Characterization of the finite simple groups by spectrum and order*)

A. V. Vasil′ev, M. A. Grechkoseeva, V. D. Mazurov

The *spectrum* of a group G is the set $\omega(G)$ of its element orders. The spectrum of a finite group G together with its order retains a substantial part of the information on the structure of G but, as demonstrated by the example of the dihedral group D_8 of order 8 and the quaternion group Q_8, does not necessarily determine G uniquely. In [1] W. Shi conjectured that the desired uniqueness will be achieved for finite simple groups. A. S. Kondrat′ev posed this conjecture in [2, Question 12.39] in the following form:

Is it true that a finite group and a finite simple group are isomorphic if they have equal orders and the same set of orders of elements ?

Later, for brevity, it was suggested to refer to a finite group G that is isomorphic to every finite group H with $\omega(H) = \omega(G)$ and $|H| = |G|$ as *recognizable by spectrum and order*. In this terminology Shi's question sounds as follows:

Is it true that all finite simple groups are recognizable by spectrum and order ?

The answer to this question is obviously affirmative for abelian simple groups. In a series of papers[1, 3–8], the affirmative answer was obtained for all nonabelian simple groups except the symplectic groups, orthogonal groups of odd dimension and orthogonal groups of type D_n with n even. In the present article we prove the recognizability by spectrum and order for this remaining groups. Thus Shi's conjecture is confirmed and the following theorem holds.

THEOREM. *If G is a finite simple group, H is a finite group with $\omega(H) = \omega(G)$ and $|H| = |G|$, then $H \simeq G$.*

*)The work is supported by the Russian Foundation for Basic Research (project 08–01–00322), the Council for Grants (under RF President) and State Aid of Leading Scientific Schools (projects NSh–344.2008.1 and MK–377.2008.1), the Program "Development of the Scientific Potential of Higher School" of the Russian Federal Agency for Education (project 2.1.1.419), and by the Federal Program "Scientific and Scientific-Pedagogical Personnel of Innovative Russia" in 2009-2013 (gov. contract no. 02.740.11.0429).

Observe that we consider the problem of recognizing a finite simple group by spectrum and order from the point of view of a more general and, in our opinion, more interesting problem of recognizing by spectrum alone. As a result of such an approach, we managed to prove a number of assertions related to the recognition of symplectic and orthogonal groups by spectrum. These assertions, which play a considerable part in proving the main result of the present article, became the subject of a separate paper [9].

§ 1. Preliminaries

Our notation for sporadic and simple groups of Lie type follows [10]. In this connection if a group of Lie type L is denoted by ${}^tX_n(q)$ [10, p. xiv, xv], we say that L is a *group of rank n over a field of order q*. In particular, the rank of a twisted group is supposed to be equal to that of the associated untwisted group. Sometimes, for brevity, we use notation f, where f and f. The alternating group of degree n is denoted by Alt_n.

For a natural number n, $\pi(n)$ denotes the set of prime divisors of n. For a prime r, n_r denotes the r-part of n, i. e., the largest power of r that divides n, while $n_{r'}$ denotes the r'-part of n, i. e., the ratio n/n_r. The greatest common divisor and the least common multiple of natural numbers $m_1, m_2, \ldots, m_k$ are denoted by $(m_1, m_2, \ldots, m_k)$ and $[m_1, m_2, \ldots, m_k]$ respectively. If $m > 2$ and n are coprime natural numbers, then we write $e(m, n)$ to denote the multiplicative order of n modulo m. Given an odd n, we put $e(2, n) = 1$ if $n \equiv 1 \pmod 4$ and put $e(2, n) = 2$ if $n \equiv 3 \pmod 4$.

Let $n > 1$. A prime r is said to be a *primitive prime divisor* of the difference $n^i - 1$ if $e(r, n) = i$.

LEMMA 1.1 (Zsigmondy [11])**.** *Let $n > 1$ be a natural number. Then for every natural number i, there is a prime r with $e(r, n) = i$, except when $n = 2$ and $i = 1$, $n = 3$ and $i = 1$, $n = 2$ and $i = 6$.*

In what follows the notation $r_i(n)$ means a primitive prime divisor of $n^i - 1$ if such exist. The product of all primitive divisors of $n^i - 1$ taken with multiplicities is said to be the *greatest primitive divisor* and denoted by $k_i(n)$. Note that for a divisor, the property of being primitive depends on the pair (n, i) and is not determined by the number $n^i - 1$. For

example, $k_6(2) = 1$, $k_3(4) = 7$, $k_2(8) = 9$, and $k_1(64) = 63$.

It is not hard to check that $k_1(n) = (n-1)/2$ if $n \equiv 3 \pmod 4$, and $k_1(n) = n-1$ in all other cases; and also that $k_2(n) = (n+1)/2$ if $n \equiv 1 \pmod 4$, and $k_2(n) = n+1$ otherwise. It follows from [12] that for $i > 2$

$$k_i(n) = \Phi_i(n)/(r, \Phi_{i_{r'}}(n)), \tag{1.1}$$

where $\Phi_i(x)$ is the ith cyclotomic polynomial and r is the largest prime dividing i, and if $i_{r'}$ does not divide $r-1$, then $(r, \Phi_{i_{r'}}(n)) = 1$.

Now we give an upper bound for element orders in simple groups of Lie type. We make use of the following number-theoretic

LEMMA 1.2. *Let m be a natural number, $m = m_1 + m_2 + \cdots + m_s$ be an expansion of m into a sum of nonzero summands, and u be an even natural number.*

(1) *If $u^{m_1}+1$, $u^{m_2}+1, \ldots$ $u^{m_s}+1$ are pairwise coprime then*

$$a = (u^{m_1}+1)(u^{m_2}+1)\ldots(u^{m_s}+1) \leqslant (u^{m'_1}+1)(u^{m'_2}+1)\ldots(u^{m'_t}+1),$$

where $m'_1 + m'_2 + \cdots + m'_t$ is the binary expansion of m. In particular, if $\widetilde{m}$ is the 2-part of m then $a \leqslant (u^{m+\widetilde{m}}-1)/(u^{\widetilde{m}}-1)$.

(2) *The number $a = [u^{m_1} \pm 1, u^{m_2} \pm 1, \ldots, u^{m_s} \pm 1]$, where signs can be chosen independently, does not exceed $(u^{m+1}-1)/(u-1)$.*

Proof. (1) We proceed by induction on m. If $m = 1$, the assertion is obvious.

Let all m_i be even. By the inductive hypothesis

$$a \leqslant ((u^2)^{m'_1}+1)((u^2)^{m'_2}+1)\ldots((u^2)^{m'_t}+1),$$

where $m'_1 + m'_2 + \cdots + m'_t$ is the binary expansion of $m/2$. Since $2m'_1 + 2m'_2 + \cdots + 2m'_t$ is the binary expansion of m, in this case the required inequality holds.

