgroups in Simple Algebraic Groups

We claim the validity of the following:

LEMMA 2.2. Let N be a closed nilpotent subgroup of a connected, simple, algebraic group G. Then there exists a reductive subgroup R of maximal rank in G, containing a group N. Let W_1 be a Weyl group of R^0. Then the following statements hold:

(1) $N = N_s \times N_u$, that is, N is representable as a direct product of its subgroups consisting of semisimple and unipotent elements;

(2) $N_u \leq R^0$ and $\zeta(N_s) \cap R^0 \leq \zeta(R^0)$;

(3) if $N_0 = N \cap R^0$ then N/N_0 is isomorphically embeddable in the group $N_W(W_1)/W_1$.

If N consists of σ-invariant elements under some Frobenius automorphism σ, then the group R is σ-invariant.

Proof. Let N be a closed nilpotent subgroup of a connected, simple, algebraic group defined over an algebraic closure of a field $GF(q)$. Then N consists of elements of finite orders and is representable as a direct product of its p-subgroups (cf. [10, Thm. 12.1.1]). In particular, N can be represented as $N_s \times N_u$, which is a direct product of its semisimple and unipotent parts, respectively.

If the group N_s is non-trivial then its center is also. Clearly, $\zeta(N_s) = (\zeta(N))_s$. Let x be some element of $\zeta(N_s)$. Then $N \subseteq C_G(x)$, with $N_u \subseteq R^0$. Denote by R the group $C_G(x)$. By Lemma 1.3, R is a reductive subgroup of maximal rank in G. Suppose that there exists an element s of $\zeta(N_s) \cap R^0$ which does not lie in $\zeta(R^0)$. Consider a group $C_R(s)$. Clearly, $N \leq C_R(s)$ and $N_u \leq R^0$. Again, $C_R(s)$ is a reductive subgroup of maximal rank in G. Since R decreases in dimension at each step, the process is finite (the dimension of G is finite). Allowing a repetition of the above process yields a reductive subgroup R of maximal rank in G containing N. If N consists of fixed points w.r.t. some Frobenius automorphism σ, R will be σ-invariant. We have thus proved clauses (1) and (2) of the lemma.

We turn to (3). We have $N/N_0 = NR^0/N_0R^0 \leq R/R^0$. The proof of Lemma 1.3 implies that every element of R is representable as nx, where $n \in N_R(T)$ for some maximal torus T of R^0, and $x \in R^0$. Since R^0 is normal in R, the group $N_R(T)/T$ is contained in the group $N_W(W_1)$. This gives us $R/R^0 \cong N_R(T)/N_{R^0}(T) \leq N_W(W_1)/W_1$.

Remark. Lemma 2.2 implies that $N_0/\zeta(N_0)$ is a nilpotent subgroup in a direct product of simple algebraic groups of lesser dimension — the group $R^0/\zeta(R^0)$. The lemma thus generalizes a result of [15] concerning the structure of semisimple nilpotent subgroups in generalized linear groups over finite fields.

We know how reductive subgroups R of maximal rank in G, and also subgroups R_σ, are structured; see [1, 2, 16]. To treat nilpotent subgroups of finite groups of Lie type, therefore, we are left to find orders of large nilpotent subgroups in Weyl groups. The Weyl groups for types B_n, C_n, and D_n are a wreath product of a 2-group and a symmetric group S_n. The data obtained on the structure of nilpotent subgroups in symmetric groups can now be used to conclude that a large nilpotent subgroup in a Weyl group for all the types mentioned is exactly a Sylow 2-group. Table 2 shows values for orders of large nilpotent subgroups in Weyl groups for all classical groups, and their structure.

TABLE 2

Type of system Φ	Structure of groups $N(W(\Phi))$	Value for $n(W(\Phi))$
A_n	cf. Table 1	2^{n+1}
B_n and C_n	lie in $Syl_2(W)$	2^{2n}
D_n	lie in $Syl_2(W)$	2^{2n-1}

2.3. Large Nilpotent Subgroups of Finite Groups of Lie Type

Here, we work to apply the above-specified general properties of nilpotent subgroups to finite Lie-type groups. In particular, we prove that a large nilpotent subgroup coincides, in most of the cases, with a maximal unipotent subgroup. Finding large nilpotent subgroups in finite Chevalley groups proceeds uniformly, so we treat $A_n(q)$ to exemplify this process.

