ISSN 0081-5438, Proceedings of the Steklov Institute of Mathematics, 2009, Suppl. 3, pp. S218–S233.

published in Trudy Instituta Matematiki i Mekhaniki UrO RAN, 2009, Vol. 15, No. 2.

On Recognizability by Spectrum of Finite Simple Groups of Types B_n, C_n, and ${}^2D_n$ for $n = 2^k$

A. V. Vasil'ev[1], I. B. Gorshkov[2], M. A. Grechkoseeva[1], A. S. Kondrat'ev[3], and A. M. Staroletov[2]

Received December 29, 2008

Abstract—The spectrum of a finite group is the set of its element orders. A group is said to be recognizable (by spectrum) if it is isomorphic to any finite group that has the same spectrum. A nonabelian simple group is called quasi-recognizable if every finite group with the same spectrum possesses a unique nonabelian composition factor and this factor is isomorphic to the simple group in question. We consider the problem of recognizability and quasi-recognizability for finite simple groups of types B_n, C_n, and ${}^2D_n$ with $n = 2^k$.
Keywords: finite simple group, spectrum of a group, prime graph, recognition by spectrum, orthogonal group, symplectic group.

DOI: 10.1134/S0081543809070207

INTRODUCTION

Let G be a finite group, let $\pi(G)$ be the set of prime divisors of the order of G, and let $\omega(G)$ be the *spectrum* of G, i.e., the set of orders of its elements. The *prime graph* (the *Gruenberg–Kegel graph*) $GK(G)$ of the group G is defined as follows: its vertices are the elements of the set $\pi(G)$, and any two distinct vertices r and s are connected by an edge if and only if the number rs is in $\omega(G)$. Evidently, the graph $GK(G)$ is uniquely determined by the spectrum $\omega(G)$, and this spectrum can be reconstructed by the set $\mu(G)$ of the elements from $\omega(G)$ that are maximal with respect to divisibility.

For a finite group G, we denote by $h(G)$ the number of finite groups H that are pairwise nonisomorphic and satisfy the condition $\omega(H) = \omega(G)$. The group G is called *recognizable* (by spectrum) if $h(G) = 1$, *almost recognizable* if $h(G) < \infty$, and *unrecognizable* if $h(G) = \infty$. Since every finite group containing a nontrivial normal solvable subgroup is unrecognizable, the question of the recognizability of nonabelian simple groups is of the greatest interest here. It turns out that many of such groups are recognizable or almost recognizable by spectrum. A survey of the latest results in this research area can be found in [1, 2]. The study of the question of the so-called quasi-recognizability of finite simple groups has become an independent research area. A nonabelian

[1]Sobolev Institute of Mathematics, Siberian Branch of the Russian Academy of Sciences, pr. Akad. Koptyuga 4, Novosibirsk, 630090 Russia
emails: vasand@math.nsc.ru, grechkoseeva@gmail.ru
[2]Novosibirsk State University, ul. Pirogova 2, Novosibirsk, 630090 Russia
e-mails: ily@gorodok.net, astaroletov@gmail.com
[3]Institute of Mathematics and Mechanics, Ural Division of the Russian Academy of Sciences, ul. S. Kovalevskoi 16, Yekaterinburg, 620219 Russia
email: A.S.Kondratiev@imm.uran.ru

finite simple group L is called *quasi-recognizable* (by spectrum) if any finite group G with the same spectrum contains only one nonabelian composition factor and this factor is isomorphic to L (see the survey of results on the quasi-recognizability of finite simple groups in [3]). Note that the greatest progress here was made in the case when the prime graph of the group L is disconnected. In particular, it was proved [4] that all nonabelian simple groups for which the number of connected components of the prime graph is greater than 2 are quasi-recognizable except for the alternating group Alt_6. In the present paper, we consider the question of the quasi-recognizability of three classes of finite simple groups such that their prime graphs have exactly two connected components. Note that, in some special cases, we are able to prove the stronger property of recognizability.

Theorem 1. *Let $L = {}^2D_n(q)$, where $n = 2^k \geqslant 4$ and q is odd. Then, the group L is quasi-recognizable.*

Theorem 2. *Let $L \in \{B_n(q), C_n(q)\}$, where $n = 2^k \geqslant 8$, $q = p^\alpha$, p is an odd prime, and $\alpha \in \mathbb{N}$. Then, the group L is quasi-recognizable. Moreover, if α is odd, then the group L is recognizable.*

Theorem 3. *Let $L \in \{B_4(q), C_4(q)\}$, where q is odd and G is a finite group satisfying the condition $\omega(G) = \omega(L)$. Then, the group G contains only one nonabelian composition factor, and this factor is isomorphic to either L or ${}^2D_4(q)$.*

Note that the question of the recognizability of the groups $B_2(q)$ ($\simeq C_2(q)$) was solved in [5]. For the case of even q, the quasi-recognizability of the groups $B_n(q)$ ($\simeq C_n(q)$) for $n = 2^k \geqslant 8$ and the groups ${}^2D_n(q)$ for $n = 2^k \geqslant 4$ was proved in [6]. The question of the quasi-recognizability of the groups $B_4(q)$ and $C_4(q)$ remains open in both cases of even and odd q.

Our notation and terminology are mostly standard. Let n be a natural number, and let p be a prime. We denote by n_p and $\pi(n)$ the p-part and the set of all prime divisors of the number n, respectively. If m is a natural number, we set $n_m = \prod_{r \in \pi(m)} n_r$ and $n_{m'} = n/n_m$. The largest power of p contained in the spectrum of G is called the *p-period* of G. If L is a group of Lie type, then we denote by $Inndiag(L)$ the group generated by inner and diagonal automorphisms of the group L. We denote by ε a variable with values $+$ or $-$.

1. PRELIMINARY RESULTS

Let G be a finite group. Denote by $s(G)$ the number of connected components of the graph $GK(G)$. For every $i \in \{1, \dots, s(G)\}$, denote by $\pi_i(G)$ the ith component of the graph $GK(G)$, and denote by $\omega_i(G)$ the subset of $\omega(G)$ consisting of all the numbers such that their prime divisors are in $\pi_i(G)$. If the order of the group G is even, then we assume that $2 \in \pi_1(G)$.

Lemma 1 (Gruenberg, Kegel [7, Theorem A])**.** *If G is a finite group such that $s(G) > 1$, then one of the following statements is true*:

(1) *$s(G) = 2$ and G is a Frobenius group*;

(2) *$s(G) = 2$ and $G = ABC$, where A and AB are normal subgroups in G, B is a normal subgroup in BC, and AB and BC are Frobenius groups*;

(3) *there exists a nonabelian simple group S such that $S \leq \overline{G} = G/K \leq \mathrm{Aut}(S)$ for some nilpotent normal subgroup K from G; moreover, K and $\overline{G}/S$ are $\pi_1(G)$-groups, $s(S) \geqslant s(G)$, and, for any $i \in \{1, \dots, s(G)\}$, there exists $j \in \{1, \dots, s(S)\}$ such that $\omega_i(G) = \omega_j(S)$.*

Finite simple groups with disconnected prime graphs were described by Williams [7] and Kondrat'ev [8]. The complete list of these groups with corrected inaccuracies can be found in [5, Tables 1a–1c]. In the present paper, we use the shortened version of this list (see table). The groups given in [5, Tables 1a–1c] separately, outside the infinite series, are absent in our version. As follows from [9, Lemma 4], if S is a simple group and $s(S) > 1$, then, for any $i \in \{2, \dots, s(G)\}$, the set $\omega_i(S)$ has a unique element that is maximal with respect to divisibility. In the table, this maximal element is denoted by $n_i = n_i(S)$ and p is an odd prime.

Infinite series of finite simple groups with disconnected prime graphs

S	Conditions on S	$n_2(S)$
Alt_m	$6 < m = p, p+1, p+2$ and one of the numbers m, $m-2$ is not prime	p
$A_{p-1}(q)$	$(p,q) \neq (3,2), (3,4)$	$(q^p-1)/(q-1)(p,q-1)$
${}^2A_{p-1}(q)$		$(q^p+1)/(q+1)(p,q+1)$
$A_p(q)$	$(q-1) \mid (p+1)$	$(q^p-1)/(q-1)$
${}^2A_p(q)$	$(q+1) \mid (p+1)$ and $(p,q) \neq (3,3), (5,2)$	$(q^p+1)/(q+1)$
$B_m(q)$	$m = 2^k \geqslant 4$ and q is odd	$(q^m+1)/2$
$C_m(q)$	$m = 2^k \geqslant 2$	$(q^m+1)/(2,q-1)$
${}^2D_m(q)$	$m = 2^k \geqslant 4$	$(q^m+1)/(2,q+1)$
${}^2D_m(2)$	$m = 2^k+1 \geqslant 5$	$2^{m-1}+1$
${}^2D_m(3)$	$9 \leqslant m = 2^k+1 \neq p$	$(3^{m-1}+1)/2$
${}^2D_p(3)$	$5 \leqslant p \neq 2^k+1$	$(3^p+1)/4$
$B_p(3)$		$(3^p-1)/2$
$C_p(q)$	$q = 2, 3$	$(q^p-1)/(2,q-1)$
$D_p(q)$	$p \geqslant 5$ and $q = 2, 3, 5$	$(q^p-1)/(q-1)$
$D_{p+1}(q)$	$q = 2, 3$	$(q^p-1)/(2,q-1)$
${}^3D_4(q)$		q^4-q^2+1
$F_4(q)$	q is odd	q^4-q^2+1
$G_2(q)$	$2 < q \equiv \varepsilon 1 \pmod 3$, $\varepsilon = \pm$	$q^2-\varepsilon q+1$
$E_6(q)$		$(q^6+q^3+1)/(3,q-1)$
${}^2E_6(q)$	$q > 2$	$(q^6-q^3+1)/(3,q+1)$