Suppose that not all m_i are even. If m_i and m_j are odd then $u^{m_i}+1$ and $u^{m_j}+1$ are not coprime. Thus there is exactly one odd number among m_i. We assume that this is m_1.

Suppose that $m_1 = 1$. By the inductive hypothesis

$$a \leqslant (u+1)(u^{m'_1}+1)(u^{m'_2}+1)\ldots(u^{m'_t}+1),$$

where $m'_1+m'_2+\cdots+m'_t$ is the binary expansion of the even number $m-1$. Since $1+m'_1+m'_2+\cdots+m'_t$ is the binary expansion of m, in this case the required inequality holds.

Suppose that $m_1 \geqslant 3$. Put $l = m - m_1$ and denote the 2-part of l by $\widetilde{l}$. Then $\widetilde{l} \geqslant 2$. By the inductive hypothesis

$$a \leqslant (u^{m_1}+1)\frac{u^{l+\widetilde{l}}-1}{u^{\widetilde{l}}-1} \leqslant (u^{m_1}+1)(u^l+u^{l-2}+\cdots+u^2+1).$$

Since m_1 is odd and l is even, we have

$$(u^{m_1}+1)(u^l+u^{l-2}+\cdots+u^2+1) \leqslant u^m+u^{m-2}+u^{m-3}+\cdots+1 \leqslant u^m+u^{m-1}.$$

It remains to observe that the binary expansion $m'_1+m'_2+\cdots+m'_t$ of m contains 1, so the polynomial $(u^{m'_1}+1)(u^{m'_2}+1)\ldots(u^{m'_t}+1)$ contains u^{m-1} in addition to u^m.

Let $m = m_1+m_2+\cdots+m_s$ be the binary expansion of m. We claim that $a \leqslant (u^{m+\widetilde{m}}-1)/(u^{\widetilde{m}}-1)$, where $\widetilde{m}$ is equal to the 2-part of m. We can assume that $\widetilde{m} = m_1$. Also $a = (u^{m_1}+1)\ldots(u^{m_s}+1) = \sum u^{m_{i_1}+\cdots+m_{i_l}}$, where the sum runs over all distinct subsets $\{i_1,\ldots,i_l\}$ of $\{1,\ldots,s\}$. The numbers m_i are pairwise different but every natural number can be uniquely expanded as a sum of pairwise different powers of two, hence each coefficient in the expansion of a by powers of u^{m_1} is equal to 0 or 1. Thus $a \leqslant u^m+u^{m-m_1}+\cdots+1 = (u^{m+m_1}-1)/(u^{m_1}-1)$.

(2) We proceed by induction on m. The assertion is obvious if $m = 1$.

Suppose that there is a minus among the signs. Assume that the minus enters into $u^{m_1}\pm 1$. Then by the inductive hypothesis

$$\begin{aligned} a &\leqslant (u^{m_1}-1)[u^{m_2}\pm 1,\ldots,u^{m_s}\pm 1] \\ &\leqslant (u^{m_1}-1)\frac{u^{m-m_1+1}-1}{u-1} = \frac{u^{m+1}-u^{m_1}-u^{m-m_1+1}+1}{u-1}, \end{aligned}$$

and the required inequality follows.

Thus all signs are pluses. Suppose that there are non-coprime numbers among $u^{m_i}+1$. Let $(u^{m_1}+1, u^{m_2}+1) \neq 1$. If $m_1 = m_2$ then $a \leqslant (u^{m-m_1+1}-1)/(u-1) < (u^{m+1}-1)/(u-1)$, so we can assume that $m_1 < m_2$. By $(u^{m_1}+1, u^{m_2}+1) \geqslant u+1$ and the inductive hypothesis,

we have

$$a \leqslant \frac{(u^{m_1}+1)(u^{m_2}+1)}{u+1} \cdot \frac{u^{m-m_1-m_2+1}-1}{u-1}$$
$$\leqslant \frac{u^{m+1}+u^{m-m_1+1}+u^{m-m_2+1}+u^{m-m_1-m_2+1}-u-1}{(u+1)(u-1)},$$

whence

$$a \leqslant \frac{u^{m+1}+u^m+u^{m-1}+u^{m-2}-u-1}{(u+1)(u-1)} \leqslant \frac{u^{m+2}+u^{m+1}-u-1}{(u+1)(u-1)} = \frac{u^{m+1}-1}{u-1}.$$

The lemma is proved.

LEMMA 1.3. *Let S be a simple group of Lie type of rank m over a field of characteristic v and order u.*

(1) *If S is a Ree or Suzuki group distinct from the Tits group ${}^2F_4(2)'$, then element orders of S is at most $v/(v-1)\cdot u^{m/2}$.*

(2) *If $S = E_8(u)$ then element orders of S is at most $(u+1)/(u-1)\cdot u^8$.*

(3) *If S is distinct from Ree and Suzuki groups and from $E_8(u)$, then element orders of S is at most $u/(u-1)\cdot u^m$.*

Proof. (1) The periods of maximal tori of ${}^2F_4(u)$, ${}^2G_2(u)$, and ${}^2B_2(u)$ do not exceed $u^2+u\sqrt{2u}+u+\sqrt{2u}+1$, $u+\sqrt{3u}+1$, and $u+\sqrt{2u}+1$ respectively (see [13, Tables 3–6]). By hypothesis $v < u$, therefore every of these numbers is bounded above by the sum of geometric series with the ratio v, the first term equal to 1 and the last term equal to $u^{m/2}$. This sum is equal to $(vu^{m/2}-1)/(v-1)$ and so does not exceed $v/(v-1)\cdot u^{m/2}$.

By [14, Prop. 0.5], the largest order of v-elements in ${}^2F_4(u)$, ${}^2G_2(u)$ and ${}^2B_2(u)$ is equal to 16, 9 and 4 respectively; in particular, it is not larger than $u^{m/2}$.

It follows from [13, Table 3] that orders of elements of mixed type in ${}^2F_4(u)$ are at most $v^2(u+\sqrt{2u}+1)$. Since $u \geqslant v^3$, this number is less than $v/(v-1)\cdot u^{m/2}$. The order of every element of mixed type in ${}^2G_2(u)$ is equal to 6 and, since $u \geqslant 27$, does not exceed $v/(v-1)\cdot u^{m/2}$. There is no elements of mixed type in ${}^2B_2(u)$.