Let N be some nilpotent subgroup of $A_n(q)$. We claim that its order does not exceed the order of the greatest nilpotent group indicated in Table 3. We may assume that the center of $A_n(q)$ is trivial. By Lemma 2.2, then, the group N is contained in some proper reductive subgroup of maximal rank in a connected, simple, algebraic group of type A_n.

First we recall the structure of reductive subgroups of maximal rank in a simple, connected, algebraic group of type A_n, and also how are structured their fixed points under the Frobenius automorphism σ; see [2]. Assume that G is of type A_n. The endomorphism σ of G induces an endomorphism of the character group X of a torus T, which is also denoted by σ and has the form $\sigma = q\sigma_0$, where q is the power of p and σ_0 is an isometry of X. The isometry σ_0 has order 1 or 2, depending on whether G_σ is normal or twisted. The group X contains the set Φ of roots, and Φ is conveniently represented as $\Phi = \{e_i - e_j : i \neq j, i, j \in \{0, 1 \ldots, n\}\}$, where $e_0, e_1, \ldots, e_n$ form an orthonormal basis for an $(n+1)$-dimensional Euclidean space. The Weyl group W acts on that space by permuting the basis elements in a way that fits the symmetric group S_{n+1}. The isometry σ_0 acts on the roots either identically or as an element of order 2.

The root system of any σ-invariant reductive subgroup of G is equivalent w.r.t. W to a system Φ_1 of the following type. Let $\lambda = (\lambda_1, \lambda_2, \ldots)$ be the partition of $n+1$ and $I_1, I_2, \ldots$ be disjoint subsets of $\{0, 1, \ldots, n\}$ satisfying the condition that $|I_1| = \lambda_1$, $|I_2| = \lambda_2$, …. Assume $\Phi_1 = \{e_i - e_j \in \Phi : i, j \in I_\alpha$ for some $\alpha\}$. Then Φ_1 is a subsystem of Φ of type $A_{\lambda_1 - 1} \times A_{\lambda_2 - 1} \times \ldots$. And it is σ-invariant on the condition that if σ_0 has order 2 then Φ_1 is invariant under a linear transformation given by the rule $e_i \to -e_{n-i}$.

LEMMA 2.3 [2, Prop. 7]. Let G be a group of type A_l and let σ be an endomorphism such that G_σ is of a normal type. Assume that G_1 is a reductive subgroup of maximal rank in G complying with the partition λ of $l+1$. Suppose that G_1^g is a σ-invariant subgroup of G obtained by twisting G_1 by an element $w \in W$ given by the rule $\pi(g^\sigma g^{-1}) = w$. Assume also that w is mapped into τ under the homomorphism $N_W(W_1) \to \mathrm{Aut}_W(\Delta_1)$. Let n_i be the number of parts in λ equal to i; then $\mathrm{Aut}_W(\Delta_1) \cong S_{n_2} \times S_{n_3} \times \ldots$. Suppose that τ delivers partitions $\mu^{(2)}, \mu^{(3)}, \ldots$ of the respective numbers $n_2, n_3, \ldots$. Then simple components of a semisimple group $(M^g)_\sigma$ are of type $A_{i-1}(q^{\mu_j^{(i)}})$, with exactly one component for each $i = 2, 3, \ldots$ and for every part $\mu_j^{(i)}$ of the partition $\mu^{(i)}$.

