Siberian Mathematical Journal, *Vol.* 45, *No.* 3, *pp.* 420–432, 2004

ON RECOGNITION OF THE FINITE SIMPLE ORTHOGONAL GROUPS OF DIMENSION 2^m, $2^m + 1$, AND $2^m + 2$ OVER A FIELD OF CHARACTERISTIC 2

A. V. Vasil′ev and M. A. Grechkoseeva

UDC 512.542

Abstract: The spectrum $\omega(G)$ of a finite group G is the set of element orders of G. A finite group G is said to be recognizable by spectrum (briefly, recognizable) if $H \simeq G$ for every finite group H such that $\omega(H) = \omega(G)$. We give two series, infinite by dimension, of finite simple classical groups recognizable by spectrum.

Keywords: recognition by spectrum, finite orthogonal group

Introduction

The *spectrum* $\omega(G)$ of a finite group G is the set of element orders of G. In other words, a natural number n is in $\omega(G)$ if and only if there is an element of order n in G. A finite group G is said to be *recognizable by spectrum* (briefly, *recognizable*) if $H \simeq G$ for every finite group H such that $\omega(H) = \omega(G)$. Since a finite group with a nontrivial normal soluble subgroup is not recognizable (see [1, Lemma 1]), each recognizable group is an extension of the direct product M of simple nonabelian groups by some subgroup of $\mathrm{Out}(M)$. So, of prime interest is the recognition problem for simple and almost simple groups (recall that G is almost simple if $S \leq G \leq \mathrm{Aut}(S)$ for some simple nonabelian group S). In the middle of the 1980s Shi found the first examples of recognizable finite simple groups (see [2, 3]). In 1994 Shi and Brandl obtained an infinite series of recognizable simple linear groups $L_2(q)$, $q \neq 9$ (see [4, 5]). The recognition (or nonrecognition) problem is solved at present for all groups with prime divisors at most 13 (see [6]) and several infinite series of recognizable finite simple and almost simple groups are obtained. The list of groups is available in [6] for which the recognition problem is solved. However, all examples of recognizable groups, except for alternating and symmetrical permutation groups, have dimensions bounded in a certain sense. Let us put it more precisely. In view of the classification theorem all finite simple nonabelian groups except for alternating permutation groups and 26 sporadic groups are groups of Lie type. The Lie rank of every finite group with the recognition problem solved is at most 6 if the group is twisted and at most 5 otherwise. In particular, the dimension of every known recognizable classical group, i.e., a group with natural matrix representation, is at most 10. The main purpose of this paper is to give two series, infinite by dimension, of finite simple groups recognizable by spectrum; namely, the series of orthogonal groups $O_{2^m+1}(2)$ and $O^-_{2^m+2}(2)$. Since the proof of this result rests mainly on the description of these groups as those of Lie type, we will use the notation of groups of Lie type.

Theorem 1. *For every natural number $m > 2$ the groups $C_{2^m}(2)$ and ${}^2D_{2^m+1}(2)$ are recognizable by spectrum.*

Remark 1. The following isomorphisms are available:

$$C_{2^m}(2^k) \simeq S_{2^{m+1}}(2^k) \simeq O_{2\cdot 2^m+1}(2^k), \quad {}^2D_{2^m+1}(q) \simeq O^-_{2(2^m+1)}(q).$$

The authors were supported by the Russian Foundation for Basic Research (Grants 02–01–00495; 02–01–39005), the State Maintenance Program for the Leading Scientific Schools of the Russian Federation (Grant NSh–2069.2003.1), the Siberian Division of the Russian Academy of Sciences (a grant of the Young Scientists Competition, Resolution No. 404 of 06.12.2002), and the Program "Universities of Russia" (Grant UR.04.01.031).

Novosibirsk. Translated from *Sibirskiĭ Matematicheskiĭ Zhurnal*, Vol. 45, No. 3, pp. 510–526, May–June, 2004. Original article submitted December 29, 2003.

 0037-4466/04/4503–0420

REMARK 2. Recognizability of ${}^2D_5(2)$ is proved in [7]. Nonrecognizability of $C_2(2) \simeq S_4(2)$ and ${}^2D_3(2) \simeq U_4(2)$ is obtained in [8, 9] respectively. The group $C_4(2)$ is not recognizable since its spectrum is equal to that of the natural extension of ${}^2D_4(2)$ by an outer automorphism of order 2. The last fact can be easily checked by using [10]. Thus, modulo Theorem 1, the recognition problem for the groups $C_{2^m}(2)$ and ${}^2D_{2^m+1}(2)$ is completely solved for all natural m.

A proof of recognizability usually includes two principal steps. The first is to prove that a group H whose spectrum equals that of the group G under study contains a composition factor isomorphic to G. The second consists in establishing that H coincides with this factor; i.e., H is isomorphic to G. Since the result of the first step itself is of great import and, moreover, the corresponding assertion can be often obtained for a wider class of groups; it is reasonable to state this result as an especial theorem. To formulate it, we will use a convenient term that was recently introduced in [11]. A finite simple nonabelian group G is said to be *quasirecognizable* if every finite group H with $\omega(H) = \omega(G)$ contains a composition factor that is isomorphic to G.

Theorem 2. *Let m and k be arbitrary natural numbers. A group G is quasirecognizable in each of the following cases:*

(a) $G = {}^2D_{2^m}(2^k)$;

(b) $G = {}^2D_{2^m+1}(2)$ *and* $m \neq 1$;

(c) $G = C_{2^m}(2^k)$ *and* $m > 2$.

REMARK 1. The fact that ${}^2D_3(2) \simeq U_4(2)$ is not quasirecognizable follows from the proof of Proposition 6 in [9]. The similar fact about $C_2(2^k)$ follows from Proposition 1 in [6]. The group $C_4(2)$ is not quasirecognizable by the argument in Remark 2 on Theorem 1. The quasirecognition problem for $C_4(2^k)$ remains open for $k > 1$. Finally, since recognizability of $G = {}^2D_2(2^k) \simeq A_1(2^{2k})$ was established by Brandl and Shi, we may assume that $m > 1$ while proving the theorem.

REMARK 2. Observe that all known quasirecognizable groups of Lie type have bounded Lie ranks in much the same way as recognizable groups.

§ 1. Preliminaries

The set $\omega(H)$ of a finite group H is closed under divisibility and uniquely determined by the set $\mu(H)$ of those elements in $\omega(H)$ that are maximal under the divisibility relation. Moreover, $\omega(H)$ determines the Gruenberg–Kegel graph $GK(H)$ whose vertices are all prime divisors of the order of H, and two primes p and q are adjacent if H has an element of order $p \cdot q$. Denote by $s(H)$ the number of connected components of $GK(H)$ and by $\pi_i(H)$, $i = 1, \ldots, s(H)$, the ith connected component of $GK(H)$. Given a group H of even order, put $2 \in \pi_1(H)$. Denote by $\mu_i(H)$ ($\omega_i(H)$) the set of numbers $n \in \mu(H)$ ($n \in \omega(H)$) such that every prime divisor of n belongs to π_i.

Lemma 1.1 (Gruenberg–Kegel). *If H is a finite group with disconnected graph $GK(H)$ then one of the following holds:*

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

(b) $s(H) = 2$ *and $H = ABC$, where A and AB are normal subgroups of H; AB and BC are Frobenius groups with kernels A and B and complements B and C respectively;*

(c) *there exists a simple nonabelian group S such that $S \leq \overline{H} = H/K \leq \mathrm{Aut}(S)$ for some nilpotent normal $\pi_1(H)$-subgroup K of H and the group $\overline{H}/S$ is a $\pi_1(H)$-subgroup; moreover, the graph $GK(S)$ is disconnected, $s(S) \geq s(H)$ and for every i, $2 \leq i \leq s(H)$, there is j, $2 \leq j \leq s(S)$, such that $\omega_i(H) = \omega_j(S)$.*

PROOF. See [12].