(2) It follows from [15] that periods of maximal tori of $E_8(u)$ are at most $(u^5-1)(u+1)(u^2+u+1) = u^8+2u^7+2u^6+u^5-u^3-2u^2-2u-1$, therefore, they are less than $u^8+2u^8/(u-1) = (u+1)/(u-1)\cdot u^8$.

By [14, Prop. 0.5], orders of v-elements of $E_8(u)$ are at most u^5. Using information from [16, Table 2], it is not hard to check that orders of elements of mixed type do not exceed $v(u^7 + 2u^7/(u-1)) = (u+1)/(u-1) \cdot vu^7$.

(3) Let S be an exceptional group of Lie type distinct from Ree and Suzuki groups and from $E_8(u)$. Using [14, Prop. 0.5; 16, Tables 1; 13], it is not hard to check that element orders of S do not exceed $u^m + u^{m-1} + \cdots + 1$, therefore, they are less than $u/(u-1) \cdot u^m$. So S is a classical group in what follows.

Let $S = A_m^{\varepsilon}(u)$. By [17, 18], $\omega(S)$ is contained in the set of divisors of the following numbers:

$(u^{m+1} - \varepsilon 1)/(u - \varepsilon 1)$, $[u^{m_1} - (\varepsilon 1)^{m_1}, \ldots, u^{m_s} - (\varepsilon 1)^{m_s}]$, where $m_1 + \cdots + m_s = m+1$ and $s \geqslant 2$;

$v^{l+1}[u^{m_1} - (\varepsilon 1)^{m_1}, \ldots, u^{m_s} - (\varepsilon 1)^{m_s}]$, where $l \geqslant 0$ and $v^l + 1 + m_1 + \cdots + m_s = m+1$;

v^{l+1}, if $v^l = m$.

Note that $(u^{m+1} - \varepsilon 1)/(u - \varepsilon 1) < (u^{m+1} - 1)/(u-1) < u^{m+1}/(u-1)$. Furthermore, for every $m_1, \ldots, m_s$ such that $m_1 + \cdots + m_s = m+1$ and $s \geqslant 2$, we have

$$[u^{m_1} - 1, \ldots, u^{m_s} - 1] \leqslant \frac{(u^{m_1} - 1) \ldots (u^{m_s} - 1)}{u - 1} \leqslant \frac{u^{m+1}}{u-1}, \tag{1.2}$$

$$\begin{aligned}[u^{m_1} - (-1)^{m_1}, \ldots, u^{m_s} - (-1)^{m_s}] &\leqslant (u+1)\frac{u^{m_1} - (-1)^{m_1}}{u+1} \ldots \frac{u^{m_s} - (-1)^{m_s}}{u+1} \\ &\leqslant (u+1)u^{m_1 - 1} \ldots u^{m_s - 1} = (u+1)u^{m+1-s} < \frac{u^{m+1}}{u-1}. \end{aligned} \tag{1.3}$$

Hence the order of a semisimple element of S is at most $u^{m+1}/(u-1)$.

Let $a = v^{l+1}[u^{m_1} - (\varepsilon 1)^{m_1}, \ldots, u^{m_s} - (\varepsilon 1)^{m_s}]$, where $l \geqslant 0$ и $v^l + m_1 + \cdots + m_s = m$. Since $l + 1 \leqslant v^l < m$ and it follows from (1.2) and (1.3) that $[u^{m_1} - (\varepsilon 1)^{m_1}, \ldots, u^{m_s} - (\varepsilon 1)^{m_s}] \leqslant u^{m_1 + \cdots + m_s} + 1$, we have $a \leqslant u^{v^l}(u^{m_1 + \cdots + m_s} + 1) = u^m + u^{v^l} \leqslant u^m + u^m/u < u^{m+1}/(u-1)$. If $v^l = m$ then $a = v^{l+1} \leqslant u^{v^l} = u^m$. Thus the assertion is proved for linear and unitary groups.

Let S be a symplectic or orthogonal group. Observe that $\omega(D_m^{\varepsilon}(u)) \subseteq \omega(B_m(u))$, because $B_m(u)$ contains the section isomorphic to $D_m^{\varepsilon}(u)$ and $\omega(B_m(u)) \subseteq \omega(C_m(u))$ by [19, Cor. 1, 3]. It suffices therefore to handle the symplectic groups.

Let $S = C_m(u)$, where u is odd. By [19, Cor. 1], the spectrum of S coincides with the set of divisors of the following numbers:

$(u^m \pm 1)/2$, $[u^{m_1} \pm 1, \dots, u^{m_s} \pm 1]$, where $m_1 + \dots + m_s = m$ и $s \geqslant 2$;

$v^{l+1}[u^{m_1} \pm 1, \dots, u^{m_s} \pm 1]$, where $l \geqslant 0$ and $(v^l + 1)/2 + m_1 + \dots + m_s = m$;

v^{l+1}, and $v^l + 1 = 2m$.

It follows by [20, Lemma 9(1)] that for $m \geqslant 4$, the order of a semisimple element of S is at most $u^m + 1$. For $m = 2, 3$ this fact can be established by direct calculation.

Let $a = v^{l+1}[u^{m_1} \pm 1, \dots, u^{m_s} \pm 1]$, where $(v^l + 1)/2 + m_1 + \dots + m_s = m$. Suppose that $l \geqslant 2$. Then $l + 1 \leqslant (v^l - 1)/2$. Together with the estimate of orders of semisimple elements, this yields

$$a \leqslant u^{(v^l-1)/2}(u^{m_1+\dots+m_s} + 1) = u^{m-1} + u^{(v^l-1)/2} < u^m.$$

If $l = 0$ then $a \leqslant v(u^{m-1} + 1) \leqslant u^m + u$. If $l = 1$ then $m \geqslant 3$ and $a \leqslant u^2(u^{m-2} + 1) = u^m + u^2 \leqslant u^m \cdot u/(u - 1)$. If $v^l + 1 = 2m$ then $a = v^{l+1} \leqslant u^{(v^l+1)/2} = u^m$.

Let $S = C_m(u)$, where u is even. By [19, Cor. 2], the spectrum of S coincides with the set of divisors of the following numbers:

$[u^{m_1} \pm 1, \dots, u^{m_s} \pm 1]$, where $m_1 + \dots + m_s = m$;

$2[u^{m_1} \pm 1, \dots, u^{m_s} \pm 1]$, where $m_1 + \dots + m_s = m - 1$;

$2^{l+1}[u^{m_1} \pm 1, \dots, u^{m_s} \pm 1]$, where $l \geqslant 1$ and $2^{l-1} + 1 + m_1 + \dots + m_s = m$;

2^{l+1}, and $2^{l-1} = m$.

Lemma 1.2 implies that the order of a semisimple element of $C_m(u)$ is at most $(u^{m+1} - 1)/(u - 1)$.