The order of a semisimple part $(S^g)_\sigma$ for the group $(G_1^g)_\sigma$ is defined by setting

$$(q-1)|(S^g)_\sigma| = \prod_{i,j} (q^{\mu_j^{(i)}} - 1).$$

Since the center of $A_n(q)$ is assumed trivial, the order of the centralizer specified in Lemma 2.3 should be multiplied by $1/(n+1, q-1)$. Indeed, if G is not one-connected, the finite group $O^{p'}(G_\sigma)$ does not coincide with G_σ, and so the order of the centralizer is less than the one specified in the lemma. In this case $G_\sigma = \hat{H} O^{p'}(G_\sigma)$, and also $|\hat{H} : H| = d_1/d$. Here, $\hat{H}$ is a maximal torus of the group G_σ, H is one in $O^{p'}(G_\sigma)$, d_1 is the order of the center of $O^{p'}(G_\sigma)$, and d is the one in $(G_{sc})_\sigma$. To find the order of a centralizer in $O^{p'}(G_\sigma)$, therefore, the order of the centralizer given in the lemma ought to be multiplied by d_1/d. In fact, the centralizer of any semisimple element contains a maximal torus of the Chevalley group, and so $(C_G(s)^0)_\sigma = \hat{H} C_{O^{p'}(G_\sigma)}(s)$. Hence $|(C_G(s)^0)_\sigma : C_{O^{p'}(G_\sigma)}(s)| = d_1/d$; consequently, $|C_{O^{p'}(G_\sigma)}(s)| = (d_1/d)|(C_G(s)^0)_\sigma|$. Thus the order of the centralizer should be multiplied by (d_1/d), but in our case $d_1 = 1$ and $d = (n+1, q-1)$.

By Lemma 2.3, there exists a subgroup N_0 of N lying in some σ-invariant, connected, reductive subgroup R of maximal rank in G. Furthermore, $|N : N_0| \leqslant 2^{n+1}$; see Table 2. Since the center of $A_n(q)$ is assumed trivial, the group R is a proper subgroup of G. In this way N_0 is representable as a central product of nilpotent subgroups of groups in a lesser dimension and the group that is a fixed-point subgroup of some torus. Therefore, the order of N is estimated thus:

$$(q-1)|N| \leqslant n(S_{n+1}) \frac{1}{(n+1, q-1)} \prod_{i,j} (q^{\mu_j^{(i)}} - 1) \prod_{i,j} (i, q^{\mu_j^{(i)}} - 1) n(A_{i-1}(q^{\mu_j^{(i)}})). \tag{1}$$

Here, as $A_{i-1}(q^{\mu_j^{(i)}})$ we consider a group with trivial center. Using induction on the Lie rank of a group, we can prove that the following hold:

$$(q^k - 1)(i, q^k - 1) n(A_{i-1}(q^k)) \leqslant (q-1)(ik, q-1) n(A_{ik-1}(q)), \tag{2}$$

$$(q-1)(i, q-1) n(A_{i-1}(q))(q-1)(k, q-1) n(A_{k-1}(q)) \leqslant (q-1)(ik, q-1) n(A_{ik-1}(q). \tag{3}$$

Using (2) and (3), the right part of (1) can be written either in the form

$$(q-1)^2 n(S_{n+1})(n_1, q-1) n(A_{n_1-1}(q))(n_2, q-1) n(A_{n_2-1}(q)), \tag{4}$$

where $n_1 + n_2 = n+1$, or in the form

$$(q^2-1) n(S_{n+1})((n+1)/2, q^2-1) n(A_{(n+1)/2-1}(q^2)). \tag{5}$$

It is not hard to verify that (4) and (5) do not exceed the values indicated in Table 3. Other finite groups of Lie type can be treated in a similar way.

Table 3 exhibits the structure of large unipotent subgroups for the case where a finite group G of a given type has trivial center. For groups with an arbitrary center, a large nilpotent subgroup is the preimage of a large nilpotent subgroup in the group with trivial center under the natural homomorphism.

2.4. Large Nilpotent Subgroups of Sporadic Groups

In dealing with large nilpotent subgroups, we make use of the information in [17]. For all sporadic groups, a large nilpotent subgroup is a Sylow subgroup, and so finding large nilpotent groups calls for a uniform argument. We just outline the idea.

If N is a nilpotent subgroup of G, and $p_1, \ldots, p_k$ are all primes dividing the order of N, then N contains a central element of order $p_1 \cdot \ldots \cdot p_k$. The study of orders of centralizers of such elements using [17] shows that the order of N, in this case, is less than the order of a Sylow subgroup. An easy consequence of this is the following:

THEOREM 2.2. Let G be a finite simple non-Abelian group and N be its nilpotent subgroup. Then $|N|^2 < |G|$.