S	Conditions on S	$n_2(S)$	$n_3(S)$
Alt_m	$m > 6$, $m = p$, and $p-2$ is prime	p	$p-2$
$A_1(q)$	$3 < q \equiv \varepsilon 1 \pmod 4$, $\varepsilon = \pm$	$\pi(q)$	$(q+\varepsilon 1)/2$
$A_1(q)$	$q > 2$ and q is even	$q-1$	$q+1$
${}^2D_p(3)$	$p = 2^k+1$	$(3^{p-1}+1)/2$	$(3^p+1)/4$
$G_2(q)$	$q \equiv 0 \pmod 3$	q^2-q+1	q^2+q+1
$F_4(q)$	q is even	q^4+1	q^4-q^2+1
${}^2G_2(q)$	$q = 3^{2k+1} > 3$	$q-\sqrt{3q}+1$	$q+\sqrt{3q}+1$
${}^2F_4(q)$	$q = 2^{2k+1} > 2$	$q^2-\sqrt{2q^3}+q-\sqrt{2q}+1$	$q^2+\sqrt{2q^3}+q+\sqrt{2q}+1$

S	Conditions on S	$n_2(S)$	$n_3(S)$	$n_4(S)$	$n_5(S)$
${}^2B_2(q)$	$q = 2^{2k+1} > 2$	$q-1$	$q-\sqrt{2q}+1$	$q+\sqrt{2q}+1$	
$E_8(q)$	$q \equiv 2, 3 \pmod 5$	$\dfrac{q^{10}-q^5+1}{q^2-q+1}$	$\dfrac{q^{10}+q^5+1}{q^2+q+1}$	q^8-q^4+1	
$E_8(q)$	$q \not\equiv 2, 3 \pmod 5$	$\dfrac{q^{10}-q^5+1}{q^2-q+1}$	$\dfrac{q^{10}+q^5+1}{q^2+q+1}$	q^8-q^4+1	$\dfrac{q^{10}+1}{q^2+1}$

Recall that a subset of vertices of a graph is called a *coclique* if any two vertices of this subset are not adjacent. Denote by $t(G)$ the maximal cardinality of cocliques in $GK(G)$ and, if $2 \in \pi(G)$, then denote by $t(2, G)$ the maximal cardinality of cocliques in $GK(G)$ that contain 2.

Lemma 2 [10,11]**.** *Let L be a finite nonabelian simple group satisfying the conditions $t(L) \geqslant 3$ and $t(2, L) \geqslant 2$, and let G be a finite group satisfying the condition $\omega(G) = \omega(L)$. Then, the following statements are valid*:

(1) *There exists a nonabelian simple group S such that $S \leq \overline{G} = G/K \leq \mathrm{Aut}(S)$, where K is the maximal normal solvable subgroup of G.*

(2) *If a coclique ρ of vertices of the graph $GK(G)$ has order greater than 2, then at most one prime from ρ is in $\pi(K) \cup \pi(\overline{G}/S)$. In particular, $t(S) \geqslant t(G) - 1$.*

(3) *Every prime $r \in \pi(G)$ that is not adjacent in $GK(G)$ with the number 2 does not divide the product $|K| \times |\overline{G}/S|$. In particular, $t(2, S) \geqslant t(2, G)$.*

Lemma 3 [12, Lemma 1]**.** *Suppose that G is a finite group, K is a normal subgroup in G, and G/K is a Frobenius group with kernel F and cyclic complement C. If $(|F|, |K|) = 1$ and F is not contained in $KC_G(K)/K$, then $r|C| \in \omega(G)$ for some prime divisor r of the number $|K|$.*

Lemma 4 [13]**.** *In the group $GL_n(q)$, there is a Frobenius subgroup with kernel of order q^{n-1} and cyclic complement of order $q^{n-1}-1$. In the group $PSL_n(q)$, there is a Frobenius subgroup with kernel of order q^{n-1} and cyclic complement of order $(q^{n-1} - 1)/(n, q - 1)$.*

If q is a natural number, r is an odd prime, and $(q, r) = 1$, then we denote by $e(r, q)$ the multiplicative order of q modulo r, i.e., the smallest natural number m satisfying the condition $q^m \equiv 1 \pmod r$. For odd q, we set $e(2, q) = 1$ if $q \equiv 1 \pmod 4$ and $e(2, q) = 2$ otherwise.

Lemma 5 (Zsigmondy [14])**.** *Let $q > 1$ be a natural number. Then, for every natural number m, there exists a prime r for which $e(r, q) = m$ except for the cases $q = 2$ and $m = 1$, $q = 3$ and $m = 1$, and $q = 2$ and $m = 6$.*

A prime r satisfying the condition $e(r, q) = m$ is called a *primitive prime divisor* of the number $q^m - 1$. In accordance with [11], the largest divisor of $q^m - 1$ such that the set of its prime divisors consists of primitive prime divisors only is called the *largest primitive divisor*. In [15, Lemma 6], the formula is given for calculating largest primitive divisors.

Lemma 6 [16]**.** *If q is an odd prime, $n \geqslant 2$, and $q^n = 2^m + \varepsilon 1$, then $q = 3$, $n = 2$, $m = 3$, and $\varepsilon = +$.*

Lemma 7. *Suppose that q is an odd natural number, n is an even natural number, and u is a power of a prime. If $u^2 + \varepsilon u + 1 = (q^n + 1)/2$, then either $u = 3$, $q = 5$, $n = 2$, and $\varepsilon = +$ or $u = 4$, $q = 5$, $n = 2$, and $\varepsilon = -$.*

Proof. Substituting the values $u \leqslant 4$ into the equation, we obtain the specified solutions. Let $u > 4$. It follows from the equation that $u(2u + \varepsilon 2) = q^n - 1$. Let $n = 2l$. Then, $2u(u + \varepsilon 2) = (q^l - 1)(q^l + 1)$. Since $(q^l - 1, q^l + 1) = 2$, then either $q^l - 1$ or $q^l + 1$ is a multiple of u. If the quotient of this number over u is greater than 1, then $2u \leqslant q^l + 1$; hence, $u + \varepsilon 2 < 2u - 2 \leqslant q^l - 1$, a contradiction. Consequently, $q^l - 1 = u$, and we have $q^l + 1 = 2u + \varepsilon 2$. Hence, $u = 2 - \varepsilon 2 \leqslant 4$. The lemma is proved.

2. PROPERTIES OF THE GROUPS $B_N(Q)$, $C_N(Q)$, AND ${}^2D_N(Q)$

In this section, the necessary information on the spectra of the groups in question, their covers, and automorphic extensions is presented.

Lemma 8 [17]**.** *Let $G \in \{B_n(q), C_n(q)\}$, where $n \geqslant 3$ and q is a power of an odd prime p. Set $d = 2$ for $G = B_n(q)$ and $d = 1$ for $G = C_n(q)$. Then, $\omega(G)$ consists of all the divisors of the following numbers*:

(1) $(q^n \pm 1)/2$;

(2) $[q^{n_1} \pm 1, \ldots, q^{n_s} \pm 1]$, *where* $s \geqslant 2$, $n_1, \ldots, n_s \in \mathbb{N}$, *and* $n_1 + \ldots + n_s = n$;

(3) $p^l(q^{n_1} \pm 1)/d$, *where* $l, n_1 \in \mathbb{N}$ *and* $(p^{l-1}+1)/2 + n_1 = n$;

(4) $p^l[q^{n_1} \pm 1, \ldots, q^{n_s} \pm 1]$, *where* $s \geqslant 2$, $l, n_1, \ldots, n_s \in \mathbb{N}$, *and* $(p^{l-1}+1)/2 + n_1 + \ldots + n_s = n$;

(5) p^l, *where* $l \in \mathbb{N}$ *and* $(p^{l-1}+1)/2 = n$.

As Lemma 8 shows, if $B_n(q) \not\simeq C_n(q)$, then $\omega(B_n(q))$ is a proper subset in $\omega(C_n(q))$. The spectra of the groups ${}^2D_n(q)$ have not been described completely, but the orders of their semisimple elements (see [18]) and the structure of their prime graphs (see [19]) are known. In addition, the group $B_n(q)$ ($\simeq \Omega_{2n+1}(q)$) has a section isomorphic to ${}^2D_n(q)$ ($\simeq P\Omega^-_{2n}(q)$); hence, $\omega({}^2D_n(q))$ is contained in $\omega(B_n(q))$. Thus, for any q, the group $C_n(q)$ has the biggest spectrum among the groups under consideration.

Lemma 9. *Suppose that* $n \geqslant 4$, q *is a power of an odd prime* p, *and* $a \in \omega(C_n(q))$.

(1) *If* $(a,p) = 1$ *and* $a > q^n/3$, *then* $(q^{n-1}+1)(q-1)/2 \leqslant a \leqslant (q^{n-1} - (-1)^n)(q+1)/2$.

(2) *If* $q > p$ *and* $a > q^n/3 + 3$, *then* $(a,p) = 1$.