Let $a = 2^{l+1}[u^{m_1} \pm 1, \dots, u^{m_s} \pm 1]$, where $l \geqslant 1$ and $2^{l-1} + 1 + m_1 + \dots + m_s = m$. Since $l \leqslant 2^{l-1}$ and $[u^{m_1} \pm 1, \dots, u^{m_s} \pm 1] \leqslant (u^{m_1+\dots+m_s+1} - 1)/(u - 1)$, we have

$$a \leqslant u^{2^{l-1}+1}\frac{u^{m_1+\dots+m_s+1} - 1}{u - 1} = \frac{u^{m+1} - u^{2^{l-1}+1}}{u - 1} \leqslant \frac{u^{m+1} - 1}{u - 1}.$$

The cases when $a = 2[u^{m_1} \pm 1, \dots, u^{m_s} \pm 1]$ or $a = 2^{l+1}$ can be handled in a similar manner. The lemma is proved.

The orders of simple groups of Lie type are well-known, so it is easy to check that the following two lemmas are valid.

LEMMA 1.4. *Let S be a simple group of Lie type of rank m over a field of characteristic v and order u, and V be a Sylow v-subgroup of S. Put $\sigma(m,S) = 2\log_u |V|/m$ if S is a Ree or Suzuki group, and $\sigma(m,S) = \log_u |V|/m$ otherwise.*

(1) *If $S = {}^2B_2(u)$ then $|V| = u^2$ and $\sigma(m,S) = 2$.*

(2) *If $S = {}^2G_2(u)$ then $|V| = u^3$ and $\sigma(m,S) = 3$.*

(3) *If $S = {}^2F_4(u)$ then $|V| = u^{12}$ and $\sigma(m,S) = 6$.*

(4) *If $S = G_2(u)$ then $|V| = u^6$ and $\sigma(m,S) = 3$.*

(5) *If $S = F_4(u)$ then $|V| = u^{24}$ and $\sigma(m,S) = 6$.*

(6) *If $S = E_6^{\varepsilon}(u)$ then $|V| = u^{36}$ and $\sigma(m,S) = 6$.*

(7) *If $S = E_7(u)$ then $|V| = u^{63}$ and $\sigma(m,S) = 9$.*

(8) *If $S = E_8(u)$ then $|V| = u^{120}$ and $\sigma(m,S) = 15$.*

(9) *If $S = A_m^{\varepsilon}(u)$ then $|V| = u^{m(m+1)/2}$ and $\sigma(m,S) = (m+1)/2$.*

(10) *If $S = B_m(u)$ or $S = C_m(u)$ then $|V| = u^{m^2}$ and $\sigma(m,S) = m$.*

(11) *If $S = D_m^{\varepsilon}(u)$ then $|V| = u^{m(m-1)}$ and $\sigma(m,S) = m-1$.*

LEMMA 1.5. *Let S be a simple group of Lie type of rank larger than 1 over a field of characteristic v, and let V be a Sylow v-subgroup of S. Then $|V|^{8/3} > |S|$.*

LEMMA 1.6. *Let L be one of the groups $B_n(q)$, $C_n(q)$, $D_n^{\varepsilon}(q)$, $v \in \pi(L)$ and $(v,q) = 1$. Then the order of a Sylow v-subgroup V of L does not exceed $f(q)^{3n/2}$, where the function $f(q)$ is defined as follows*:

(1) *for $v > 3$, put $f(q) = q$ if q is odd or $v \neq q^i + 1$, and put $f(q) = q+1$ if q is even and $v = q^i + 1$;*

(2) *for $v = 3$, put $f(q) = q$ if $q \neq 2, 8$, and put $f(q) = q+1$ if $q = 2, 8$;*

(3) *for $v = 2$, put $f(q) = (q^2-1)_2$; if none of $q \pm 1$ is a power of 2 then $f(q) \leqslant (q+1)$, and in all cases $f(q) \leqslant 2(q+1)$.*

More precisely, $|V| \leqslant f(q)^n \cdot v^{\delta(n,v)}$, where $\delta = \delta(n,v) = \sum_{l=1}^{\infty} [\frac{n}{v^l}]$.

Proof. The order of L divides $q^{n^2} \prod_{j=1}^{n} (q^{2j}-1)$, therefore

$$|V| \leqslant \prod_{j=1}^{n} (q^{2j}-1)_v.$$

Let i be the multiplicative order of q^2 modulo v and $v^k = (q^{2i}-1)_v$. If i does not divide j, then $(q^{2j}-1)_v = 1$. If i divides j then $(q^{2j}-1)_v = (q^2-1)_v(j/i)_v = v^k(j/i)_v$ (cf. [21, Lemma 1]). Among natural numbers less than or equal to n, there are exactly $[n/i]$ numbers divisible by i; among them, there are exactly $[n/iv^l]$ numbers divisible by iv^l. Hence the order of V is at most $v^{k[n/i]+t}$, where $t = \sum_{l=1}^{\infty}\left[n/iv^l\right]$. We have

$$t = \sum_{l=1}^{\infty}\left[\frac{n}{iv^l}\right] \leqslant \frac{1}{i}\sum_{l=1}^{\infty}\left[\frac{n}{v^l}\right] = \frac{\delta}{i} \leqslant \frac{1}{i}\left[\sum_{l=1}^{\infty}\frac{n}{v^l}\right] = \frac{1}{i}\left[\frac{n}{v-1}\right].$$

Now we estimate $v^k = (q^i-1)_v(q^i+1)_v$ in terms of q.

Let $v \neq 2$. Then $(q^i-1, q^i+1)_v = 1$, and so v^k divides either q^i+1 or q^i-1. If q is odd and $v^k \neq q^i+1$ then $v^k < q^i+1$, hence $v^k \leqslant q^i$. If q is even and $v^k = q^i+1$ then $v^k \leqslant (q+1)^i$. Observe that the equality $v^k = q^i+1$ is possible for $v > 3$ only if $k = 1$, and for $v = 3$ it is possible only if $q = 2, 8$.

If $v = 2$ then $i = 1$, so $v^k = (q^2-1)_2 = (q-1)_2(q+1)_2 \leqslant 2(q+1)$. If neither $q-1$ nor $q+1$ is a power of 2, then $v^k = (q-1)_2(q+1)_2 \leqslant 2(q+1)/3 < q+1$.

In all cases $v^k \leqslant f(q)^i$, therefore

$$|V| \leqslant v^{k[n/i]+\delta/i} \leqslant v^{kn/i}\cdot v^{\delta/i} \leqslant f(q)^n \cdot v^{\delta/i},$$

and so the last assertion of the lemma holds. Since

$$v^{\delta/i} \leqslant v^{[n/(v-1)]/i} \leqslant f(q)^{[n/(v-1)]/k}$$

and $k \geqslant 3$ for $v = 2$, we derive that $v^{\delta/i} \leqslant f(q)^{n/2}$. Thus $|V| \leqslant f(q)^{3n/2}$. The lemma is proved.