Lemma 1.2. *Let S be a finite simple group with the disconnected graph $GK(S)$. Then $|\mu_i(S)| = 1$ for $2 \leq i \leq s(S)$. Denote by $n_i = n_i(S)$ the only element of $\mu_i(S)$, $i \geq 2$. Then S, $\pi_1(S)$, and $n_i(S)$, $2 \leq i \leq s(S)$, are as indicated in Tables* 1a–1c.

PROOF. See [13, Lemma 2].

Table 1a. Finite simple groups S with $s(S) = 2$

S	Restrictions on S	$\pi_1(S)$	n_2
A_n	$6 < n = p, p+1, p+2$; not both n and $n-2$ are primes	$\pi((n-3)!)$	p
$A_{p-1}(q)$	$(p,q) \neq (3,2),(3,4)$	$\pi(q\prod_{i=1}^{p-1}(q^i-1))$	$\frac{q^p-1}{(q-1)(p,q-1)}$
$A_p(q)$	$(q-1)\|(p+1)$	$\pi(q(q^{p+1}-1)\prod_{i=1}^{p-1}(q^i-1))$	$\frac{q^p-1}{q-1}$
${}^2A_{p-1}(q)$		$\pi(q\prod_{i=1}^{p-1}(q^i-(-1)^i))$	$\frac{q^p+1}{(q+1)(p,q+1)}$
${}^2A_p(q)$	$(q+1)\|(p+1)$, $(p,q) \neq (3,3),(5,2)$	$\pi(q(q^{p+1}-1)\prod_{i=1}^{p-1}(q^i-(-1)^i))$	$\frac{q^p+1}{q+1}$
${}^2A_3(2)$		$\{2,3\}$	5
$B_n(q)$	$n = 2^m \geq 4$, q odd	$\pi(q\prod_{i=1}^{n-1}(q^{2i}-1))$	$(q^n+1)/2$
$B_p(3)$		$\pi(3(3^p+1)\prod_{i=1}^{p-1}(3^{2i}-1))$	$(3^p-1)/2$
$C_n(q)$	$n = 2^m \geq 2$	$\pi(q\prod_{i=1}^{n-1}(q^{2i}-1))$	$\frac{q^n+1}{(2,q-1)}$
$C_p(q)$	$q = 2,3$	$\pi(q(q^p+1)\prod_{i=1}^{p-1}(q^{2i}-1))$	$\frac{q^p-1}{(2,q-1)}$
$D_p(q)$	$p \geq 5$, $q = 2,3,5$	$\pi(q\prod_{i=1}^{p-1}(q^{2i}-1))$	$\frac{q^p-1}{(q-1)}$
$D_{p+1}(q)$	$q = 2,3$	$\pi(q(q^p+1)\prod_{i=1}^{p-1}(q^{2i}-1))$	$\frac{q^p-1}{(2,q-1)}$
${}^2D_n(q)$	$n = 2^m \geq 4$	$\pi(q\prod_{i=1}^{n-1}(q^{2i}-1))$	$\frac{q^n+1}{(2,q+1)}$
${}^2D_n(2)$	$n = 2^m+1 \geq 5$	$\pi(2(2^n+1)\prod_{i=1}^{n-2}(2^{2i}-1))$	$2^{n-1}+1$
${}^2D_p(3)$	$5 \leq p \neq 2^m+1$	$\pi(3\prod_{i=1}^{p-1}(3^{2i}-1))$	$(3^p+1)/4$
${}^2D_n(3)$	$9 \leq n = 2^m+1 \neq p$	$\pi(3(3^n+1)\prod_{i=1}^{n-2}(3^{2i}-1))$	$(3^{n-1}+1)/2$
$G_2(q)$	$2 < q \equiv \varepsilon(3)$, $\varepsilon = \pm 1$	$\pi(q(q^2-1)(q^3-\varepsilon))$	$q^2-\varepsilon q+1$
${}^3D_4(q)$		$\pi(q(q^6-1))$	q^4-q^2+1
$F_4(q)$	q odd	$\pi(q(q^6-1)(q^8-1))$	q^4-q^2+1
${}^2F_4(2)'$		$\{2,3,5\}$	13
$E_6(q)$		$\pi(q(q^5-1)(q^8-1)(q^{12}-1))$	$\frac{q^6+q^3+1}{(3,q-1)}$
${}^2E_6(q)$	$q > 2$	$\pi(q(q^5+1)(q^8-1)(q^{12}-1))$	$\frac{q^6-q^3+1}{(3,q+1)}$
M_{12}		$\{2,3,5\}$	11
J_2		$\{2,3,5\}$	7
Ru		$\{2,3,5,7,13\}$	29
He		$\{2,3,5,7\}$	17
McL		$\{2,3,5,7\}$	11
Co_1		$\{2,3,5,7,11,13\}$	23
Co_3		$\{2,3,5,7,11\}$	23
Fi_{22}		$\{2,3,5,7,11\}$	13
HN		$\{2,3,5,7,11\}$	19

Table 1b. Finite simple groups S with $s(S) = 3$

S	Restrictions on S	$\pi_1(S)$	n_2	n_3
A_n	$n > 6$, $n = p$	$\pi((n-3)!)$	p	$p-2$
	$p-2$ is a prime			
$A_1(q)$	$3 < q \equiv \varepsilon(4)$, $\varepsilon = \pm 1$	$\pi(q-\varepsilon)$	$\pi(q)$	$(q+\varepsilon)/2$
$A_1(q)$	$q > 2$, q even	$\{2\}$	$q-1$	$q+1$
${}^2A_5(2)$		$\{2,3,5\}$	7	11
${}^2D_p(3)$	$p = 2^m + 1$	$\pi(3(3^{p-1}-1)\prod_{i=1}^{p-2}(3^{2i}-1))$	$\frac{3^{p-1}+1}{2}$	$(3^p+1)/4$
$G_2(q)$	$q \equiv 0(3)$	$\pi(q(q^2-1))$	q^2-q+1	q^2+q+1
${}^2G_2(q)$	$q = 3^{2m+1} > 3$	$\pi(q(q^2-1))$	$q-\sqrt{3q}+1$	$q+\sqrt{3q}+1$
$F_4(q)$	q even	$\pi(q(q^4-1)(q^6-1))$	q^4+1	q^4-q^2+1
${}^2F_4(q)$	$q = 2^{2m+1} > 2$	$\pi(q(q^3+1)(q^4-1))$	$q^2-\sqrt{2q^3}+$	$q^2+\sqrt{2q^3}+$
			$+q-\sqrt{2q}+1$	$+q+\sqrt{2q}+1$
$E_7(2)$		$\{2,3,5,7,11,13,17,19,31,43\}$	73	127
$E_7(3)$		$\{2,3,5,7,11,13,19,$	757	1093
		$37,41,61,73,547\}$		
M_{11}		$\{2,3\}$	5	11
M_{23}		$\{2,3,5,7\}$	11	23
M_{24}		$\{2,3,5,7\}$	11	23
J_3		$\{2,3,5\}$	17	19
HiS		$\{2,3,5\}$	7	11
Suz		$\{2,3,5,7\}$	11	13
Co_2		$\{2,3,5,7\}$	11	23
Fi_{23}		$\{2,3,5,7,11,13\}$	17	23
F_3		$\{2,3,5,7,13\}$	19	31
F_2		$\{2,3,5,7,11,13,17,19,23\}$	31	47

Lemma 1.3. *Let H be a finite group, and let K be a normal nilpotent subgroup of H with $H/K \simeq S$ and $R \leq S$. Assume that for some prime p a Sylow p-subgroup V of K is an elementary abelian p-subgroup and denote the natural semidirect product $V \leftthreetimes R$ by M. Then $\omega(M) \subseteq \omega(H)$.*

Proof. Since $V \subseteq Z(K)$, the action of R on V is defined correctly. If $v \in V$, $r \in R \leq S$ and $\bar{r}$ is the coset of H in K corresponding to r then $v^r = v^h$ for all $h \in \bar{r}$.