(3) *If* $q > p$, *then* $a \leqslant (q^{n-1} - (-1)^n)(q+1)/2$; *if* $q = p > 3$, *then* $a \leqslant q^n + q$; *if* $q = p = 3$, *then* $a \leqslant q^n + q^2$.

Proof. (1) Note that, for $q = 3$, the lower bound $(q^{n-1}+1)(q-1)/2$ is greater than $q^n/3$ by exactly 1; hence, for the proof, it is sufficient to establish that $a \leqslant (q^{n-1}-1)(q+1)/2$.

The number a divides one of the numbers specified in the first two items of Lemma 8. If a is a proper divisor of $(q^n \pm 1)/2$, then $a \leqslant (q^n+1)/4 < q^n/3$. If $a = (q^n \pm 1)/2$, then the inequalities required in statement (1) are satisfied.

If a divides $[q^{n_1}-1, q^{n_2}-1]$, where $n_1 + n_2 = n$ and $q > 3$, then

$$a \leqslant \frac{(q^{n_1}-1)(q^{n_2}-1)}{q-1} \leqslant \frac{q^n - q^{n_1} - q^{n_2} + 1}{3} \leqslant \frac{q^n}{3},$$

a contradiction with the conditions of the lemma.

Let a divide $[q^{n_1}-1, q^{n_2}+1]$, where $n_1 + n_2 = n$ and $q > 3$. If a is a proper divisor of this number or $(q^{n_1}-1, q^{n_2}+1) > 2$, then

$$a \leqslant \frac{(q^{n_1}-1)(q^{n_2}+1)}{4} = \frac{q^n + q^{n_1} - q^{n_2} - 1}{4} \leqslant \frac{q^n + q^{n-1}}{4} \leqslant \frac{q^n + q^n/3}{4} = \frac{q^n}{3},$$

which contradicts the conditions of the lemma. Consequently, $a = [q^{n_1}-1, q^{n_2}+1] = (q^{n_1}-1)(q^{n_2}+1)/2$ and the required inequalities are satisfied.

Let a divide $[q^{n_1}+1, q^{n_2}+1]$, where $n_1 + n_2 = n$ and $q > 3$. If a is a proper divisor of this number or $(q^{n_1}+1, q^{n_2}+1) > 2$, then

$$a \leqslant \frac{(q^{n_1}+1)(q^{n_2}+1)}{4} = \frac{q^n + q^{n_1} + q^{n_2} + 1}{4} \leqslant \frac{q^n + q^{n-2} + q^{n-3} + 1}{4} \leqslant \frac{q^n + q^{n-1}}{4} \leqslant \frac{q^n}{3},$$

a contradiction with the conditions. If $a = [q^{n_1}+1, q^{n_2}+1]$, $(q^{n_1}+1, q^{n_2}+1) = 2$, and $n_1 > 1$, then

$$\frac{q^n+1}{2} \leqslant a = \frac{q^n + q^{n_1} + q^{n_2} + 1}{2} \leqslant \frac{q^n + q^{n-2} + q^2 + 1}{2} \leqslant \frac{q^n + q^{n-1} - q - 1}{2};$$

hence, the required inequalities are satisfied. Finally, let $a = [q^{n-1}+1, q+1]$. If n is odd, then $a = (q^{n-1}+1)(q+1)/2$ and the inequalities are satisfied. If n is even, then $a = q^{n-1}+1$ and, hence, $a \leqslant q^n/3$ for $q > 3$ and $a = (q^{n-1}+1)(q-1)/2$ for $q = 3$; i.e., the inequalities are satisfied again.

Let a divide $[q^{n_1} \pm 1, q^{n_2} \pm 1, \ldots, q^{n_s} \pm 1]$, where $s \geqslant 3$ and $n_1 + n_2 + \ldots + n_s = n$. Let us find an upper estimate for a. Since the number $[q^b \pm 1, q^b \pm 1]$, where the signs are chosen independently, divides $q^{2b} - 1$, one can assume that $n_1 < n_2 < \ldots < n_s$. Since the 2-part of the least common multiple of several numbers coincides with the 2-part of one of these numbers, we have

$$a \leqslant \frac{(q^{n_1}+1)\ldots(q^{n_s}+1)}{2^{s-1}} = \frac{q^n + q^{n-n_1} + q^{n-n_2} + \ldots + 1}{2^{s-1}} \leqslant \frac{q^n + q^{n-1} + q^{n-2}}{4} + 2q^{n-3}.$$

If $q > 3$, then $(q^n + q^{n-1} + q^{n-2} + 8q^{n-3})/4 \leqslant q^n(1 + 1/5 + 1/25 + 8/125)/4 = 163q^n/500 < q^n/3$. If $q = 3$, then $a \leqslant (q^{n-1} - 1)(q+1)/2$.

(2) Assume that $(a, p) \neq 1$. Then, a divides one of the numbers specified in the last three items of Lemma 8.

Let a divide $p^l[q^{n_1} \pm 1, q^{n_2} \pm 1, \ldots, q^{n_s} \pm 1]$, where $s \geqslant 1$ and $(p^{l-1}+1)/2 + n_1 + n_2 + \ldots + n_s = n$. Denote $(p^{l-1}+1)/2$ by n_0. It follows from (1) that $a \leqslant p^k(q^{n-n_0}+1)$. Since $k \leqslant n_0$ and $p^2 \leqslant q$, we have $p^k \leqslant q^{n_0/2}$. Thus, $a \leqslant q^{n-n_0/2} + q^{n_0/2} \leqslant q^{n-1/2} + q^{1/2}$. If $q^{1/2} \geqslant 5$, then $a \leqslant q^n/5 + q^{1/2} < q^n/3$. If $q^{1/2} < 5$, then $q = 9$ and $a \leqslant q^n/3 + 3$, which contradicts the assumption.

Let $a = p^l$, where $p^{l-1} + 1 = 2n$. Then, $l \leqslant n$; hence, $a \leqslant q^{n/2} < q^n/3$, a contradiction.

(3) For $q > p$ and $(a, p) = 1$, the required inequality follows from (1) and (2). Let $a = p^{l+1}[q^{n_1} \pm 1, \ldots, q^{n_s} \pm 1]$, where $(p^l+1)/2 + n_1 + \ldots + n_s = n$.

If $l \geqslant 2$, then $l + 1 \leqslant (p^l - 1)/2$ and, consequently,

$$a \leqslant q^{(p^l-1)/2}(q^{n_1+\ldots+n_s}+1) = q^{n-1} + q^{(p^l-1)/2} < q^n.$$

If $l = 1$ and $q > 3$, then $a \leqslant p^2(q^{n-(p+1)/2}+1) \leqslant q^{n-1} + p^2 \leqslant q^n + q$.

If $l = 1$ and $q = 3$, then $a \leqslant q^2(q^{n-2}+1) = q^n + q^2$.

If $l = 0$, then $a \leqslant p(q^{n-1}+1) \leqslant q^n + q$. The lemma is proved.

Lemma 10. *Let $S \in \{B_n(q), C_n(q)\}$, where $n = 2^m \geqslant 4$ and q is a power of an odd prime p. Assume that G is a finite group, K is a nontrivial normal nilpotent subgroup of G, and $G/K \simeq S$. Then, either $\omega(G) \nsubseteq \omega(C_n(q))$ or K is a p-group.*

Proof. Assume that $\omega(G) \subseteq \omega(C_n(q))$ and $r \in \pi(K)$, where $r \neq p$. Without loss of generality, one can assume that K is an r-group. If r divides $(q^n+1)/2$, then $pr \in \omega(G) \setminus \omega(C_n(q))$; hence, $(r, (q^n+1)/2) = 1$. Since the group S is simple, the centralizer $C_G(K)$ either lies in K or contains the preimage in G of the group S. In the latter case, $r(q^n+1)/2 \in \omega(G)$, which is impossible, since $(q^n+1)/2 \in \mu(C_n(q))$. Thus, $C_G(K) \subseteq K$.

The group S contains a subgroup isomorphic to $SL_n(q)$. By Lemma 4, the group $PSL_n(q)$ contains a Frobenius subgroup with kernel of order q^{n-1} and cyclic complement of order $(q^{n-1}-1)/d$, where $d = (n-1, q-1)$. If we take a Hall $\pi(d)'$-subgroup in its preimage in the group $SL_n(q)$, it will be a Frobenius group with kernel of order q^{n-1} and complement of order $t = (q^{n-1}-1)_{d'}$. Hence, by Lemma 3, the group G contains an element of order rt. The group $C_n(q)$ contains an element of order rt only if r divides $q \pm 1$.

Let r divide $q \pm 1$. The group S contains a subgroup isomorphic to $GL_{n-1}(q)$; hence, by Lemma 4, for any $i < n-1$, there is a Frobenius subgroup with kernel of order q^i and cyclic complement of order $q^i - 1$.

Let $r = 2$. Since $n/2 < n - 1$, the group S contains a Frobenius subgroup with kernel of order $q^{n/2}$ and cyclic complement of order $q^{n/2} - 1$. Then, by Lemma 3, the group G contains an element of order $2(q^{n/2} - 1)$, which contradicts the fact that $(q^{n/2} - 1)_2$ coincides with the 2-period of the group $C_n(q)$.