LEMMA 1.7. *Let S be a finite nonabelian simple group whose Sylow p-subgroup P has order p^γ. If $|S| < |P|^3$ then S is one of the following groups*:

(1) *a group of Lie type over a field of characteristic p*;

(2) *an alternating or sporadic group*;

(3) $A_1(u)$;

(4) ${}^2A_2(3)$, *where* $\gamma = 5$ *and* $p = 2$;

(5) ${}^2A_4(2)$, *where* $\gamma = 5$ *and* $p = 3$.

Proof. The claim follows from [22, Lemmas 1, 2].

LEMMA 1.8 [23, Lemma 1]**.** *Let G be a finite group, K be a normal subgroup of G, G/K be 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 $|K|$.*

§ 2. Gruenberg — Kegel graph and groups isospectral to simple groups

The *Gruenberg — Kegel graph* $GK(G)$, or the *prime graph*, of a finite group G is the graph with vertex set $\pi(G)$ in which two distinct vertices p and q are adjacent if and only if $pq \in \omega(G)$. Obviously, the graph $GK(G)$ is uniquely determined by the spectrum $\omega(G)$ of G. The number of connected components of $GK(G)$ is denoted by $s(G)$, and the connected components are denoted by $\pi_i(G)$ with $1 \leq i \leq s(G)$. If G has even order, then by default $2 \in \pi_1(G)$. According to this partition, $\omega_i(G)$ is the subset of $\pi_i(G)$-numbers of $\omega(G)$ for every $1 \leq i \leq s(G)$.

LEMMA 2.1 (Gruenberg — Kegel [24])**.** *If G is a finite group with $s(G) > 1$ then one of the following holds:*

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

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

(3) *there is a nonabelian simple group S such that $S \leq \overline{G} = G/K \leq \operatorname{Aut} S$ for some nilpotent normal subgroup K of G; moreover, K and $\overline{G}/S$ are $\pi_1(G)$-groups, $s(S) \geq s(G)$, and for every $1 < i \leq s(G)$ there is $1 < j \leq s(S)$ such that $\omega_i(G) = \omega_j(S)$.*

Finite simple groups with disconnected prime graph were described in [24, 25]. The complete list of these groups, with corrected inaccuracies, can be found in [26, Tables 1a–1c]. By results of [24, 25], if S is a simple group and $s(S) > 1$ then for every $1 < i \leq s(S)$ the set $\omega_i(S)$ has a unique maximal under divisibility element. In the tables mentioned above and in the present paper, this maximal element is denoted by $n_i(S)$.

Recall that an *independent set of vertices*, or a *coclique*, in a graph Γ is a set of vertices that are pairwise non-adjacent to each other in Γ. We write $t(\Gamma)$ to denote the independence number of Γ, i. e., the maximal number of vertices in its cocliques. Given a group G, put

$t(G) = t(GK(G))$. By analogy, given a prime r, define the r-independence number $t(r, G)$ to be the maximal number of vertices in cocliques of $GK(G)$ containing the vertex r.

LEMMA 2.2 [27, 28]**.** *Let L be a finite non-abelian simple group such that $t(L) \geq 3$ and $t(2, L) \geq 2$, and G be a finite group with $\omega(G) = \omega(L)$. Then the following hold.*

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

(2) *For every coclique ρ of $GK(G)$ of size at least 3, at most one prime of ρ divides the product $|K| \cdot |\overline{G}/S|$. In particular, $t(S) \geq t(G) - 1$.*

(3) *Every prime $r \in \pi(G)$ not adjacent to 2 in $GK(G)$ does not divide the product $|K| \cdot |\overline{G}/S|$. In particular, $t(2, S) \geq t(2, G)$.*

If Γ is a prime graph and π is a set of natural numbers, we write $\Gamma \setminus \pi$ to denote the maximal subgraph of Γ all whose vertices do not lie in π. Observe that assertion (2) of Lemma 2.2 yields, alongside the inequality $t(S) \geq t(G) - 1$, the inequality $t(GK(S) \setminus \pi) \geq t(GK(G) \setminus \pi) - 1$ for every set of primes π.

LEMMA 2.3. *Let L be one of the simple groups $B_n(q)$ with $n \geq 2$ and $(n, q) \neq (2, 3)$, $C_n(q)$ with $n \geq 3$, $D_n(q)$, ${}^2D_n(q)$ with $n \geq 4$, and G be a finite group with $\omega(G) = \omega(L)$. Then there exists a simple nonabelian group S such that*

$$S \leq \overline{G} = G/K \leq \operatorname{Aut} S,$$

where K is the soluble radical of G. Furthermore, G, K and S satisfy assertions (2) *and* (3) *of Lemma* 2.2.

Proof. If $n > 2$ and $L \neq D_4(2)$ then it follows from [29] that L satisfies $t(L) \geq 3$ and $t(2, L) \geq 2$, so Lemma 2.2 implies the assertion. Let $n = 2$ or $L = D_4(2)$. Then L has disconnected prime graph, therefore, the claim follows by the Gruenberg — Kegel theorem and the main result of [30] together with the fact that in this case $t(L) = 2$. The lemma is proved.

Note that the assertion of Lemma 2.3 is false for $B_2(3)(\simeq C_2(3))$. As it is shown in [31], there exists a soluble group isospectral to L. The fact that $B_2(3)$ is recognizable by spectrum and order will be established in §3.

In what follows in this section, L is a finite simple symplectic or orthogonal group distinct from $B_2(3)$, and G is a finite group with the same spectrum (in other words, L and G are *isospectral*). Then it follows from the last lemma that G satisfies the conclusion of Lemma 2.2 and, in particular, contains a unique nonabelian composition factor S.