Suppose that $g \in M$ and $|g| \notin \omega(H)$. Then $g = r \cdot v$, where $r \in R$, $v \in V$. If $|r| = m$ then $g^m = r^m v^{r^{m-1}} \dots v^r v \in V$. Therefore the order of g is equal to mp, and $mp \notin \omega(H)$. Consider the coset $\bar{r}$. Each $h \in \bar{r}$ has order mt for some t. If $(t,p) = p$ then $mp \in \omega(H)$, hence $(t,p) = 1$. Denote by N the least common multiple of the element of $\{|h|, h \in \bar{r}\}$. Then N is divisible by m and not divisible by mp. For each $h \in \bar{r}$, $k \in K$ we have $hk \in \bar{r}$. Therefore,

$$1 = (hk)^N = h^N k^{h^{N-1}} \dots k^h k = k^{h^{N-1}} \dots k^h k.$$

Since $V \subseteq K$, for every $v \in V$ we have $v^{h^{N-1}} \dots v^h v = 1$ if $h \in \overline{r}$. On the other hand, $v^h = v^r$. Hence,

$$g^N = (r \cdot v)^N = r^N v^{r^{N-1}} \dots v^r v = v^{h^{N-1}} \dots v^h v = 1.$$

But N does not divide the order of g; a contradiction. The lemma is proved.

Table 1c. Finite simple groups S with $s(S) > 3$

$s(S)$	S	Restrictions on S	$\pi_1(S)$	n_2	n_3	n_4	n_5	n_6
4	$A_2(4)$		$\{2\}$	3	5	7		
	${}^2B_2(q)$	$q = 2^{2m+1} > 2$	$\{2\}$	$q-1$	$q-\sqrt{2q}+1$	$q+\sqrt{2q}+1$		
	${}^2E_6(2)$		$\{2,3,5,7,11\}$	13	17	19		
	$E_8(q)$	$q \equiv 2,3(5)$	$\pi(q(q^8-1)$	$\frac{q^{10}-q^5+1}{q^2-q+1}$	$\frac{q^{10}+q^5+1}{q^2+q+1}$	q^8-q^4+1		
			$(q^{12}-1)$					
			$(q^{14}-1)$					
			$(q^{18}-1)$					
			$(q^{20}-1))$					
	M_{22}		$\{2,3\}$	5	7	11		
	J_1		$\{2,3,5\}$	7	11	19		
	$O'N$		$\{2,3,5,7\}$	11	19	31		
	LyS		$\{2,3,5,7,11\}$	31	37	67		
	Fi'_{24}		$\{2,3,5,7,11,13\}$	17	23	29		
	F_1		$\{2,3,5,7,11,13,17,$	41	59	71		
			$19,23,29,31,47\}$					
5	$E_8(q)$	$q \not\equiv 2,3(5)$	$\pi(q(q^8-1)$	$\frac{q^{10}-q^5+1}{q^2-q+1}$	$\frac{q^{10}+q^5+1}{q^2+q+1}$	q^8-q^4+1	$\frac{q^{10}+1}{q^2+1}$	
			$(q^{10}-1)$					
			$(q^{12}-1)$					
			$(q^{14}-1)$					
			$(q^{18}-1))$					
6	J_4		$\{2,3,5,7,11\}$	23	29	31	37	43

Lemma 1.4. *Let H be a finite group, and let $K \lhd H$ and H/K be a Frobenius group with kernel F and cyclic complement C. If $(|F|,|K|) = 1$ and F does not lie in $KC_H(K)/K$ then $p|C| \in \omega(H)$ for some prime divisor p of $|K|$.*

Proof. See [14, Lemma 1].

Lemma 1.5 (Zsigmondy). *Let q be a prime and let s be a natural, $s \geq 2$. Then one of the following holds:*

(a) *there exists a prime p such that p divides $q^s - 1$ and p does not divide $q^t - 1$ for all natural $t < s$;*
(b) *$s = 6$ and $q = 2$;*
(c) *$s = 2$ and $q = 2^t - 1$ for some natural t.*

Proof. See [15].

A prime p satisfying condition (a) of Lemma 1.5 is called a *primitive* prime divisor of $q^s - 1$.

Lemma 1.6. *Let $r = q^l$ be a power of a prime q and s be a natural number, $s \geq 2$. Then the following hold:*

(a) *if s is odd then a primitive prime divisor of $r^s - 1$ does not divide $r^t + 1$ for all natural $t < s$;*
(b) *if $(r,s) \neq (2,3)$ then there exists a prime p such that p divides $r^s + 1$ and p does not divide $r^t - 1$ and $r^t + 1$ for all natural $t < s$ (by analogy with the previous definition we will call this prime p a primitive prime divisor of $r^s + 1$);*
(c) *if p is a primitive prime divisor of $r^s - \varepsilon$, $\varepsilon = \pm 1$, then p does not divide l.*

PROOF. (a) Let p be a primitive prime divisor of r^s-1. Suppose that p divides r^t+1 for some $t<s$. Then p divides the greatest common divisor of r^s-1 and $r^{2t}-1$ that equal to $r^{(s,2t)}-1$. Since s is odd, we have $(s,2t)=(s,t)<s$; a contradiction with the choice of p.

(b) Let p be a primitive prime divisor of $r^{2s}-1$. Then p does not divide r^s-1, therefore p divides r^s+1. Moreover, p does not divide $r^{2t}-1$ for all $t<s$.

(c) Suppose that p divides l and let $l=tp$. By hypothesis, p divides $r^s-\varepsilon=q^{ls}-\varepsilon=q^{tps}-\varepsilon$. On the other hand, p divides $q^{tps}-q^{ts}$ by Fermat's Little Theorem. Hence p divides $q^{ts}-\varepsilon$; this contradicts the primitivity of p.

Lemma 1.7. *Let l and s be natural numbers. Then the following hold:*
(a) $2^{3^{l-1}}+1$ *is divisible by* 3^l *and not divisible by* 3^{l+1}*;*
(b) *if* 2^s+1 *or* 2^s-1 *is divisible by* 3^l *then* $s\geq 3^{l-1}$.

PROOF. (a) We proceed by induction. The claim is true for $l=1$. Assume that it is true for all natural numbers smaller than $l+1$ and consider the number

$$2^{3^l}+1=(2^{3^{l-1}}+1)(2^{2\cdot 3^{l-1}}-2^{3^{l-1}}+1).$$

An expression in the first parentheses is divisible by 3^l and not divisible by 3^{l+1}; an expression in the second is divisible by 3 and not divisible by 9. Therefore, the whole expression is divisible by 3^{l+1} and not divisible by 3^{l+2}.

(b) Suppose that $s<3^{l-1}$. By hypothesis, $2^{2s}-1$ is divisible by 3^l. Thus the greatest common divisor of $2^{2\cdot 3^{l-1}}-1$ and $2^{2s}-1$ equal to $2^{2(s,3^{l-1})}-1=2^{2\cdot 3^t}-1$, where $t<l-1$, is divisible by 3^l as well. Therefore, $2^{3^t}+1$ is divisible by 3^l; this contradicts item (a) of the lemma.

§ 2. Properties of $C_n(q)$ and ${}^2D_n(q)$

Lemma 2.1. *Let T be a maximal torus in $C_n(q)$ or ${}^2D_n(q)$. Then the order of T is given by*

$$|T|=\prod_{j=1}^{t}(q^{t_j}-1)\prod_{i=1}^{s}(q^{s_i}+1),$$

where natural numbers s_i and t_j satisfy

$$\sum_{j=1}^{t}t_j+\sum_{i=1}^{s}s_i=n \tag{1}$$

and in the case of ${}^2D_n(q)$ a number s is odd.

Conversely, if natural numbers t_j, s_i, $1\leq j\leq t$, $1\leq i\leq s$, satisfy (1)*, then $C_n(q)$ contains a torus of the corresponding order. If, in addition, s is odd then ${}^2D_n(q)$ contains such torus as well.*

PROOF. See [16, Part E, Chapter II, § 1, Theorem 1.7 (b) and Part G, Items 15 and 16].