Let r be odd. The group S contains a Frobenius subgroup with kernel of order q^{n-2} and cyclic complement of order $q^{n-2} - 1$. Then, by Lemma 3, the group G contains an element of order $r(q^{n-2} - 1)$. Assume that $r(q^{n-2} - 1) \in \omega(C_n(q))$. Then, by Lemma 8, this number divides a number of the form $a = [q^{n_1} \pm 1, q^{n_2} \pm 1, \ldots, q^{n_s} \pm 1]$, where $n_1 + n_2 + \ldots + n_s = n$. Among n_i, there must be either a number divisible by $n - 2$ or two different numbers divisible by $n/2 - 1$. Consequently, a divides $[q^{n-2} - 1, q^2 + 1]$. However, $[q^{n-2} - 1, q^2 + 1]_r = (q^{n-2} - 1)_r < r(q^{n-2} - 1)_r$, a contradiction. The lemma is proved.

According to [20], a simple group L of Lie type over a field of characteristic p is called *unisingular* if, under the action of the group L on any nontrivial finite abelian p-group K, any semisimple element from L has a nontrivial fixed point in K.

Lemma 11 [20, Theorem 1.3]**.** *The simple groups $B_n(p)$ and $C_n(p)$, where p is an odd prime, are unisingular. The group $E_8(q)$ is unisingular for any q.*

Lemma 12. *Suppose that $n = 2^m \geqslant 4$, p is an odd prime, $\alpha \in \mathbb{N}$, $q = p^\alpha$, and r_{2n-2} is a primitive prime divisor of the number $q^{2n-2} - 1$.*

(1) *Assume that S is one of the groups $B_n(q)$, $C_n(q)$, and ${}^2D_n(q)$; $S \le G \le \mathrm{Aut}(S)$; and $\omega(G) \subseteq \omega(C_n(q))$. If α is odd, then $G = S$; if α is even, then $\pi(G/S) \subseteq \{2\}$.*

(2) *Assume that α is even, $S = B_n(q)$, $S \le G \le \mathrm{Aut}(S)$, and $\omega(G) \subseteq \omega(C_n(q))$. Then, $2pr_{2n-2}$ lies in $\mu(C_n(q)) \setminus \mu(G)$.*

Proof. (1) First of all, $q^n + 1 \in \omega(\mathrm{Inndiag}(S)) \setminus \omega(S)$; hence, G does not contain $\mathrm{Inndiag}(S)$.

Let $r \in \pi(G/S)$ be an odd prime. Then, G contains a field automorphism φ of order r of S. By [21, Proposition 4.9.1(a)], the centralizer $C_S(\varphi)$ is isomorphic to a group of the same Lie type as S but over a field of order $q^{1/r}$; hence, it contains elements of orders 2 and $(q^{n/r} + 1)/2$. Hence, G contains elements of orders $2r$ and $r(q^{n/r} + 1)/2$. However, for odd r, the number $q^{n/r} + 1$ divides $q^n + 1$; hence, 2 and the prime divisors of $(q^{n/r} + 1)/2$ are in different components of the graph $GK(C_n(q))$, a contradiction. Hence, $\pi(G/S) \subseteq \{2\}$.

(2) If $G = B_n(q)$, then the assertion follows from Lemma 8. Therefore, one can assume that $G > S$. As proved above, $\pi(G/S) = \{2\}$. Assume that $2pr_{2n-2} \in \omega(G)$. Then, in $G \setminus S$, there is an involution t such that its centralizer in S contains an element of order pr_{2n-2}. The involution t is not in $\mathrm{Inndiag}(S)$; hence, by [21, Proposition 4.9.1(d)], it is a field automorphism of the group S. By [21, Proposition 4.9.1(a)], the centralizer $C_S(t)$ is isomorphic to a group of type B_n over a field of order $\sqrt{q}$. However, there are no elements of order r_{2n-2} in such a group, a contradiction. The lemma is proved.

3. PROOF OF THE THEOREMS

Let us fix the notation that will be used everywhere in this section.

Let L be one of the groups $B_n(q)$, $C_n(q)$, and ${}^2D_n(q)$, where $q = p^\alpha$ is a power of an odd prime p and $n = 2^k \geqslant 4$ $(\alpha, k \in \mathbb{N})$. Then, as shown in the table, $s(L) = 2$ and $n_2(L) = (q^n + 1)/2$. In addition, by [19, Tables 6, 8] we have $t(L) = (3n + 4)/4$.

The set $\pi(L)$ consists of the number p and of the divisors of the numbers $q^i - 1$, where $1 \leqslant i \leqslant 2n$. If not stated otherwise, r_i denotes some primitive prime divisor of $q^i - 1$. By the Zsigmondy theorem

(Lemma 5), such a divisor exists for any $i > 2$. Note that the 2-period of the group L coincides with the 2-part of the number $(q^n - 1)/2$.

Let G be a finite group with the property $\omega(G) = \omega(L)$. By the Gruenberg–Kegel theorem (Lemma 1), there exists a nonabelian simple group S such that $S \leq \overline{G} = G/K \leq \mathrm{Aut}(S)$, where K is a normal nilpotent subgroup of G; moreover, $s(S) \geqslant 2$ and $n_2(L) = n_i(S)$ for some $i > 1$. In addition, $t(S) \geqslant t(L) - 1 = 3n/4$ by item (2) of Lemma 2.

Let $K \neq 1$. Then, $S \cap C_G(K)K/K = 1$. Indeed, the group $C_G(K)K/K$ would otherwise contain the whole simple group S; hence, the group G would have an element of order $rn_2(S)$, where $r \in \pi_1(G)$, which is impossible.

Proposition 1. *The group S is isomorphic to one of the groups $B_n(q)$, $C_n(q)$, and ${}^2D_n(q)$.*

Proof. In the proof, we successively take for the group S the groups specified in the table. The information on cyclic tori of groups of Lie type that is used in the proof can be found in [18] for classical groups and in [22] for exceptional groups.

1. Assume that $S \simeq Alt_m$. Then, $(q^n + 1)/2 = r$, where $r = m$, $m - 1$, or $m - 2$. Consider a coclique in $GK(L)$ consisting of primitive divisors r_{n-1}, r_{2n-2}, and r_{2n-4}. By Lemma 2, at least two numbers from this coclique are in $\pi(S)$. On the other hand,

$$r_{n-1} \leqslant \frac{q^{n-1}-1}{q-1} \leqslant \frac{q^{n-1}-1}{2} < \frac{q^n+1}{4} = \frac{r}{2} \leqslant \frac{m}{2},$$

$$r_{2n-2} \leqslant \frac{q^{n-1}+1}{q+1} \leqslant \frac{q^{n-1}+1}{4} < \frac{q^n+1}{4} = \frac{r}{2} \leqslant \frac{m}{2},$$

$$r_{2n-4} \leqslant \frac{q^{n-2}+1}{2} < \frac{q^n+1}{4} = \frac{r}{2} \leqslant \frac{m}{2};$$

consequently, the product of any two of these numbers lies in $\omega(S) \setminus \omega(L)$, a contradiction.

2. Assume that $S \simeq A_m^{\varepsilon}(u)$, where $u = v^{\beta}$, v is a prime, $\beta \in \mathbb{N}$, m is an odd prime, and $u - \varepsilon 1$ divides $m + 1$. Then, $(q^n + 1)/2 = (u^m - \varepsilon 1)/(u - \varepsilon 1)$. This equality implies that

$$\frac{q^n-1}{2} = u\frac{u^{m-1}-1}{u-\varepsilon 1}. \tag{1}$$

Assume that $u = 2^{\beta}$. Then, $u = (q^n - 1)_2/2 \geqslant 8$ coincides with the 2-period of the group L. On the other hand, $u - \varepsilon 1 \leqslant (m + 1)/2$; hence, $m \geqslant u + 1 = 2^{\beta} + 1$. Consequently, the group S contains a unipotent element of order $2^{\beta+1} = 2u = (q^n - 1)_2$, a contradiction.

Assume that u is odd. Then, it follows from (1) that $(u^{m-1} - 1)_2 > (q^n - 1)_2/2$. Since S contains a cyclic torus of order $u^{m-1} - 1$, the 2-period of the group S exceeds the 2-period of the group L in this case as well, a contradiction.

3. Assume that $S \simeq A_{m-1}^{\varepsilon}(u)$, where $u = v^{\beta}$, v is a prime, $\beta \in \mathbb{N}$, and m is an odd prime not dividing $u - \varepsilon 1$. Then, as in the previous case, $(q^n + 1)/2 = (u^m - \varepsilon 1)/(u - \varepsilon 1)$; hence,

$$2u(u^{m-1} - 1) = (q^n - 1)(u - \varepsilon 1). \tag{2}$$

Note that $u \neq 2$ because $q^n - 1$ is a multiple of 16. In addition, $t(S) = (m + 1)/2 \geqslant 3n/4$, which implies $m \geqslant 3n/2 - 1 \geqslant 5$.

It follows from (1) that the number $e(v, q)$ is a power of 2. Assume that $e(v, q) > 2$. Then, $\{v, r_{2n}, r_{2n-2}, r_{n-1}\}$ is an independent set of vertices of the graph $GK(G)$; hence, by Lemma 2, the set $\pi(S)$ contains, in addition to v and r_{2n}, at least one of the numbers r_{2n-2} and r_{n-1}.