LEMMA 2.4 [9, Thm. 1]**.** *Let L be one of the simple groups $B_n(q)$ with $n \geq 2$ and $(n,q) \neq (2,3)$, $C_n(q)$ with $n \geq 3$, and $D_n(q)$, ${}^2D_n(q)$ with $n \geq 4$. Then there are no alternating groups among nonabelian composition factors of finite groups isospectral to L.*

LEMMA 2.5 [9, Thm. 2]**.** *Let L be one of the simple groups $B_n(q)$ with $n \geq 2$ and $(n,q) \neq (2,3)$, $C_n(q)$ with $n \geq 3$, and $D_n(q)$, ${}^2D_n(q)$ with $n \geq 4$. Then there are no sporadic groups nor the Tits group ${}^2F_4(2)'$ among nonabelian composition factors of finite groups isospectral to L.*

LEMMA 2.6 [9, Thm. 3]**.** *Let q be a power of a prime p, L be one of the simple groups $B_n(q)$ with $n \geq 2$ and $(n,q) \neq (2,3)$, $C_n(q)$ with $n \geq 3$, and $D_n(q)$, ${}^2D_n(q)$ with $n \geq 4$, G be the finite group with $\omega(G) = \omega(L)$. Suppose that there is a factor S among nonabelian composition factors of G which is isomorphic to a group of Lie type over a field of characteristic p.*

(1) *If $L = B_2(q)$, where $q > 3$, then S is isomorphic to one of the groups $A_1(q^2), B_2(q)$.*

(2) *If $L \in \{B_3(q), C_3(q), D_4(q)\}$, then S is isomorphic to one of the groups $A_1(q^3), B_3(q), C_3(q), D_4(q), G_2(q)$.*

(3) *If $n \geq 4$ and $L \in \{B_n(q), C_n(q), {}^2D_n(q)\}$, then S is isomorphic to one of the groups $B_n(q), C_n(q), {}^2D_n(q)$.*

(4) *If $n \geq 6$ is even and $L = D_n(q)$, then S is isomorphic to one of the groups $B_{n-1}(q), C_{n-1}(q), D_n(q)$.*

(5) *If $n \geq 5$ is odd and $L = D_n(q)$, then S is isomorphic to L.*

These results implies that the unique nonabelian composition factor S of a group G isospectral to L must be a group of Lie type; moreover, when L and S are defined over fields of the same characteristic, the number of possibilities for S is small. For a number of symplectic and orthogonal groups of small orders, there are some stronger assertions on G and S obtained by various authors.

LEMMA 2.7. *Let L be one of the groups $B_n(q)$, $C_n(q)$, $D_n(q)$, and G be a finite group with $\omega(G) = \omega(L)$.*

(1) *If $L = B_3(2)$ then $G \simeq B_3(2)$ or $G \simeq D_4(2)$ (see* [26, 32]*).*

(2) *If $L = B_3(3)$ then $G \simeq B_3(3)$ or $G \simeq D_4(3)$ (see* [32]*).*

(3) *If $L = B_4(2)$ then G has a unique nonabelian composition factor S and $S \in \{B_4(2), {}^2D_4(2)\}$ (see* [33]*).*

(4) *If $L = B_4(3)$ then G has a unique nonabelian composition factor S and $S \in \{B_4(3), {}^2D_4(3)\}$ (see* [20]*).*

(5) *If $L = C_3(3)$ then $G \simeq C_3(3)$ (see* [23]*).*

(6) *If $L = C_4(3)$ then G has a unique nonabelian composition factor S and u $S \in \{C_4(3), {}^2D_4(3)\}$ (see* [20]*).*

(7) *If $L = D_4(2)$ then $G \simeq B_3(2)$ or $G \simeq D_4(2)$ (see* [26, 32]*).*

(8) *If $L = D_4(3)$ then $G \simeq B_3(3)$ or $G \simeq D_4(3)$ (see* [32]*).*

It follows by Lemma 2.2 that many properties of the prime graph of L can be transferred to the graph of S in some way or other. For that reason, our proof of the main result uses an adjacency criterion of prime graphs of simple groups from [29] (with amendments from [34, § 4]). For symplectic and orthogonal groups, this criterion is formulated in terms of the function $\eta : \mathbb{N} \to \mathbb{N}$ defined by

$$\eta(n) = \begin{cases} n, \text{ if } n \text{ is odd} \\ n/2 \text{ otherwise.} \end{cases}$$

LEMMA 2.8 [9, Lemma 2.2]**.** *Let L, G, S and K be as in Lemma* 2.3*.*

(1) *Suppose $L = B_n(q)$ or $L = C_n(q)$, where $n \geqslant 3$ and $(n, q) \neq (3, 2)$. If there exists i such that $n/2 < \eta(i) \leq n$ and $k_i(q) \notin \omega(S)$ then for every $j \neq i$ with $n/2 \leq \eta(j) \leq n$, the number $k_j(q)$ is coprime to $|K| \cdot |\overline{G}/S|$ and lies in $\omega(S)$.*

(2) *Suppose $L = D_n(q)$, where $n \geq 4$ and $(n, q) \neq (4, 2)$. If there exists $i \neq 2n$ such that $n/2 < \eta(i) \leq n$ and $k_i(q) \notin \omega(S)$ then for every $j \notin \{i, 2n\}$ with $n/2 \leq \eta(j) \leq n$, the number $k_j(q)$ is coprime to $|K| \cdot |\overline{G}/S|$ and lies in $\omega(S)$.*

(3) *Suppose $L = {}^2D_n(q)$, where $n \geq 4$ and $(n, q) \neq (4, 2), (5, 2)$. If there exists $i \neq n$*

such that $n/2 < \eta(i) \leq n$ *and* $k_i(q) \notin \omega(S)$ *then for every* $j \notin \{i, n\}$ *with* $n/2 \leq \eta(j) \leq n$, *the number* $k_j(q)$ *is coprime to* $|K| \cdot |\overline{G}/S|$ *and lies in* $\omega(S)$.

LEMMA 2.9. *Let* L *be one of the simple groups* $B_n(q)$, *where* $n \geqslant 2$ *and* $(n, q) \neq (2, 3)$, $C_n(q)$, *where* $n \geqslant 3$, $D_n(q)$, *where* n *is even and* $n \geqslant 4$; G *be a finite group with* $\omega(G) = \omega(L)$, *and* S *and* K *be as in Lemma* 2.3. *Then* S *contains an element of order at least* $h(q)$, *where* $h(q)$ *is defined by the following*:

(1) *If* $L = B_n(q)$, $C_n(q)$, *where* $n \geqslant 7$, *or* $L = D_n(q)$, *where* $n \geqslant 8$, *then*

$$h(q) = \begin{cases} (q^7+1)/(q+1), & \text{if } 7 \nmid q^2-1; \\ (q^7+1)/7(q+1), & \text{if } 7 \mid q^2-1. \end{cases}$$

(2) *If* L *is one of the groups* $B_4(q)$, $C_4(q)$, $B_5(q)$, $C_5(q)$, $B_6(q)$, $C_6(q)$, $D_6(q)$, *then* $h(q) = (q^4+1)/2$.

(3) *If* L *is one of the groups* $B_2(q)$, $B_3(q)$, $C_3(q)$, $D_4(q)$, *where* $q > 2$, *then* $h(q) = (q^2+1)/2$.