Lemma 2.2. *Let $n\geq 4$, $q=2^k\geq 2$ and let p be an odd prime. Then the following hold:*
(a) *if $n=2^m$ and $G=C_n(q)$, ${}^2D_n(q)$, or ${}^2D_{n+1}(q)$, then $4n\notin\omega(G)$;*
(b) *if n is even and $p(q^{n-1}-1)\in\omega(C_n(q))$ then p divides $q+1$ or $q-1$;*
(c) *if $3^l<n<3^{l+1}$ then $3^{l+2}\notin\omega(C_n(2))$.*

PROOF. (a) Since ${}^2D_n(2^k)<C_n(2^k)<{}^2D_{n+1}(2^k)<D_{n+1}(2^{2k})$, it suffices to prove that $4n\notin\omega(D_{n+1}(2^{2k}))$. A Sylow 2-subgroup U of $D_{n+1}(2^{2k})$ is generated by elements of order 2. Hence, if $U^{(l)}$ is the lth derived group of U and u is an arbitrary element of U then $u^{2^l}\in U^{(l)}$. By [17, Theorem 5.3.3] the class of U is equal to $2n-1=2^{m+1}-1$. Therefore, $U^{(m+1)}=1$ and there is no an element of order $2^{m+2}=4n$ in U.

(b) Let T be a maximal torus of $C_n(q)$ containing an element of order $p(q^{n-1}-1)$. By Lemma 2.1 the order of T is equal to $\prod_{j=1}^{t}(q^{t_j}-1)\prod_{i=1}^{s}(q^{s_i}+1)$, where $\sum_{j=1}^{t} t_j + \sum_{i=1}^{s} s_i$ is equal to n. Let p' be a primitive prime divisor of $q^{n-1}-1$. The number $n-1$ is odd, therefore, if $s_i < n-1$ and $t_i < n-1$ then p' does not divide the order of T by Lemma 1.6(a). Moreover, if $s_i = n, n-1$ then $(q^{n-1}-1, q^{s_i}+1) = 1$; if $t_j = n$ then $(q^{n-1}-1, q^{t_j}-1) = q-1$. Thus, $t_1 = n-1$ and $t_2 = 1$, or $t_1 = n-1$ and $s_1 = 1$. Hence the order of T is equal to $(q^{n-1}-1)(q-1)$ or $(q^{n-1}-1)(q+1)$. From this the conclusion of (b) follows at once.

(c) Suppose that there is an element of order 3^{l+2} in the group $C_n(2)$ and let T be a maximal torus containing this element. From results of Parts E and G in [16] it follows that $T \simeq T_1 \times T_2 \times \cdots \times T_s$, where $|T_i| = 2^{s_i} + \varepsilon_i$, $s_i \leq n$, $\varepsilon_i = \pm 1$, $1 \leq i \leq s$. Therefore there is a number i, $1 \leq i \leq s$, such that $3^{l+2} \in \omega(T_i)$ and hence $2^{s_i} + \varepsilon_i$ is divisible by 3^{l+2}. Lemma 1.7(b) implies that $s_i \geq 3^{l+1} > n$; a contradiction.

Lemma 2.3. *The group $A_n(q)$, $n \geq 4$, $q \geq 2$, contains a Frobenius subgroup with kernel of order q^n and cyclic complement of order $q^n - 1$.*

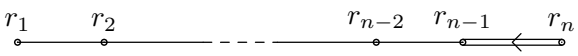
Proof. See [18, Lemma 3].

The group $C_n(2)$ contains a subgroup isomorphic to $A_{n-1}(2)$. Thus, by Lemma 2.3 we have

Corollary. *The group $C_n(2)$, $n \geq 5$, contains a Frobenius group with kernel of order 2^{n-1} and cyclic complement of order $2^{n-1} - 1$.*

We need some definitions and notations related to the groups of Lie type, first of all to $C_n(2)$. See [17] for details.

Let Φ be a root system, Φ^+ be a positive system and $\Pi = \{r_1, r_2, \ldots, r_n\}$ be a fundamental system of the algebra C_n, and let Dynkin diagram be as below:



Denote by Π_i the subset $\Pi \setminus \{r_i\}$ of the fundamental system; by Φ_i, the set of those roots that are integral combinations of roots in Π_i; and by Φ_i^+, the set $\Phi_i \cap \Phi^+$.

Let W be the Weyl group of Φ and w_r be the reflection in the hyperplane orthogonal to the root r. For simplicity we will denote by w_i the reflection w_{r_i} corresponding to the fundamental root r_i.

The group $G = C_n(2)$ is generated by the root subgroups X_r for all $r \in \Phi$. The order of every root subgroup X_r is 2. Denote by x_r the only nontrivial element of X_r.

Let $n_r = x_r x_{-r} x_r$, where $r \in \Phi$. The subgroup $N = \langle n_r \mid r \in \Phi \rangle$, the monomial subgroup of G, is isomorphic to the Weyl group. Moreover, under a suitable isomorphism the element n_r maps into the element w_r. We will thus identify N with W.

Lemma 2.4. *Let $n = 2^m \geq 2$. Then $G = C_n(2)$ contains a Frobenius subgroup with kernel of order $2^n + 1$ and cyclic complement of order $2n$.*

Proof. There is a maximal torus T of order $2^n + 1$ in G. The set $\pi(T)$ constitutes the connected component $\pi_2(G)$ of $GK(G)$, therefore, the normalizer $N_G(T)$ of T in G is a Frobenius group with complement T. The factor-group $N_G(T)/T$ is isomorphic to the centralizer of a Coxeter element $w_0 = w_1 w_2 \ldots w_n$ in the Weyl group (see [16, Parts E and G]). Therefore it contains an element having the same order as the element w_0 has. The order of the element w_0 is $2n$ (see, for instance, [17, Theorem 10.5.3]), and the lemma is proved.

The group ${}^2D_{n+1}(2)$ contains a subgroup isomorphic to $C_n(2)$. By Lemma 2.4 we have

Corollary. *Let $n = 2^m \geq 4$. Then ${}^2D_{n+1}(2)$ contains a Frobenius subgroup with kernel of order $2^n + 1$ and cyclic complement of order $2n$.*

Lemma 2.5. *Let $n = 3^l + 1$. Then $G = C_n(2)$ contains a Frobenius subgroup with kernel of order $2^{2\cdot 3^l}$ and cyclic complement of order 3^{l+1}.*

Proof. Consider a parabolic subgroup P_1 of G associated with the set Π_1 of fundamental roots. By the Levi decomposition [17, Theorem 8.5.2] the group P_1 equals $U_1 : L_1$, where $U_1 = \langle X_r \mid r \in \Phi^+ \setminus \Phi_1\rangle$ and $L_1 = \langle X_r \mid r \in \Phi_1\rangle$.

The order of the group U_1 equals 2^{2n-1}. It is proved in [19] that U_1 is an elementary abelian 2-group. The element $x = w_2 w_3 \dots w_{n-1} x_{r_n} x_{-r_n} \in L_1$ acts on U_1 by conjugation. This action is determined by the action of elements w_2, $w_3, \dots, w_{n-1}$, x_{r_n}, x_{-r_n} on the generators of U_1. Put $a = r_1 + r_2 + \dots + r_{n-1}$, $b = r_1 + r_2 + \dots + r_n$, and $c = 2(r_1 + r_2 + \dots + r_{n-1}) + r_n$. Then

$$x_r^{w_i} = x_{w_i(r)}, \quad r \in \Phi,$$
$$x_{r_n} x_r x_{r_n} = x_r, \quad r \in \Phi^+ \setminus (\Phi_1 \cup \{a\}),$$
$$x_{-r_n} x_r x_{-r_n} = x_r, \quad r \in \Phi^+ \setminus (\Phi_1 \cup \{b\}),$$
$$x_{r_n} x_a x_{r_n} = x_{-r_n} x_b x_{-r_n} = x_a x_b x_c.$$

These formulae provide the following action pattern for x:

$$x_a \xrightarrow{x} x_{a-r_{n-1}} \xrightarrow{x} x_{a-r_{n-1}-r_{n-2}} \xrightarrow{x} \dots \xrightarrow{x} x_{r_1} \xrightarrow{x} x_b,$$
$$x_b \xrightarrow{x} x_{b+r_{n-1}} \xrightarrow{x} x_{b+r_{n-1}+r_{n-2}} \xrightarrow{x} \dots \xrightarrow{x} x_{c-r_1} \xrightarrow{x} x_a x_b x_c,$$
$$x_c \xrightarrow{x} x_c.$$