Let us denote it by r. The vertices r and v are not adjacent in $GK(S)$ and r does not divide $(u^m-\varepsilon 1)/(u-\varepsilon 1)=(q^n+1)/2$; consequently, by [19, Proposition 3.1], the number r is a primitive divisor of $u^{m-1}-1$. Since $m\geqslant 5$, the number r does not divide $u-\varepsilon 1$. Then, it follows from (1) that r divides q^n-1, a contradiction with the definition of a primitive divisor. Thus, v is a primitive divisor of either $q-1$ or q^2-1.

There is an element of order $u^{m-1}-1$ in the group S and, hence, in the group L. As follows from (2), this order is a multiple of the primitive divisors $r_n, r_{n/2},\ldots,r_4$. Moreover, by the equality

$$u^{m-1}-1=\frac{u-\varepsilon 1}{u}\times\frac{q^n-1}{2},$$

it does not divide $(q^n-1)/2$ and does not exceed $(q^n-1)/3$ because $u\geqslant 3$. Since $u^{m-1}-1$ does not divide $(q^n\pm 1)/2$, it follows, by Lemma 8, that it divides a number a of one of the following two forms:

$$[q^{n_1}-\varepsilon_1,\ldots,q^{n_s}-\varepsilon_s],\qquad \text{where } n_1+\ldots+n_s=n \quad\text{and}\quad \varepsilon_i=\pm 1;$$

$$p^l[q^{n_1}-\varepsilon_1,\ldots,q^{n_s}-\varepsilon_s],\quad \text{where } (p^{l-1}+1)/2+n_1+\ldots+n_s=n \quad\text{and}\quad \varepsilon_i=\pm 1.$$

We assume that $n_1\geqslant\ldots\geqslant n_s$. The number a is a multiple of r_n; consequently, $n_1=n/2$ and $\varepsilon_1=-1$. Further, a is a multiple of $r_{n/2}$; hence, either $n_2=n/2$ and $\varepsilon_2=1$ or $n_2=n/4$ and $\varepsilon_2=-1$. In the former case, $n_1+n_2=n$; hence, $a=[q^{n/2}+1,q^{n/2}-1]$ divides q^n-1, a contradiction. Therefore, $n_2=n/4$. Proceeding with the argument in a similar way, we find that $s\geqslant k-1$ for some natural number k and

$$n_1+n_2+\ldots+n_{k-1}=n/2+n/4+\ldots+2=n-2.$$

If p does not divide a, then a divides q^n-1, which is impossible. Consequently, p divides a; hence, either

$$a=p[q^{n/2}+1,\ldots,q^2+1,q\pm 1]=p\,\frac{q^n-1}{2^{k-1}(q\mp 1)}$$

or $p=3$ and

$$a=p^2[q^{n/2}+1,\ldots,q^2+1]=p^2\frac{q^n-1}{2^{k-2}(q^2-1)}.$$

Since $a\geqslant(q^n-1)/3$, we find in the former case that $3p\geqslant 2^{k-1}(q\mp 1)$, which implies either $k=2$ and $q=p$ or $k=3$ and $q=p=3$. In the latter case, we have $3p^2\geqslant 2^{k-2}(q^2-1)$, which implies that $k\in\{2,3\}$ and $q=p=3$.

Let $k\in\{2,3\}$ and $q=p=3$. The number v is a divisor of $q-1=2$ or $q^2-1=8$, which implies $v=2$. It follows from (2) that $u=2^{k+1}$. It can be verified directly that, for $(q,u,n)\in\{(3,8,4),(3,16,8)\}$, equality (2) is impossible for all m.

Let $k=2$ and $p=q$. Then, $u^{m-1}-1=(q^n-1)(u-\varepsilon 1)/(2u)$ divides $(q^n-1)p/(2(p\pm 1))$. Consequently, $(u-\varepsilon 1)(p\pm 1)$ divides pu, which implies $p=u-\varepsilon 1$. Since $u<p$, we find that $\varepsilon=-$ and $u=p-1$. Thus, $2(p-1)^{m-1}=(p^2+1)(p+1)p+2$. The right-hand side is congruent to 6 modulo $p-1$; hence, $p\in\{3,7\}$, which implies $u\in\{2,6\}$, a contradiction.

4. Assume that $S\simeq A^{\varepsilon}_{m-1}(u)$, where $u=v^{\beta}$, v is a prime, $\beta\in\mathbb{N}$, m is an odd prime, and $u-\varepsilon 1$ is a multiple of m. Then,

$$\frac{q^n+1}{2}=\frac{u^m-\varepsilon 1}{(u-\varepsilon 1)m}. \tag{3}$$

In view of [19, Table 6] and the inequality $t(S) \geqslant 3n/4$, we have $(m+1)/2 \geqslant 3n/4$, which implies $m \geqslant 3n/2-1$. Since $n \geqslant 4$, we find that $m \geqslant 5$ and $u \geqslant m+\varepsilon 1 \geqslant 4$. For $q \geqslant 3$, $n \geqslant 4$, $m \geqslant 5$, and $u \geqslant 4$, it follows from (3) that $q > u+1$.

The group S contains an element of order $t = (u^{m-1}-\varepsilon 1)/m$. Consequently, $t \in \omega(L)$ and

$$t = \frac{u-\varepsilon 1}{u}\left(\frac{u^m-1}{(u-\varepsilon 1)m} - \frac{1}{m}\right) = \frac{u-\varepsilon 1}{u}\left(\frac{q^n+1}{2} - \frac{1}{m}\right) = \frac{u-\varepsilon 1}{u} \times \frac{mq^n+m-2}{2m}. \qquad (4)$$

Assume that $q = p$. Then, $p > u-\varepsilon 1 \geqslant m-2$; hence, p divides neither $u-\varepsilon 1$ nor $m-2$. Consequently, p does not divide the right-hand side of (4); hence, p does not divide t. Thus, either $q > p$ or $(t,p) = 1$.

Let $\varepsilon = -$. Then,

$$t = \frac{u+1}{u}\left(\frac{q^n+1}{2} - \frac{1}{m}\right) \geqslant \frac{q+1}{q} \times \frac{q^n-1}{2} = \frac{q^n+q^{n-1}-1-1/q}{2}.$$

On the other hand, by item (3) of Lemma 9, the number t does not exceed

$$\frac{(q^{n-1}-1)(q+1)}{2} = \frac{q^n+q^{n-1}-q-1}{2},$$

a contradiction.

Let $\varepsilon = +$. Then, $u \geqslant m+1 \geqslant 6$. If $u = 7$, then $m = 5$, a contradiction with the fact that m divides $u-1$. Thus, $u \geqslant 8$; hence, t satisfies the estimate

$$t = \frac{u-1}{u}\left(\frac{q^n+1}{2} - \frac{1}{m}\right) \geqslant \frac{7}{8} \times \frac{q^n-1}{2} > \frac{q^n}{3} + 3.$$

By items (1) and (2) of Lemma 9, the inequality $t \geqslant (q^{n-1}+1)(q-1)/2$ is satisfied, which implies the estimate

$$\left(\frac{q^n+1}{2} - t\right) : \frac{q^n+1}{2} \leqslant \left(\frac{q^n+1}{2} - \frac{(q^{n-1}+1)(q-1)}{2}\right) : \frac{q^n+1}{2} = \frac{q^{n-1}-q+2}{q^n+1} < \frac{1}{q}.$$

On the other hand,

$$\left(\frac{u^m-1}{m(u-1)} - \frac{u^{m-1}-1}{m}\right) : \frac{u^m-1}{m(u-1)} = \frac{u^{m-1}+u-2}{u^m-1} > \frac{1}{u}.$$

Consequently, $1/u < 1/q$; hence, $u > q$, a contradiction.

5. Assume that $S \simeq A_1(u)$, where $u = v^\beta$ for a prime v and a natural number β.

Let $v = 2$. Then, $(q^n+1)/2 = u \pm 1$. If $(q^n+1)/2 = u-1$, then $q^n+3 = 2^{\beta+1}$; however, q^n+3 is not a multiple of 8, a contradiction. Hence, $q^n-1 = 2^{\beta+1}$ and, by Lemma 6, we find that $n = 2$, a contradiction.

Thus, v is odd. Then, either $(q^n+1)/2 = v$ or $(q^n+1)/2 = (u\pm 1)/2$. Since $t(S) = 3$ and $t(S) \geqslant 3n/4$, we have $n = 4$. The numbers r_3, r_4, r_6, and r_8 form a coclique in the graph $GK(G)$. It follows from item (2) of Lemma 2 and from the equality $t(S) = 3$ that one of them is not in $\pi(S)$ and the remaining three are in $\pi(S)$. Since these three numbers are not adjacent in $GK(S)$, one of them coincides with v, the second divides $(u-1)/2$, and the third divides $(u+1)/2$. In particular, $v \neq p$.

If $(q^4+1)/2 = (u+1)/2$, then $u = q^4$, a contradiction.

Assume that $(q^4+1)/2=(u-1)/2$. Then, $u=q^4+2$ and $u+1=q^4+3$. Hence, r_4 is not in $\pi(S)$. If one of the numbers r_3 or r_6 divides u, then, by the equality $(q^4+2, q^3-\varepsilon 1)=(q-\varepsilon 2, 9)$, it is equal to 3, a contradiction.