TABLE 3

Group G	Structure of groups in $N(G)$	$n(G)$
$A_1(2^n)$	cyclic group	2^n+1
$A_1(q)$, $q-1=2^n$	lies in $Syl_2(A_1(q))$	2^n
${}^2A_2(2^2)$	lies in $Syl_3({}^2A_2(2^2))$	27
${}^2A_2(3^2)$	lies in $Syl_2({}^2A_2(3^2))$	32
for all other G	a large unipotent group	

Proof. If $N(G)$ coincides with $Syl_p(G)$ for some prime p, the statement of the theorem follows from [7, Thm. 2]. If $G=A_n$, $n=2(2k+1)+1$ for some natural k, it is easy to see that $N(G)^2 < 2^{2(n-1)} < |G|$. Finally, if G coincides with $A_1(2^n)$, then the group $N(G)$ is Abelian, and by [18], $N(G)^2 < |G|$.

Acknowledgement. I express my sincere gratitude to V. D. Mazurov for useful consultations and valuable comments. I am also indebted to A. V. Vasiliev who read and with whom we discussed the manuscript, which helped me correct a handful of mistakes and inaccuracies in the initial version of the article.

REFERENCES

1. R. W. Carter, “Centralizers of semisimple elements in finite groups of Lie type,” *Proc. London Math. Soc., III. Ser.*, **37**, No. 3, 491-507 (1978).

2. R. W. Carter, “Centralizers of semisimple elements in the finite classical groups,” *Proc. London Math. Soc., III. Ser.*, **42**, No. 1, 1-41 (1981).

3. R. W. Carter and P. Fong, “The Sylow 2-subgroups of the finite classical groups,” *J. Alg.*, **1**, No. 2, 139-151 (1964).

4. A. J. Weir, “Sylow p-subgroups of the classical groups over finite fields with characteristic prime to p,” *Proc. Am. Math. Soc.*, **6**, No. 4, 529-533 (1955).

5. W. J. Wong, “Twisted wreath product and Sylow 2-subgroups of classical simple groups,” *Math. Z.*, **97**, No. 5, 406-424 (1967).

6. V. V. Kabanov and A. S. Kondratyev, *Sylow 2-Subgroups of Finite Groups* [in Russian], UrO AN SSSR, Sverdlovsk (1979).

7. V. I. Zenkov and V. D. Mazurov, “The intersection of Sylow subgroups in finite groups,” *Algebra Logika*, **35**, No. 4, 424-432 (1996).

8. A. Mann, “Soluble subgroups of symmetric and linear groups,” *Israel J. Math.*, **55**, No. 2, 162-172 (1986).

9. Y. Segev, Ph. D. Thesis, The Hebrew Univ., Jerusalem (1985).

10. D. J. S. Robinson, *A Course in the Theory of Groups*, Springer, New York (1996).

11. R. W. Carter, *Simple Groups of Lie Type*, Wiley, London (1972).

12. J. E. Humphreys, *Linear Algebraic Groups*, Springer, New York (1975).

13. J. E. Humphreys, *Conjugacy Classes in Semisimple Algebraic Groups, Math. Surv. Mon.*, Vol. 43, Am. Math. Soc., Providence, R.I. (1995).

14. D. Gorenstein and R. Lyons, *The Local Structure of Finite Groups of Characteristic 2 Type, Mem. Am. Math. Soc.*, Vol. 276, Providence, R.I. (1983).

15. R. F. Apamenok and D. A. Suprunenko, "Nilpotent irreducible linear groups over a finite field," *Dokl. Akad. Nauk BSSR*, **3**, No. 12, 475-478 (1959).

16. D. Deriziotis, "The Brauer complex and its application to the Chevalley groups," Ph. D. Thesis, University of Warwick (1977).

17. J. Conway, R. Curtis, S. Norton, et al., *Atlas of Finite Groups*, Clarendon, Oxford (1985).

18. A. Chermak and A. Delgado, "A measuring argument for finite groups," *Proc. Am. Math. Soc.*, **107**, No. 4, 907-914 (1989).