Put

$$v_1 = x_a x_c, \quad v_2 = x_{a-r_{n-1}} x_c, \dots, v_{n-1} = x_{r_1} x_c,$$
$$v_n = x_b x_c, \quad v_{n+1} = x_{b+r_{n-1}} x_c, \dots, v_{2n-2} = x_{c-r_1} x_c.$$

The element x normalizes the group $U_1' = \langle v_1, v_2, \dots, v_{2n-2}\rangle$. Identify the group U_1' with a vector space V over the field of order 2. The elements $v_1, v_2, \dots, v_{2n-2}$ are a basis for V. Above identification implies a natural homomorphism of the group $\langle x\rangle$ to the group $GL_{2n-2}(2)$ of all $2n-2 \times 2n-2$ nonsingular matrices over the field of order 2. This homomorphism sends the element x to the matrix

$$X = \begin{bmatrix} 0_{2n-3,1} & E_{2n-3} \\ E_1 & v \end{bmatrix},$$

where E_k is the $k \times k$ identity matrix, $0_{k_1,k_2}$ is the $k_1 \times k_2$ null matrix, and v is a row of length $2n-3$ whose $(n-1)$th entry is 1 and the others are all 0.

It is easy to obtain that

$$X^k = \begin{bmatrix} 0_{2n-2-k,k} & E_{2n-2-k} \\ E_k & Y \end{bmatrix}, \quad \text{where} \quad Y = \begin{bmatrix} 0_{k,n-k-1} & E_k & 0_{k,n-k-1} \end{bmatrix}.$$

Hence

$$X^{n-1} = \begin{bmatrix} 0_{n-1,n-1} & E_{n-1} \\ E_{n-1} & E_{n-1} \end{bmatrix} \quad \text{and} \quad X^{3(n-1)} = E_{2n-2}.$$

Since $n-1 = 3^l$, X acts regularly on V if X^{n-1} does. The latter is true because $\det(X^{n-1} + E_{2n-2}) = 1$.

The order of x is divisible by $|X| = 3^{l+1}$ and is not divisible by 3^{l+2} by Lemma 2.2(c). Therefore, $|x| = 3^{l+1}t$, where $(t,3) = 1$. The element x^t is of order 3^{l+1} and, moreover, acts regularly on U_1', since its image X^t acts regularly on V. Thus, $U_1' \cdot \langle x^t\rangle$ is a desired Frobenius group.

Lemma 2.6. *Let $n = 2^m \geq 4$. Then $G = {}^2D_{n+1}(2)$ contains a Frobenius subgroup with kernel of order 2^{2n} and cyclic complement of order $2^n + 1$.*

Proof. In [19] some description is found for the parabolic subgroup P_1^1 of G. Namely, $P_1^1 = U_1^1 : L_1^1$, where U_1^1 is an elementary abelian 2-group of order 2^{2n} and the group L_1^1 is isomorphic to ${}^2D_n(2)$. The group L_1^1 acts on U_1^1 by conjugation and contains an element y of order $2^n + 1$. This element acts regularly, since prime divisors of $2^n + 1$ constitute the connected component $\pi_2(G)$. Thus, $U_1 \cdot \langle y\rangle$ is a desired Frobenius group.

§ 3. Proof of Theorem 2

Let k and m be natural numbers, $m \geq 2$, and let $n = 2^m$, $r = 2^k$. Throughout this section, except for specially mentioned cases, G will denote one of the groups ${}^2D_n(r)$, $C_n(r)$, or ${}^2D_{n+1}(2)$. In the last case we assume that $r = 2$, $k = 1$.

Let H be a finite group with $\omega(H) = \omega(G)$. By Table 1a we then have $s(H) = s(G) = 2$ and $n_2(H) = n_2(G) = r^n + 1$.

Since $s(H) > 1$, there are three possibilities for the group H corresponding to items (a)–(c) of Lemma 1.1. The results of [20] imply that condition (c) holds for H. Thus, $H = K \cdot S_1$, where $S \leq S_1 \leq \mathrm{Aut}(S)$ for some simple nonabelian group S. Moreover, $\omega(S) \subseteq \omega(H)$, $s(S) \geq 2$, and there is i, $2 \leq i \leq s(S)$, such that $n_i(S) = n_2(H) = r^n + 1$.

We claim that $S \simeq G$. Consider each group in Tables 1a–1c. In these tables p denotes an odd prime and q denotes the order of the field related to a group. The orders and automorphism groups of the groups under consideration can be found in [10]. We will first assume that n is sufficiently large. The cases of small dimensions, remaining unproved, will be considered specially at the end of this section.

It is easy to verify that S coincides with none of the groups listed in the tables individually. Show that S is not an alternating group A_l with $l > 6$ either.

If $S = A_l$, where $l = p, p+1, p+2$ and at least one of the members l and $l-2$ is not prime; then $s(S) = 2$ and $n_2(S) = p$. Since $n_2(S) = n_2(H)$, we have $p = r^n + 1$. The groups A_{r^n+1}, A_{r^n+2}, and A_{r^n+3} contain a product of two independent cycles of length $r^n/2$, i.e., an element of order $r^n/2 = 2^{kn-1}$. By Lemma 2.2(a) the set $\omega(G)$ does not contain $4n$, therefore $2n \geq r^n/2 \geq 2^{n-1}$. This contradicts to the fact that $2n < 2^{n-1}$ for $n > 4$.

If $S = A_p$ and $p - 2$ is prime then $s(S) = 3$ and $n_2(S) = p$, $n_3(S) = p - 2$. If $n_2(H) = n_2(S)$ then $r^n + 1 = p$ and $p - 2$ is not prime. If $n_2(H) = n_3(S)$ then $r^n + 1 = p - 2$, $S = A_{r^n+3}$, and this case is already considered.

Now we may assume that S is a group of Lie type over the field of order q. Then suppose that S and i, $1 < i \leq s(S)$, are such that the number $n_i(S)$ can be represented as $q^l f(q) + 1$, where $f(x)$ is some polynomial with integer coefficients and $(q, f(q)) = 1$. If $f(q) \neq 1$ then $q^l f(q) \neq r^n$ and hence $n_i(S) \neq n_2(H)$. Thus it suffices to consider the groups S to which the above argument is inapplicable.

Suppose $S = A_{p-1}(q)$, where $(p, q) \neq (3, 2), (3, 4)$ and p divides $q - 1$, or $S = {}^2A_{p-1}(q)$, where p divides $q + 1$. Then $s(S) = 2$ and $n_2(S) = (q^p - \varepsilon)/p(q - \varepsilon)$, where $\varepsilon = 1$ in the first case and $\varepsilon = -1$ in the second. Since $n_2(H) = n_2(S)$, we have $r^n + 1 = (q^p - \varepsilon)/p(q - \varepsilon)$ and $p(q - \varepsilon)(r^n + 1) = q^p - \varepsilon$. Let $q - \varepsilon = pt$. Then $p^2 t(r^n + 1) = (pt + \varepsilon)^p - \varepsilon = p^3 ts + p^2 t$, where s is some natural number. Dividing it by $p^2 t$, obtain $r^n + 1 = ps + 1$ and $2^{kn} = r^n = ps$, which is impossible.

Let S be equal to $B_{n'}(q)$, ${}^2D_{n'}(q)$, or $C_{n'}(q)$, where q is odd, $n' = 2^{m'}$, $n' \geq 4$ in the first and second cases and $n' \geq 2$ in the last case. Then $s(S) = 2$ and $n_2(S) = (q^{n'} + 1)/2$. Since $n_2(S) = n_2(H)$, we have $q^{n'} = 2r^n + 1 \equiv 0\,(3)$, therefore $q = 3^l$ and $3^{ln'} = 2^{kn+1} + 1$. The last equation has only two solutions: $nk + 1 = 1$ and $nk + 1 = 3$, which is false for $n > 2$.