Thus, $(q^4+1)/2=v$. Then, $u=v$, otherwise $(u+1)/2$ would be greater than $v^2/2=(q^4+1)^2/8$ and, hence, greater than all the elements from $\omega(L)$. Consequently, $u-1=(q^4-1)/2$ and $u+1=(q^4+3)/2$. Thus, r_4 divides $u-1$. Hence, one of the numbers r_3 and r_6 divides q^4+3 and the other number does not divide the order of the group S. Assume that $r_i\in\pi(S)$ and r_j does not divide $|S|$, where $i,j\in\{3,6\}$. Then, any primitive divisor of q^i-1 lies in $\pi(S)$ and divides q^4+3; hence, the largest primitive divisor of q^i-1, which is equal to $(q^2+\varepsilon q+1)/(q-\varepsilon 1,3)$, divides q^4+3. By the equality $(q^4+3, q^3-\varepsilon 1)=(q+\varepsilon 3, 28)$, we find that $(q^2+\varepsilon q+1)/(q-\varepsilon 1,3)=(q+\varepsilon 3,7)$. The only odd solution of this equation is the number $q=3$.

Let $q=3$. Then, $u=41$ and $r_3=13\in\pi(K)$. By Lemma 4, the group S has a Frobenius subgroup with kernel of order u and cyclic complement of order $(u-1)/2=20$. It follows from Lemma 3 that $260\in\omega(G)\setminus\omega(L)$, a contradiction.

6. Assume that S is isomorphic to one of the groups $B_m(u)$, $C_m(u)$, and ${}^2D_m(u)$, where m is a power of 2. If u is even, then $(q^n+1)/2=u^m+1$; consequently, $q^n-1=2u^m$, which implies $n=2$ by Lemma 6, a contradiction. Thus, $u=v^\beta$, where v is an odd prime and $\beta\in\mathbb{N}$. Then, $(q^n+1)/2=(u^m+1)/2$, which implies $p=v$ and $\alpha n=\beta m$. In addition, $t(S)=3m/4+1\geqslant 3n/4$; hence, $m\geqslant n-4/3$. Since m and n are powers of 2 greater than 1, the stronger inequality $m\geqslant n$ is true. If $m>n$, then $\beta<\alpha$; consequently, $2\alpha(n-1)<2\beta(m-1)<2\alpha n$. Then, the number r with the property $e(r,p)=2\beta(m-1)$ lies in $\omega(S)\setminus\omega(L)$, which is impossible. Thus, $m=n$ and $u=q$.

7. Assume that S is isomorphic to one of the groups $D_m(u)$, $B_m(u)$, $C_m(u)$, and $D_{m+1}(u)$, where m is a prime; moreover, $m\geqslant 5$ and $u\in\{2,3,5\}$ in the first case and $u\in\{2,3\}$ in the remaining cases. Then, $(q^n+1)/2=(u^m-1)/(2,u-1)$ and $(3m+3)/4\geqslant t(S)\geqslant 3n/4$. Thus, $m\geqslant n-1$.

Let $u=2$. Then, $q^n-1=2^m-4$, which is impossible, since q^n-1 is a multiple of 8.

Let $u\in\{3,5\}$. The group S contains a parabolic subgroup P such that its Levy factor is of type A_{m-1} and, consequently, contains an element of order $t=(u^m-1)/(q-1)$. This element and the unipotent radical of the group P generate a Frobenius group with cyclic complement of order t. Hence, if $r\in\pi(K)$ and $r\neq u$, then, by Lemma 3, the group G has an element of order rt, a contradiction, since $t\in\mu(L)$. Thus, $\pi(\overline{G}/S)\cup\pi(K)\subseteq\{2,u\}$.

Let $m>3$. Then, $t(S)>3$; hence, the cocliques of the graph $GK(S)$ of maximal cardinality contain neither 2 nor u. Consequently, $t(S)=t(L)$; i.e., $[(3m+5)/4]=(3n+4)/4$ for $S\not\simeq D_m(u)$ and $[(3m+1)/4]=(3n+4)/4$ for $S\simeq D_m(u)$. In the former case, we have $3m+3=3n+4$ or $3m+5=3n+4$, a contradiction. The latter case is possible only for $m=n+1$; hence, $q^n+1=u^{n+1}-1$. If $q^4\geqslant u^5$ or $q\leqslant u$, then this equality is impossible. Hence, $u=5$, $q=7$, and $7^n+2=5^{n+1}$; however, 7^n has remainder 1 or 4 when divided by 5, a contradiction.

8. Assume that $S\simeq {}^2D_m(2)$, where $m=2^l+1\geqslant 5$. Then, $(q^n+1)/2=2^{m-1}+1$; hence, $2^m=q^n-1$. By Lemma 6, we find that $n=2$, a contradiction.

9. Assume that $S\simeq {}^2D_m(3)$, where $m=2^l+1$ or m is a prime. Then, either $(q^n+1)/2=(3^{m-1}+1)/2$ or $(q^n+1)/2=(3^m+1)/4$. In the former case, $m=n+1$ and $q=3$. Then, $(3^m+1)/4\in\omega(S)\setminus\omega(L)$, a contradiction. In the latter case, $2(q^n-1)=3(3^{m-1}-1)$. The group S has a cyclic torus of order $(3^{m-1}-1)/2$; hence, the 2-period of the group S is greater than the 2-period of the group L, a contradiction.

10. Assume that S is isomorphic to one of the groups ${}^3D_4(u)$, $G_2(u)$, and $F_4(u)$. In this case,

$(q^n+1)/2$ is equal to one of the numbers u^4-u^2+1, $u^2\pm u+1$, and u^4+1. Then, $n=2$ by Lemmas 7 and 6, a contradiction.

11. Assume that $S\simeq {}^2B_2(u)$, where $u=2^{2\beta+1}>2$ ($\beta\in\mathbb{N}$). Then, either $(q^n+1)/2=u-1$ or $(q^n+1)/2=u\pm\sqrt{2u}+1$. In the former case, $q^n+3=2^{2\beta+2}$; however, q^n+3 is not a multiple of 8, a contradiction.

In the latter case, $q^n=2u\pm2\sqrt{2u}+1=2^{2\beta+2}\pm2^{\beta+2}+1=(2^{\beta+1}\pm1)^2$. Then, $q^{n/2}=2^{\beta+1}\pm1$; hence, $q=3$, $n=4$, and $\beta=2$ by Lemma 6. In this case, $31\in\omega(S)\setminus\omega(L)$, a contradiction.

12. Assume that $S\simeq {}^2G_2(u)$, where $u=3^{2\beta+1}>3$ ($\beta\in\mathbb{N}$). Then, $(q^n+1)/2=u\pm\sqrt{3u}+1$; hence, $q^n-1=2\times3^{\beta+1}(3^\beta\pm1)$. Consequently, q^n-1 is a multiple of $3^{\beta+1}$. Taking into account that $q^{2i}+1$ is not a multiple of 3, we find that $q+1\geqslant3^{\beta+1}$. Thus,

$$q^n-1>6(q+1)(q-1)\geqslant6\times3^{\beta+1}(3^{\beta+1}-2)>2\times3^{\beta+1}(3^\beta+1),$$

a contradiction.

13. Assume that $S\simeq {}^2F_4(u)$, where $u=2^{2\beta+1}\geqslant8$ ($\beta\in\mathbb{N}$). Then,

$$\frac{q^n+1}{2}=u^2+\varepsilon\sqrt{2u^3}+u+\varepsilon\sqrt{2u}+1. \tag{5}$$

Since $t(S)=5$ and $t(S)\geqslant3n/4$, we have $n=4$. It is verified directly that the case $\beta\leq3$ is impossible; hence, $\beta\geqslant4$. Then, the number q^4-1, which is equal to

$$2\sqrt{2u}(u+1)\Big(\sqrt{\frac{u}{2}}+1\Big),$$

must be a multiple of $2\sqrt{2u}\geqslant64$; consequently, $q\equiv\pm1\pmod{16}$. In particular, $q\geqslant17$.

The group S contains an element of order $t=u^2-\varepsilon\sqrt{2u^3}+u-\varepsilon\sqrt{2u}+1$. Assume that $q=p$ and p divides t. Then, p divides the number q^4-t, which is equal to

$$u^2+\varepsilon3\sqrt{u^3}+u+\varepsilon3\sqrt{2u}=\sqrt{2u}(u+1)\Big(\sqrt{\frac{u}{2}}+3\varepsilon\Big).$$

On the other hand, $t=u^2+(u+1)(1-\varepsilon\sqrt{2u})$; hence, p does not divide $u+1$. Consequently, p divides $\sqrt{u/2}+3\varepsilon=2^\beta+3\varepsilon$. Assume that $p<2^\beta$. Then, $q^4=p^4<2^{4\beta}$. On the other hand,

$$q^4=2u^2-2\varepsilon\sqrt{2u^3}+2u-2\varepsilon\sqrt{2u}+1>u^2=2^{4\beta+4},$$

a contradiction. Hence, $\varepsilon=+$ and $p=2^\beta+3$, which is impossible, since $q=p\equiv\pm1\pmod{16}$. Thus, $(t,p)=1$ or $q>p$.

Let $\varepsilon=-$. Then, it follows from (5) that $q^4>(q^2+1)/2>u^2/4$; hence, $q>\sqrt{u/2}$. In addition, $t>(q^4+1)/2$ and, by Lemma 9, we have $t\leqslant(q^4+q^3-q-1)/2$. Consequently,

$$\Big(t-\frac{q^4+1}{2}\Big):\frac{q^4+1}{2}\leqslant\frac{q^3-q+2}{q^4+1}\leqslant\frac{1}{q}.$$

On the other hand,

$$\Big(t-\frac{q^4+1}{2}\Big):\frac{q^4+1}{2}=\frac{2\sqrt{2u^3}+2\sqrt{2u}}{u^2+\sqrt{2u^3}+u+\sqrt{2u}+1}\geqslant\frac{2\sqrt{2u}}{2u^2}=\sqrt{\frac{2}{u}},$$

a contradiction.