Proof. (1) Let $n < 14$. By Lemma 2.8 at least one of the numbers $k_7(q)$, $k_{14}(q)$ lies in $\omega(S)$. We compare these numbers using (1.1). If $7 \nmid q^2-1$ then $k_7(q) \geqslant k_{14}(q) = (q^7+1)/(q+1)$. If $7 \mid q^2-1$ then each of the numbers $k_{14}(q)$, $k_7(q)$ is at least $(q^7+1)/7(q+1)$.

Let $n \geqslant 14$. There exist two distinct primes i and j such that $n/2 < i < j < n$. By Lemma 2.8 at least one of the numbers $k_i(q)$, $k_j(q)$ lies in $\omega(S)$. On the other hand, $k_i(q) \geqslant (q^i-1)/(q-1)^2 \geqslant (q^{11}-1)/(q-1)^2 > (q^7+1)/(q+1)$, therefore, S contains an element of the required order.

(2) For $B_4(q)$ and $C_4(q)$ the assertion follows by the Gruenberg — Kegel theorem and [26, Table 1a], so we can assume that $n = 5, 6$. Lemma 2.8 implies that at least two of the numbers $k_{10}(q)$, $k_5(q)$, $k_8(q)$ lie in $\omega(S)$. Compare these numbers. If q is even and $5 \nmid q-1$ then $k_5(q)$ and $k_8(q)$ are greater than $(q^4+1)/2$; and if $5 \mid q-1$ then $k_{10}(q)$ and $k_8(q)$ are greater than $(q^4+1)/2$. If q is odd and $5 \nmid q^2-1$ then $k_8(q) = (q^4+1)/2$ is the least number among $k_5(q)$, $k_{10}(q)$, and $k_8(q)$; and if $5 \mid q^2-1$ then $k_8(q)$ is the second largest among them.

(3) For $B_2(q)$ the assertion follows by he Gruenberg — Kegel theorem and [26, Table 1a],

so we can assume that $n = 3, 4$. By Lemma 2.8 at least two of the numbers $k_6(q)$, $k_3(q)$, and $k_4(q)$ lie in $\omega(S)$. The further argument is similar to the proof of (2). The lemma is proved.

§ 3. Proof of the theorem: Reduction

Let L be a finite simple group and G be a finite group with $\omega(G) = \omega(L)$ and $|G| = |L|$. The conclusion of the theorem obviously holds for groups of prime order, therefore, we can assume that L is nonabelian. For sporadic and alternating groups the assertion was proved in [1] and [3] respectively. Also the theorem was proved for Suzuki and Ree groups in [4] and for exceptional groups of Lie type in [5]. Furthermore, the conclusion of the theorem holds if L is a simple linear group [6], unitary group [7], orthogonal group ${}^2D_n(q)$, where n is arbitrary, or orthogonal group $D_n(q)$, where n is odd [8]. Thus, in view of the classification of the finite simple groups, to complete the prove of the theorem, it suffices to establish the following result.

THEOREM 3.1. *If L if one of the simple groups $B_n(q)$, where $n \geqslant 2$, $C_n(q)$, where $n \geqslant 3$, and $D_n(q)$, where n is even and $n \geqslant 4$, and G is a finite group with $\omega(G) = \omega(L)$ and $|G| = |L|$, then $G \simeq L$.*

It is precisely the assertion we prove in what follows.

PROPOSITION 3.1. *If $L = B_2(3)$ and G is a finite group with $\omega(G) = \omega(L)$ and $|G| = |L|$ then $G \simeq L$.*

Proof. We have $|L| = 2^6 \cdot 3^4 \cdot 5$. The graph $GK(L)$ has two connected components and $n_2(L) = (3^2 + 1)/2 = 5$. Suppose that $G \not\simeq L$. By the Gruenberg — Kegel theorem, G is either Frobenius, or 2-Frobenius, or a nonsoluble group having a unique nonabelian composition factor S. In the last case S is isomorphic to one of the alternating groups A_5 and A_6, because $\pi(S) \subseteq \pi(L) = \{2, 3, 5\}$ and $S \not\simeq L$. In all cases G includes a subgroup isomorphic to a Frobenius group with kernel A being a 3-group and complement of order 5. Since $|G|_3 = 3^4$, the inequality $|A| \leqslant 3^4$ holds. On the other hand, $e(5, 3) = 4$, so A is an elementary abelian group of order 3^4 and is a Sylow 3-subgroup of G. Therefore the 3-period of G is equal to 3, and hence $9 \in \omega(L) \setminus \omega(G)$; a contradiction.

By Proposition 3.1 we can assume that $L \neq B_2(3)$. By Lemma 2.3 for a finite group G

with $\omega(G) = \omega(L)$, there is a nonabelian simple group S such that $S \leqslant \overline{G} = G/K \leqslant \operatorname{Aut} S$, where K is the soluble radical of G. Lemmas 2.4 and 2.5 imply that S is neither alternating nor sporadic. Thus S is a group of Lie type other than the Tits group.

Now we prove a number of auxiliary results. In each of them we assume that G is a finite group with $\omega(G) = \omega(L)$ and $|G| = |L|$, while S, K and $\overline{G}$ are as in the previous paragraph.

LEMMA 3.1. *Suppose that $q = p^\alpha$, where p is a prime, L is one of the simple groups $B_n(q)$, $C_n(q)$, $(n, q) \neq (2, 3)$, or is $D_{n+1}(q)$, n is odd.*

(1) *If the order of the soluble radical K of G is divisible by p then the order of a Sylow p-subgroup of K is equal to $q^{2n\gamma}$, where γ is a positive integer.*

(2) *If p divides $|\overline{G}/S|$ then a Sylow p-subgroup of $\overline{G}/S$ is cyclic for odd p and is either cyclic or a general quaternion group for $p = 2$. In particular, if the p-period of L is equal to p^δ then $|\overline{G}/S|_p$ is at most p^δ for odd p and at most $2^{\delta+1}$ for $p = 2$. Moreover, if p divides the order of K then $|\overline{G}/S|_p \leqslant p^{\delta-1}$ for odd p and $|\overline{G}/S|_2 \leqslant 2^\delta$ for $p = 2$.*

Proof. (1) If $L = B_n(q)$ or $L = C_n(q)$ and n is even then every primitive prime divisor $r_{2n}(q)$ is not adjacent to 2 in $GK(G)$, therefore, $k_{2n}(q)$ is coprime to $|K| \cdot |\overline{G}/S|$ by Lemma 2.2(3). Note that $r_{2n}(q)$ is not adjacent to p either. If n is odd and L is one of the groups $B_n(q)$, $C_n(q)$ or $D_{n+1}(q)$, then $\{p, r_n(q), r_{2n}(q)\}$ is a coclique in $GK(G)$ (by Lemma 2.7 we can assume that $L \neq B_3(2), D_4(2)$, and so $k_{2n}(q) \neq 1$). By hypothesis $p \in \pi(K)$ and then Lemma 2.2(2) implies that $k_{2n}(q)$ is coprime to $|K| \cdot |\overline{G}/S|$. Thus in all cases $k_{2n}(q)$ is coprime to $|K| \cdot |\overline{G}/S|$ and so lies in $\omega(S)$.