If $S = B_p(3)$, $C_p(3)$, or $D_{p+1}(3)$ then $n_2(S) = (3^p - 1)/2$. It follows from $n_2(H) = n_2(S)$ that $3^p = 2r^n + 3$, which is false.

If $S = C_p(2)$ or $D_{p+1}(2)$ then $n_2(S) = 2^p - 1$, but the equality $2^p - 1 = 2^{kn} + 1$ is impossible. By similar reasons the case of $S = {}^2B_2(q)$, $q = 2^{2l+1} > 2$, $n_2(S) = n_2(H)$ is impossible either.

If $S = {}^2D_{n'}(3)$, where $9 \leq n' = 2^{m'} + 1 \neq p$, then $s(S) = 2$ and $n_2(S) = (3^{n'-1} + 1)/2$. Since $(3^{n'-1} + 1)/2 = r^n + 1$, we have $3^{n'-1} = 2r^n + 1$. The last equation, as mentioned, has no solutions for $n > 2$. It can be proved similarly that the case of $S = {}^2D_p(3)$ is impossible either.

Let $S = E_6(q)$ or ${}^2E_6(q)$, $q > 2$, and 3 divides $q - \varepsilon$, where $\varepsilon = 1$ in the first case and $\varepsilon = -1$ in the last. Then $n_2(S) = (q^6 + \varepsilon q^3 + 1)/3$. Since $n_2(S) = n_2(H)$, we have $q^6 + \varepsilon q^3 - 2 = 3 \cdot r^n$. Note that if $q - \varepsilon$ is divisible by 3 then $q^3 - \varepsilon$ is divisible by 9. Thus $q^6 + \varepsilon q^3 - 2 = q^6 - 1 + \varepsilon(q^3 - \varepsilon)$ is divisible by 9, therefore r^n is divisible by 3; a contradiction.

Suppose that $S = A_1(q)$, where $q = p^l$, $3 < q \equiv \varepsilon(4)$, $\varepsilon = \pm 1$. Then $s(S) = 3$, $n_2(S) = p$, and

$n_3(S) = (q+\varepsilon)/2$. If $p = r^n + 1$ then the Cartan subgroup of S contains a cyclic subgroup of order $(p-1)/2 = r^n/2 = 2^{kn-1}$. By Lemma 2.2(a) the set $\omega(G)$ does not contain $4n$. Therefore, $2^{kn-1} \le 2n$, which is false for $n > 4$. Now let $n_3(S) = n_2(H)$. If $\varepsilon = 1$ then $q = 2r^n + 1 \equiv 0(3)$, hence $p = 3$ and $3^l = 2^{kn+1} + 1$, which is impossible for $n > 2$. If $\varepsilon = -1$ then $q = 2r^n + 3 \equiv 0(5)$, therefore $q \equiv 1(4)$; a contradiction.

Suppose that $S = F_4(q)$, where q is even, and $n_2(S) = n_2(H)$. Then $q^4+1 = r^n+1$ and $q = r^{n/4}$. Let p' be a primitive prime divisor of $q^6 + 1 = r^{3n/2} + 1$. Then p' divides the order of S and, by primitivity, does not divide that of G, since

$$\pi(G) \subseteq \pi(2(r^{n+1}+1)(r^n+1)(r^n-1)(r^{n-1}+1)(r^{n-1}-1)\dots(r+1)(r-1)).$$

Hence $\omega(S) \not\subseteq \omega(G)$, and this case is impossible.

Suppose that $S = {}^2D_{n'+1}(2)$, $n' = 2^{m'} \ge 4$, and $G \ne S$. Then $n_2(S) = 2^{n'} + 1$ and $2^{n'} + 1 = r^n + 1$, thus $n' = kn$. Let p' be a primitive prime divisor of $2^{n'+1} + 1 = 2^{nk+1} + 1$. Then p' divides $|S|$ and, by primitivity, does not divide $|G|$, since

$$\pi(G) = \pi(2(2^{nk}+1)(2^{nk}-1)(2^{nk-k}+1)(2^{nk-k}-1)\dots(2^k+1)(2^k-1)).$$

Thus $\omega(S) \not\subseteq \omega(G)$, and this case is impossible either.

Suppose that $S = C_{n'}(2^{k'})$, $n' = 2^{m'} \ge 2$, ${}^2D_{n'}(2^{k'})$, $n' = 2^{m'} \ge 4$, and $n_2(H) = n_2(S) = 2^{k'n'} + 1$, or $S = A_1(2^{k'})$ and $n_2(H) = n_3(S) = 2^{k'} + 1$. In the latter case we assume that $n' = 1$. Then $r^n + 1 = 2^{n'k'} + 1$, thereby $r^{n/n'} = 2^{k'}$ and $k' = kn/n'$. Observe that $|\operatorname{Out}(S)| = dk' = dk2^{m-m'}$, where $d = 1$ or $d = 2$.

If a pair (r, n) does not equal $(2, 4)$ then there exist primitive prime divisors p^+ and p^- of $r^{n-1} + 1$ and $r^{n-1} - 1$ respectively, and they are distinct. We will prove that if $n \ne n'$ then p^+ and p^- do not divide the order of S, and hence that of S_1 by Lemma 1.6(c).

If $S = A_1(r^n)$ then $|S| = r^n(r^n+1)(r^n-1)^2$ and the assertion is valid, since if $\varepsilon_1, \varepsilon_2 = \pm 1$ then $(r^n + \varepsilon_1, r^{n-1} + \varepsilon_2)$ divides $r - \varepsilon_1\varepsilon_2$.

If $S = C_{n'}(r^{n/n'})$ then

$$|S| = r^{nn'}(r^n+1)(r^n-1)(r^{n-n/n'}+1)(r^{n-n/n'}-1)\dots(r^{n/n'}+1)(r^{n/n'}-1).$$

If $S = {}^2D_{n'}(r^{n/n'})$ then

$$|S| = r^{n(n'-1)}(r^n+1)(r^{n-n/n'}+1)(r^{n-n/n'}-1)\dots(r^{n/n'}+1)(r^{n/n'}-1).$$

Since $n \ne n'$, it follows that p^+ and p^- do not divide the order of S by primitivity and the above remark.

Unlike the order of S_1, the order of G is divisible by $r^{n-1}+1$ and $r^{n-1}-1$. Therefore $p^+, p^- \in \omega(G)$. Suppose that $p^+ \cdot p^- \in \omega(G)$. Then some maximal torus T of G contains an element of order $p^+ \cdot p^-$. By Lemma 2.1 the order of this torus equals $\prod_i (r^{s_i}+1)\prod_j (r^{t_j}-1)$, where $\sum_i s_i + \sum_j t_j = n$. The number $|T|$ is divisible by $(r^{n-1}+1)(r^{n-1}-1)$ because p^+ and p^- are primitive. But $n-1+n-1 > n$ for $n > 2$ and there is no such torus in the group G. Hence $p^+ \cdot p^- \notin \omega(G)$.

Since $p^+ \in \omega(H) \setminus \omega(S_1)$, we have $p^+ \in \omega(K)$. The same is true for p^-. The group K is nilpotent, hence $p^+ \cdot p^- \in \omega(K) \subseteq \omega(H) = \omega(G)$; a contradiction.

To complete the proof, it remains to consider the cases when $S = C_n(r)$ or $S = {}^2D_n(r)$.

Let $G = {}^2D_n(r)$ and $S = C_n(r)$. Let p_1^+ and p_1^- be primitive prime divisors of $r^{n/2+1} - 1$ and $r^{n/2-1} - 1$ respectively. The numbers p_1^+ and p_1^- are distinct for $n > 4$, since for such n we have

$$(r^{n/2+1} - 1, r^{n/2-1} - 1) = (r^2 - 1, r^{n/2-1} - 1) = 1.$$

By Lemma 2.1 the group S contains a torus of order $(r^{n/2+1}+1)(r^{n/2-1}+1)$, therefore $p_1^+ \cdot p_1^- \in \omega(S)$.