Let $\varepsilon = +$. Then, it follows from (5) that $q^4 > 2u^2$. Hence, $q^2 > \sqrt{2}u$ and

$$t = \frac{q^4+1}{2} - 2\sqrt{2u^3} - 2\sqrt{2u} \geqslant \frac{q^4+1}{2} - 2^{3/4}q^3 - 2^{5/4}q \geqslant \frac{q^4-4q^3-5q+1}{2} > \frac{q^n}{3} + 3.$$

By Lemma 9, we have $t \geqslant (q^4 - q^3 + q - 1)/2$. Consequently,

$$\left(\frac{q^4+1}{2} - t\right) : \frac{q^4+1}{2} \leqslant \frac{q^3-q-2}{q^4+1} \leqslant \frac{1}{q}.$$

On the other hand, as shown above, this ratio is greater than $\sqrt{2/u}$, a contradiction.

14. Let $S \simeq E_6^{\varepsilon}(u)$. Then, $(q^n+1)/2 = (u^6+\varepsilon u^3+1)/(u-\varepsilon 1, 3)$. If 3 does not divide $u-\varepsilon 1$, then $n = 2$ by Lemma 7, which is not so. Therefore, 3 divides $u - \varepsilon 1$. Then, $(u^6+\varepsilon u^3+1)/3 = (q^n+1)/2$, which implies $2(u^6 + \varepsilon u^3 - 2) = 3(q^n - 1)$. If u is even, then the left-hand side is congruent to 4 modulo 8. On the other hand, the right-hand side is a multiple of 8. Thus, u is odd.

Let us compare the 2-periods of the groups S and L. Since S has a cyclic torus of order $u^4 - 1$, we have $(u^4 - 1)_2 \leqslant (q^n - 1)_2/2$. On the other hand, it follows from the relations

$$\frac{3(q^n-1)}{2} = u^6 + \varepsilon u^3 - 2 = (u^3 - \varepsilon 1)(u^3 + \varepsilon 2)$$

that $(q^n - 1)_2/2 = (u^3 - \varepsilon 1)_2$. Thus, $(u^4 - 1)_2 \leqslant (u^3 - \varepsilon 1)_2 = (u - \varepsilon 1)_2$, a contradiction.

15. Assume that $S \simeq E_8(u)$. Then,

$$\frac{q^n+1}{2} \in \left\{\frac{u^{10}+u^5+1}{u^2+u+1}, \frac{u^{10}-u^5+1}{u^2-u+1}, u^8-u^4+1, \frac{u^{10}+1}{u^2+1}\right\}.$$

Note that $(u^{10}+u^5+1)/(u^2+u+1) = k_{15}$, $(u^{10}-u^5+1)/(u^2-u+1) = k_{30}$, $u^8-u^4+1 = k_{24}$, and $(u^{10}+1)/(u^2+1) = (5, u^2+1)k_{20}$, where k_i is the largest primitive divisor of $u^i - 1$. The case $(q^n+1)/2 = u^8 - u^4 + 1$ is impossible by Lemma 7. Let us fix a number l from the set $\{15, 30, 20\}$ such that $(q^n + 1)/2 = k_l$.

If $(q^n + 1)/2 = (u^{10} + 1)/(u^2 + 1)$, then

$$\frac{q^n-1}{2} = u^2(u^2-1)(u^4+1). \tag{6}$$

If $(q^n + 1)/2 = (u^{10} + \varepsilon u^5 + 1)/(u^2 + \varepsilon u + 1)$, then

$$\frac{q^n-1}{2} = u(u^4-1)(u^3-\varepsilon u^2+\varepsilon 1). \tag{7}$$

Assume first that u is odd. Then, as seen from (6) and (7), $(q^n-1)_2/2 = (u^4-1)_2$. The group S has a cyclic torus of order u^8-1; hence, it has an element of order $(u^8-1)_2 > (u_4-1)_2$. Consequently, the 2-period of the group S is greater than the 2-period of the group L, a contradiction.

Now, let $u = 2^{\beta}$ ($\beta \in \mathbb{N}$). It is specified in [19, Tables 6, 5] that $t(2, L) = 2$ and $t(2, S) = 5$. Let w_{20}, w_{24}, and w_{30} be prime divisors of the numbers k_{20}, k_{24}, and k_{30}, respectively. Note that all these divisors are greater than 5, pairwise nonadjacent, and not adjacent to 2 in $GK(L)$. Assume that one of them, say r, divides $|\overline{G}/S|$. Then, the group $\overline{G}$ has a field automorphism of order r of S. The centralizer of this automorphism in S is isomorphic to the group $E_8(u_0)$, where $u_0 = u^{1/r}$. Consequently, it contains an element of order w_l, where w_l is a primitive prime divisor of $u_0^l - 1$.

Since $(r, l) = 1$, the number w_l is a primitive prime divisor of $u^l - 1$. Then, $r \in \pi(\overline{G}/S) \subseteq \pi_1(G)$, w_l divides $(q^n + 1)/2$, and $rw_l \in \omega(G)$, a contradiction. Let the group $\overline{G}$ have a field automorphism of order 2 of S. Then, its centralizer in S is isomorphic to the group $E_8(u_0)$, where $u_0 = u^{1/2}$. It can easily be verified that the order $|E_8(u_0)|$ is mutually prime with each of the numbers k_{20}, k_{24}, and k_{30}. Thus, w_{20}, w_{24}, w_{30}, and 2 are pairwise nonadjacent in $GK(\overline{G})$. Since $t(2, L) = 2$, it follows that either $2 \in \pi(K)$ or $w_i, w_j \in \pi(K)$, where $i, j \in \{20, 24, 30\}$, $i \neq j$, and $i \neq l \neq j$.

Let $2 \in \pi(K)$. Without loss of generality, one can assume that K is an elementary abelian 2-group. By Lemma 11, the group S is unisingular; hence, its semisimple element of order $k_l = (q^n + 1)/2$ has a nontrivial fixed point in K. Consequently, $q^n + 1 \in \omega(G) \setminus \omega(L)$, a contradiction.

Let $w_i, w_j \in \pi(K)$, where $i, j \in \{20, 24, 30\}$, $i \neq j$. The numbers k_i and k_j are mutually prime; hence, at least one of them is not a multiple of p. Let it be k_i. Assume that $2k_i \notin \omega(G)$. Then, k_i can divide only odd orders of maximal tori of the group L. By Lemma 8 and [18, Theorem 6], the only torus of odd order in the group L is the torus of order $(q^n + 1)/2 = k_l$, which is not a multiple of w_i. Hence, $2k_i \in \omega(G)$. Since $2r \notin \pi(\overline{G})$ for any prime divisor r of the number k_i and $2 \notin \pi(K)$, the group K contains an element of order k_i. Since the group K is nilpotent, we have $k_i w_j \in \omega(K)$.

As follows from item (3) of Lemma 9, any element from $\omega(G)$ does not exceed $10q^n/9$. The right-hand sides of equalities (6) and (7) are less than $2u^8$; hence, $q^n \leqslant 4u^8$. Consequently, $k_i w_j \leqslant 40u^8/9$. On the other hand, $k_i \geqslant k_{20} \geqslant (u^{10}+1)/(5u^2+5) > u^{10}/(5u^2+5)$ and $w_j \geqslant 40$ because $w_j - 1$ must be a multiple of j. Thus, $8u^{10}/(u^2 + 1) < 40u^8/9$, which implies $9u^{10} < 5u^{10} + 5u^8$ and $4u^2 < 5$, a contradiction.

16. Let S be a simple group with a disconnected prime graph not specified in the table. Then, $(q^n + 1)/2 = n_i = n_i(S)$ for some $i > 1$; consequently, $2n_i - 1$ is equal to the fourth power of a natural number. It is verified directly that this is possible only in the case $S \simeq F_1$ and $n_i = 41$. Then, $q = 3$ and $n = 4$. Since $23 \in \omega(F_1) \setminus \omega(L)$, this case is impossible.

The proposition is proved.

Since $\omega(^2D_n(q)) \subset \omega(B_n(q)) \subset \omega(C_n(q))$, it follows from Proposition 1 that, if $L = {}^2D_n(q)$, then the group S is isomorphic to L. Thus, Theorem 1 is proved.

It follows from Proposition 1 and the above strict inclusions that, if $L = B_n(q)$, then S is isomorphic to $^2D_n(q)$ or L.

Proposition 2. *Let the group L be equal to $B_n(q)$ or $C_n(q)$ with $n \geqslant 8$. Then, $S \not\simeq {}^2D_n(q)$.*

Proof. Assume the contrary. Then, $r_{n-2}r_{n+2} \in \omega(L) \setminus \omega(S)$. By Lemma 12, the index $|\overline{G} : S|$ is not a multiple of an odd prime. Hence, one of the numbers r_{n-2} and r_{n+2} divides $|K|$. Let us denote it by r. Let k_{n-2} be the largest primitive prime divisor of the number $q^{n-2} - 1$. The group S contains a subgroup of type A_{n-2} over a field of order q. By Lemma 4, the group S has Frobenius subgroups with kernels of order q^{n-2} and q^{n-3} and cyclic complements of order k_{n-2} and $q^{n-3} - 1$, respectively. Consequently, rk_{n-2}, $r(q^{n-3} - 1) \in \omega(G)$. On the other hand, if $r = r_{n-2}$, then $rk_{n-2} \notin \omega(L)$ and, if $r = r_{n+2}$, then $r(q^{n-3} - 1) \notin \omega(L)$ by the inequality $n - 3 + n/2 + 1 > n$, a contradiction. The proposition is proved.

Proposition 3. *Suppose that L, $S \in \{B_n(q), C_n(q)\}$ and α is odd. Then, $G = S \simeq L$.*

Proof. Assume that $K \neq 1$. Then, K is a p-group by item (1) of Lemma 10. Without loss of generality, one can assume that K is an elementary abelian group. The group S has a subgroup isomorphic to $B_n(p)$ or $C_n(p)$. Consequently, by Lemma 11, some element of order $(p^n + 1)/2$ of the group S has a nontrivial fixed point in K. Thus, the natural semidirect product KS contains an element of order $p(p^n + 1)/2$. By [23, Lemma 10], the group G also contains an element of this order. On the other hand, α is odd; hence, $p^n + 1$ divides $q^n + 1$. Therefore, in view of the table, the prime divisors of the number $(p^n+1)/2$ and p are in different components of the graph $GK(L)$, a contradiction.

Thus, $K=1$. By item (1) of Lemma 12, the group G coincides with S. Since $\omega(B_n(q)) \neq \omega(C_n(q))$, we find that $S \simeq L$. The proposition is proved.

The assertion of Theorem 2 follows from Propositions 1, 2, and 3 in the case when α is odd.

Proposition 4. *Let α be even, and let $L = C_n(q)$. Then, $S \not\simeq B_n(q)$.*

Proof. Assume the contrary. Then, $pr_{2n-2}(q^{n-1}+1)_2 \in \omega(G)\setminus\omega(\overline{G})$ by item (2) of Lemma 12. Hence, the subgroup K is not equal to 1 and, by Lemma 10, it is a p-group. Moreover, the group G has an element x of order $r = r_{2n-2}$ such that $C =: C_K(x) \neq 1$. Denote by $\overline{x}$ the image of x in $\overline{G}$. By item (1) of Lemma 12, we have $\pi(\overline{G}/S) \subseteq \{2\}$; hence, $\overline{x}$ is an element of order r of the group S. A Sylow r-subgroup of the group S is cyclic; hence, all such elements are conjugate in S. As follows from the description of the centralizers of semisimple elements of groups of type B_n [24, Proposition 11], $C_S(\overline{x})$ has a subgroup $\overline{H} = \langle \overline{x}\rangle \times M$, where $M \simeq B_1(q)$.

Let $1 = Z_0(K) \leq Z_1(K) \leq \ldots \leq Z_s(K) = K$ be the upper central series of the group K. There exists $i \geqslant 0$ such that $Z_i(K) \cap C = 1$ and $Z_{i+1}(K) \cap C \neq 1$. Taking the quotient group of G modulo $Z_i(K)$, one can assume without loss of generality that $V := C \cap Z(K) \neq 1$. Note that V is an elementary abelian group, otherwise G would contain an element of order p^2r, which is impossible. The preimage H of the group $\overline{H}$ in G normalizes V and K centralizes V; hence, conjugation by elements of H induces the action of the group $\overline{H}$ on V.

Let $p>3$. The group M has a subgroup isomorphic to $B_1(p)$. For $p>3$, the group $B_1(p)$ is simple and, by Lemma 11, unisingular. Hence, the natural semidirect product VM contains an element of order $pr(p+1)/2$. By [23, Lemma 10], G also contains an element of this order. By the hypothesis, α is even; hence, $(q^{n-1}+1, p+1) = 2$. Since $(p+1)/2 > 2$, the group L has no elements of order $pr_{2n-2}(p+1)/2$, a contradiction.

Thus, $p=3$. Then, $q \geqslant 9$. If M does not centralize V, then $C_M(V) = 1$ because M is simple. Consider a subgroup F of the group M isomorphic to $B_1(3) \simeq Alt_4$. The group F is a Frobenius group with kernel of order 4 and complement of order 3. Assume that $\overline{y} \in F$ and $|\overline{y}| = 3$. By Lemma 3, the natural semidirect product $V\overline{H}$ contains an element of order 9. This means that there exists an element v in V such that $w = v^{\overline{y}^2}v^{\overline{y}}v \neq 1$. Let y be some preimage of the element $\overline{y}$ in H. The elements x and y commute modulo K; hence, xy and xyv are elements of order $3^l r$. In this case,

$$(xyv)^{3r} = (xy)^{3r} v^{(xy)^{3r-1}} v^{(xy)^{3r-2}} \ldots v = (xy)^{3r} v^{\overline{y}^{3r-1}} v^{\overline{y}^{3r-2}} \ldots v = (xy)^{3r} w^r;$$

therefore, xy and xyv cannot be of order $3r$ simultaneously. Consequently, there is an element of order $9r = 3^2 r_{2n-2}$ in G, which contradicts the fact that the number $3^2 r_{2n-2}$ is absent in $\omega(L)$. Thus, M centralizes V. Hence, G has an element of order $pr_{2n-2}(q-1)/2$. Since $(q^{n-1}+1, q-1) = 2$ and $(q-1)/2 > 2$, there are no elements of this order in L. The proposition is proved.

The assertion of Theorem 2 in the case when α is even follows from Propositions 1, 2, and 4.

The assertion of Theorem 3 follows from Propositions 1, 3, and 4.

ACKNOWLEDGMENTS

This work was supported by the Russian Foundation for Basic Research (project nos. 06-01-39001 and 08-01-00322), by the Presidium of the Siberian Branch of the Russian Academy of Sciences (integration project no. 2006.1.2), by the Council on Grants of the President of the

Russian Federation (project nos. NSh-344.2008.1, MD-2848.2007.1, and MK-377.2008.1), and by the Program of the Federal Education Agency "Development of the Scientific Potential of Higher Schools" (project no. 2.1.1/419). The fourth author was supported by the Russian Foundation for Basic Research (project no. 07-01-00148), by the Joint Competition of the Russian Foundation for Basic Research and the Belarusian Republican Foundation for Basic Research (project no. 08-01-90006), by the Division of Mathematical Sciences of the Russian Academy of Sciences, and by Programs of Joint Research of the Ural Division of the Russian Academy of Sciences with the Siberian Branch of the Russian Academy of Sciences and the Belarusian National Academy of Sciences.

REFERENCES

1. V. D. Mazurov, Izv. Ural'sk. Gos. Univ., Ser. Mat. Mekh. **36** (7), 119 (2005).
2. M. A. Grechkoseeva, W. J. Shi, and A. V. Vasil'ev, Front. Math. China **3** (2), 275 (2008).
3. A. S. Kondrat'ev, Sib. Mat. Zh. **48** (6), 1250 (2007).
4. O. A. Alekseeva and A. S. Kondrat'ev, Sib. Mat. Zh. **44** (2), 241 (2003).
5. V. D. Mazurov, Algebra i Logika **41** (2), 166 (2002).
6. A. V. Vasil'ev and M. A. Grechkoseeva, Sib. Mat. Zh. **45** (3), 510 (2004).
7. J. S. Williams, J. Algebra **69** (2), 487 (1981).
8. A. S. Kondrat'ev, Mat. Sb. **180** (6), 787 (1989).
9. A. S. Kondrat'ev and V. D. Mazurov, Sib. Mat. Zh. **41** (2), 359 (2000).
10. A. V. Vasil'ev, Sib. Mat. Zh. **46** (3), 511 (2005).
11. A. V. Vasil'ev and I. B. Gorshkov, Sib. Mat. Zh. **50** (2), 292 (2009).
12. V. D. Mazurov, Algebra i Logika **36** (1), 37 (1997).
13. A. V. Zavarnitsin, Preprint No. 48, IM SO RAN (Inst. of Mathematics, Siberian Branch of the Russian Academy of Sciences, 2000).
14. K. Zsigmondy, Monatsh. Math. Phys. **3**, 265 (1892).
15. A. V. Vasil'ev and M. A. Grechkoseeva, Algebra i Logika **47** (5), 558 (2008).
16. G. C. Gerono, Nouv. Ann. Math. (2) **9**, 469 (1870).
17. A. A. Buturlakin, Preprint, IM SO RAN (Inst. of Mathematics, Siberian Branch of the Russian Academy of Sciences, 2008).
18. A. A. Buturlakin and M. A. Grechkoseeva, Algebra i Logika **46** (2), 129 (2007).
19. A. V. Vasil'ev and E. P. Vdovin, Algebra i Logika **44** (6), 682 (2005).
20. R. M. Guralnick and P. H. Tiep, J. Group Theory **6** (3), 271 (2003).
21. D. Gorenstein, R. Lyons, and R. Solomon, *The Classification of the Finite Simple Groups* (Amer. Math. Soc., Providence, RI, 1998).
22. W. M. Kantor and A. Seress, J. Algebra **247** (3), 370 (2002).
23. A. V. Zavarnitsin and V. D. Mazurov, Algebra i Logika **38** (3), 296 (1999).
24. R. W. Carter, Proc. London Math. Soc. (3) **42** (1), 1 (1981).

Translated by E. Vasil'eva