By the lemma the orders of maximal tori of G coincide with the numbers $\prod_{i=1}^s (r^{s_i}+1)\prod_j (r^{t_j}-1)$, where s is odd and $\sum_{i=1}^s s_i + \sum_j t_j = n$. Therefore p_1^+, $p_1^- \in \omega(G)$. Suppose that $p_1^+ \cdot p_1^- \in \omega(G)$. Then

there is a torus T in G of order divisible by $r^{n/2+1}-1$ and $r^{n/2-1}-1$. Since a number of those factors in $|T|$ that are in form of $2^{s'}+1$ must be odd, $|T|$ has at least one more factor in form of $2^{s'}+1$. On the other hand, $s'+(n/2+1)+(n/2-1)=s'+n>n$; a contradiction. Therefore $p_1^+p_1^-\notin\omega(G)$. Thus $\omega(S)\not\subseteq\omega(G)$, and this case is impossible.

Conversely, let $G=C_n(r)$ and $S={}^2D_n(r)$. Consider numbers p_1^+, p_1^-, p_2^+, p_2^-, p_3^+, and p_3^- that are primitive prime divisors of $r^{n/2+1}-1$, $r^{n/2-1}-1$, $r^{n/2+1}+1$, $r^{n/2-1}+1$, $r^{n/2+3}+1$, and $r^{n/2-3}+1$ respectively. If $n>8$ then p_1^+, p_1^-, p_2^+, p_2^-, p_3^+, and p_3^- are pairwise distinct. By analogy to the previous case we find that for each $i=1,2,3$ a number $p_i^+\cdot p_i^-$ lies in $\omega(G)$, but does not lie in $\omega(S)$. Moreover, by Lemma 1.6(c) this number does not lie in $\omega(S_1)$.

Suppose that $p_1^{\varepsilon_1}\cdot p_2^{\varepsilon_2}\cdot p_3^{\varepsilon_3}\in\omega(G)$ for some ε_1, ε_2, $\varepsilon_3\in\{+,-\}$. Then there is a torus T in G of order divisible by

$$(r^{n/2+\varepsilon_1}-1)(r^{n/2+\varepsilon_2}+1)(r^{n/2+3\varepsilon_3}-1),$$

but

$$n/2+\varepsilon_1+n/2+\varepsilon_2+n/2+3\varepsilon_3\geq 3n/2-5>n$$

for $n>10$; a contradiction.

For each $i=1,2,3$ we have $p_i^+\cdot p_i^-\in\omega(H)\backslash\omega(S_1)$, therefore there is $\varepsilon_i\in\{+,-\}$ such that $p_i^{\varepsilon_i}\in\omega(K)$. The group K is nilpotent. Hence,

$$p_1^{\varepsilon_1}\cdot p_2^{\varepsilon_2}\cdot p_3^{\varepsilon_3}\in\omega(K)\subseteq\omega(H)=\omega(G),$$

which is false.

It remains to consider $G={}^2D_{n+1}(2)$ and $S=C_n(2)$ or ${}^2D_n(2)$. Note that $S_1=S$ or $S_1=S\cdot 2$ in this case. By above, if p' is a primitive prime divisor of $2^{n+1}-1$ then $p'\in\omega(G)\setminus\omega(S)$. Let p_1 and p_2 be the primitive prime divisors of $2^{n/2}+1$ and $2^{n/2+1}-1$ respectively. The numbers p', p_1 and p_2 are pairwise distinct for $n>2$.

The number $p_1\cdot p_2$ belongs to $\omega(G)\setminus\omega(S)$, since by Lemma 2.1 there is a torus of order $(2^{n/2}+1)(2^{n/2+1}-1)$ in G, and there is no such torus in S. By the lemma there are no tori of order $(2^{n+1}-1)(2^{n/2}+1)$ and $(2^{n+1}-1)(2^{n/2+1}-1)$ in G. Hence, $p'\cdot p_1$, $p'\cdot p_2\notin\omega(G)$.

Since $p',p_1\cdot p_2\in\omega(H)\setminus\omega(S)$, it implies that $p',p_i\in\omega(K)$ for some $i\in\{1,2\}$. Therefore, $p'\cdot p_i\in\omega(K)\subseteq\omega(H)=\omega(G)$, which is false.

Thus the theorem is proved for all ${}^2D_{n+1}(2)$ and ${}^2D_n(2^k)$ with $n>4$, and for all $C_n(2^k)$ with $n>8$. Furthermore, it proved in [7] that ${}^2D_4(2)$ and ${}^2D_5(2)$ are recognizable by spectrum. Therefore, to complete the proof, we need to consider ${}^2D_4(r)$, $r>2$, and $C_8(r)$.

Let $G={}^2D_4(r)$, $r=2^k>2$. It suffices to consider those groups S that we rejected using the condition $n>4$.

Suppose that $S=A_{p+1},A_{p+2},A_{p+3}$, where $p=r^4+1$. Let p' be a primitive prime divisor of r^6+1. Then p' divides $(r^6+1)/(r^2+1)=r^4-r^2+1<p$. Therefore, there is an element of order p' in S. On the other hand, p' does not divide the order of G by primitivity. Thus $p'\in\omega(S)\setminus\omega(G)$, and we arrive at a contradiction.

Suppose that $S=A_1(p^l)$, where $p=r^4+1$. The order of S equals $p^l(p^l+1)(p^l-1)^2$. It is easy to show that this number is divisible by

$$p+1=r^4+2=2^{4k}+2=2(2^{4k-1}+1).$$

Since $k>1$, a primitive prime divisor of $2^{4k-1}+1$ does not divide the order of G. Hence, $\omega(S)\not\subseteq\omega(G)$, and we arrive at a contradiction again.

Suppose that $S=C_4(r)$. It suffices to show that $\omega(S)\not\subseteq\omega(G)$.

We prove a more general assertion that for some odd prime p a number $2\cdot p$ belongs to $\omega(C_n(r))\setminus\omega({}^2D_n(r))$, where $r=2^k\geq 2$, $n\geq 4$. The properties of involution centralizers in $C_n(r)$ and ${}^2D_n(r)$ are described in [21]. If C is a centralizer of an involution in ${}^2D_n(r)$ then the factor-group $C/O_2(C)$

is isomorphic to $C_l(r) \times {}^2D_{n-2l}(r)$ or $C_{l-1}(r) \times C_{n-2l}(r)$, where $l \leq n/2$. Thus, $\pi(C) \subseteq \pi(C_{n-2}(r))$. There is an involution centralizer C in $C_n(r)$ such that $C/O_2(C) \simeq C_{n-1}(r)$. If $(n,r) \neq (4,2)$ and p is a primitive prime divisor of $r^{n-1}+1$ then p does not divide the order of $C_{n-2}(r)$ and divides that of $C_{n-1}(r)$. If $(n,r) = (4,2)$ then $p = 7$ has the same property. Thus p is connected with 2 in $\omega(C_n(r))$ and not connected with it in $\omega({}^2D_n(r))$.

The case if $G = {}^2D_4(r)$ is examined completely.

Let $G = C_8(r)$. The only simple group S that we rejected using the condition $n > 8$ is $S = {}^2D_8(r)$. By above, if p_1^+ and p_1^- are primitive prime divisors of $r^{n/2+1}-1$ and $r^{n/2-1}-1$ respectively then $p_1^+p_1^- \in \omega(G) \setminus \omega(S)$. Hence $p = p_1^\varepsilon \in \omega(K)$ for some $\varepsilon \in \{+,-\}$.

Let P be a Sylow p-subgroup of the group K. The subgroup $\Phi(P)$ is normal in H. Consider the factor-groups $\overline{H} = H/\Phi(P)$, $\overline{K} = K/\Phi(P)$, and $V = P/\Phi(P)$ instead of H, K and P. It is easy to observe that since $p \in \pi_1(H)$, the graph $GK(\overline{H})$, as well as $GK(H)$, is disconnected. By the Corollary of Lemma 2.3 there is a Frobenius subgroup R with kernel of order r^7 and cyclic complement of order r^7-1 in G. The groups $\overline{H}$, $\overline{K}$, $R \leq G \simeq \overline{H}/\overline{K}$, V, and $M = V \leftthreetimes R$ satisfy the conditions of Lemma 1.3. Hence, $\omega(M) \subseteq \omega(\overline{H}) \subseteq \omega(H) = \omega(G)$.

Since $\overline{K} \leq C_{\overline{H}}(V) \trianglelefteq (\overline{H})$ and a group $\overline{H}/\overline{K} \simeq G$ is simple, we have $C_{\overline{H}}(V) = \overline{K}$ or $C_{\overline{H}}(V) = \overline{H}$. Since the graph $GK(\overline{H})$ is disconnected, the latter is impossible and $C_{\overline{H}}(V) = \overline{K}$. By Lemma 1.4 the group M contains an element of order $p \cdot (r^7-1)$, so does the group G. Lemma 2.2(b) implies that p divides either $r+1$ or $r-1$, which contradicts the primitivity of p.

The case if $G = C_8(r)$ is examined similarly, and the theorem is proved.

§ 4. Proof of Theorem 1

Let $G = C_n(2)$, $n = 2^m > 4$, and let H be a finite group such that $\omega(H) = \omega(G)$. By the results of the preceding section, H contains a normal nilpotent subgroup K such that $G \leq H/K \leq \mathrm{Aut}(G)$. We have $\mathrm{Aut}(G) = G$, therefore $H/K = G$. We will prove that $K = 1$.

Suppose that $K \neq 1$. We may assume without loss of generality that K is an elementary abelian p-group. Since $GK(H)$ is disconnected, $C_H(K) \neq H$. Since G is simple, $C_H(K) = K$. Therefore, H induces by conjugation a group of automorphisms of K isomorphic to G. We will use Lemma 1.4 and the Frobenius subgroups of G in further reasoning.

By Lemma 2.4 the group G contains a Frobenius subgroup with kernel of order 2^n+1 and cyclic complement of order $2n$. If $p = 2$ then by Lemma 1.4 the group H, as well as G, contains an element of order $2 \cdot 2n$, which contradicts Lemma 2.2(a).

By Lemma 2.5 G contains a Frobenius subgroup with kernel of order $2^{2\cdot 3^l}$ and cyclic complement of order 3^{l+1}, where $3^l < n < 3^{l+1}$. If $p = 3$ then by Lemma 1.4 H contains an element of order $3 \cdot 3^{l+1}$, which contradicts Lemma 2.2(c).

Now let $p \neq 2,3$. By the Corollary of Lemma 2.3, G contains a Frobenius subgroup with kernel of order 2^{n-1} and cyclic complement of order $2^{n-1}-1$. Since $p \neq 2$, by Lemma 1.4 H contains an element of order $p \cdot (2^{n-1}-1)$. Lemma 2.2(b) implies that p equals 3; a contradiction.

Thus $K = 1$. Hence $H = G$, and the theorem is proved for $C_n(2)$.

Let $G = {}^2D_{n+1}(2)$, $n = 2^m > 4$, and let H be a finite group such that $\omega(H) = \omega(G)$. By the results of the preceding section, H contains a normal nilpotent subgroup K such that $G \leq H/K \leq \mathrm{Aut}(G)$. It is known that $\mathrm{Aut}(G) = G \cdot 2$ and $\mathrm{Aut}(G) \setminus G$ contains an involutive field automorphism g. The centralizer of g in G contains a subgroup isomorphic to $C_n(2)$. Therefore, it contains an element of order 2^n+1. Thus, $2 \cdot (2^n+1)$ belongs to $\omega(\mathrm{Aut}(G))$ and does not belong to $\omega(G)$. Hence, $\omega(\mathrm{Aut}(G)) \neq \omega(G) = \omega(H)$ and $H/K = G$.

As in the previous case, we may assume that K is an elementary abelian p-group and $C_H(K) = K$.

If $p = 2$ then we apply the same argument as to $C_n(2)$. By the Corollary of Lemma 2.4 the group G contains a Frobenius subgroup with kernel of order 2^n+1 and cyclic complement of order $2n$. Hence, by Lemma 1.4 H contains an element of order $2 \cdot 2n$, which contradicts Lemma 2.2(a).

Let $p \neq 2$. By Lemma 2.6 the group G contains a Frobenius subgroup with kernel of even order and cyclic complement of order $2^n + 1$. By Lemma 1.4 H contains an element of order $p(2^n + 1)$, but a number $2^n + 1$ belongs to $\mu(G) = \mu(H)$ by Lemma 1.2. This contradiction completes the proof.

References

1. *Mazurov V. D.*, "On the set of element orders in a finite group," Algebra i Logika, **33**, No. 1, 81–89 (1994).
2. *Shi W.*, "A characteristic property of $PSL_2(7)$," J. Austral. Math. Soc. Ser. A., **36**, No. 3, 354–356 (1984).
3. *Shi W.*, "A characteristic property of A_5," J. Southwest-China Teachers Univ., **3**, 11–14 (1986).
4. *Shi W.*, "A characteristic property of J_1 and $PSL_2(2^n)$," Adv. Math., **16**, 397–401 (1987).
5. *Brandl R. and Shi W.*, "The characterization of $PSL(2, q)$ by its element orders," J. Algebra, **163**, No. 1, 109–114 (1994).
6. *Mazurov V. D.*, "Recognition of the finite simple groups $S_4(q)$ by their element orders," Algebra i Logika, **41**, No. 2, 166–198 (2002).
7. *Shi W. and Tang C. J.*, "A characterization of some orthogonal groups," Prog. Nat. Sci., **7**, No. 2, 155–162 (1997).
8. *Mazurov V. D., Xu M. C., and Cao H. P.*, "Recognition of the finite simple groups $L_3(2^m)$ and $U_3(2^m)$ by their element orders," Algebra i Logika, **39**, No. 5, 567–585 (2000).
9. *Mazurov V. D.*, "On recognition of finite groups by the set of element orders," Algebra i Logika, **37**, No. 6, 651–666 (1998).
10. *Conway J. H., Curtis R. T., Norton S. P., Parker R. A., and Wilson R. A.*, Atlas of Finite Groups, Clarendon Press, Oxford (1985).
11. *Alekseeva O. A. and Kondrat′ev A. S.*, "On recognition of the group $E_8(q)$ by the set of element orders," Ukrain. Mat. Zh., **54**, No. 7, 998–1003 (2002).
12. *Williams J. S.*, "Prime graph components of finite groups," J. Algebra, **69**, No. 2, 487–513 (1981).
13. *Kondrat′ev A. S. and Mazurov V. D.*, "Recognition of alternating groups of prime degree from their element orders," Sibirsk. Mat. Zh., **41**, No. 2, 359–369 (2000).
14. *Mazurov V. D.*, "Characterization of finite groups by sets of element orders," Algebra i Logika, **36**, No. 1, 37–53 (1997).
15. *Zsigmondy K.*, "Zur Theorie der Potenzreste," Monatsh. Math. Phys., **3**, 265–284 (1892).
16. *Seminar on Algebraic Groups and Related Finite Groups*, Springer-Verlag, Berlin; Heidelberg; New York (1970).
17. *Carter R. W.*, Simple Groups of Lie Type, John Wiley & Sons, London (1972).
18. *Zavarnitsin A. V.*, Element Orders in Coverings of the Groups $L_n(q)$ and Recognition of the Alternating Group A_{16} [in Russian] [Preprint, No. 48], NII Diskret. Mat. Inform., Novosibirsk (2000).
19. *Grechkoseeva M. A.*, "On minimal permutation representations of classical simple groups," Sibirsk. Mat. Zh., **44**, No. 3, 560–586 (2003).
20. *Aleeva M. R.*, "On finite simple groups with the set of element orders as that of the Frobenius or double Frobenius group," Mat. Zametki, **73**, No. 3, 323–339 (2003).
21. *Aschbacher M. and Seitz G. M.*, "Involutions in Chevalley groups over fields of even order," Nagoya Math. J., **63**, 1–91 (1976).