Let P be a Sylow p-subgroup of K and N be its normalizer in G. Among prime divisors of $k_{2n}(q)$ we choose a prime r that satisfies not only the condition $e(r, p^\alpha) = 2n$ but also a stronger condition $e(r, p) = 2n\alpha$. In other words, $r = r_{2n\alpha}(p)$. By the Frattini argument $\overline{G} = G/K \simeq N/N \cap K$, hence G contains an element x of order r normalizing P. Since r is not adjacent to p, x induces a automorphism of P, which acts fixed-point-freely. Thus $|K|_p = p^{2n\alpha\gamma} = q^{2n\gamma}$ for a positive integer γ.

(2) Suppose that p divides $|\overline{G}/S|$. Reasoning as in (1), it is easy to establish that $k_{2n}(q)$ lies in $\omega(S)$ and is coprime to $|K| \cdot |\overline{G}/S|$. Since the orders of L and G coincide, a cyclic subgroup H of order $k_{2n}(q)$ is a Hall subgroup of S. Since every prime divisor of $k_{2n}(q)$ is

non-adjacent to p, a Sylow p-subgroup A of the normalizer N of H in $\overline{G}$ acts on H freely. Then $H : A$ is a Frobenius group with kernel H and complement A, and hence A is cyclic if p is odd and either cyclic or a general quaternion group if $p = 2$. By the Frattini argument $N/N \cap S \simeq \overline{G}/S$. So a Sylow p-subgroup of $\overline{G}/S$ is isomorphic to a section of A. Thus it is either cyclic or a general quaternion group. Obviously, the p-period of $\overline{G}/S$ does not exceed the p-period of G and hence the p-period of L as well.

Let p divide the order of K and x be an element of A of order p^κ. By the Frattini argument the normalizer of a Sylow p-subgroup P of K includes a Frobenius group isomorphic to $H : \langle x \rangle$. Considering the action of this Frobenius group on the factor group $P/\Phi(P)$ of P by its Frattini subgroup and applying Lemma 1.8, we infer that G contains an element of order $p^{\kappa+1}$. This proves the last assertion of the lemma.

LEMMA 3.2. *Let $L \in \{B_3(q), C_3(q), D_4(q)\}$, where q is a power of a prime p and $q > 3$. Suppose that p divides the order of the soluble radical K of G. Then $k_3(q)k_4(q)k_6(q)$ is coprime to $|K| \cdot |\overline{G}/S|$.*

Proof. Let L be one of the groups $B_3(q)$, $C_3(q)$, $D_4(q)$. For every prime divisors $r_3 = r_3(q)$ and $r_6 = r_6(q)$ the set $\{p, r_3, r_6\}$ is a coclique in $GK(L)$. By our assumption, $p \in \pi(K)$. It follows by Lemma 2.2(2) that the numbers $k_3 = k_3(q) = (q^2 + q + 1)/(3, q - 1)$ and $k_6 = k_6(q) = (q^2 - q + 1)/(3, q + 1)$ lie in $\omega(S)$ and are coprime to $|K| \cdot |\overline{G}/S|$. Denote cyclic subgroups of S of orders k_3 and k_6 by H_1 and H_2 respectively. Observe that the equality of the orders of G and L implies that H_1 and H_2 are Hall subgroups of S. By Lemma 3.1 the order of a Sylow p-subgroup P of K is equal to q^6 if $L = B_3(q)$ or $L = C_3(q)$ and equal to q^6 or q^{12} if $L = D_4(q)$.

Let r be an arbitrary prime divisor of $k_4(q) = (q^2 + 1)/(2, q - 1)$. Note that $r > 3$. Suppose that r divides $|\overline{G}/S|$. Then the normalizers N_1, N_2 of H_1, H_2 in $\overline{G}$ contain elements of order r. Since r is non-adjacent to divisors of k_3 and k_6 in $GK(L)$, $\overline{G}$ includes Frobenius groups with kernels of orders k_3 and k_6 and complements of order r. Hence r divides $k_3 - 1$ and $k_6 - 1$. At least one of the numbers $q^2 + q + 1$ and $q^2 - q + 1$ is not divisible by 3, so one of the numbers $q^2 + q$ and $q^2 - q$ must be a multiple of r. On the other hand, $(q^2 \pm q, (q^2 + 1)/(2, q - 1)) = (q \pm 1, (q^2 + 1)/(2, q - 1)) = 1$; a contradiction.

Now we prove that $(k_4(q), |K|) = 1$ by exploiting the following lemma.

LEMMA 3.3. *Let q be a natural number, $q > 3$, r be a prime and r^δ divide $k_4(q) = (q^2+1)/(2, q-1)$ for a natural number δ. Then a cyclic subgroup of order k, where $k = k_3(q) = (q^2+q+1)/(3, q-1)$ or $k = k_6(q) = (q^2-q+1)/(3, q+1)$, cannot act freely on a group of order r^δ.*

Proof. Otherwise, $r^\delta - 1$ is divisible by k and, in particular, $k < r^\delta$. If $r^\delta \neq (q^2+1)/(2, q-1)$ then, since $((q^2+1)/(2, q-1), 6) = 1$ and $q > 3$, we have $r^\delta \leqslant k_4(q)/5 \leqslant \min\{k_3(q), k_6(q)\} \leqslant k$; a contradiction. Thus $r^\delta = k_4(q)$ and so k divides $k_4(q) - 1$, which is equal to q^2 if q is even and to $(q^2-1)/2$ if q is odd. Both cases are impossible, since $(q^2, q^2 \pm q + 1) = 1$ and $(q^2 - 1, q^2 \pm q + 1) = (q^2 - 1, 3)$. The lemma is proved.

We return to the proof of Lemma 3.2. Suppose that a prime divisor r of $k_4(q)$ divides the order of K. Let r^δ be the largest power of r that divides $(q^2+1)/(2, q-1)$. Then the r-period of L is equal to r^δ and the order of a Sylow r-subgroup of L is equal to r^δ if $L = B_3(q), C_3(q)$ and to $r^{2\delta}$ if $L = D_4(q)$. Let V_1, V_2 be normal subgroups of G, $V_1 \leqslant V_2 \leqslant K$, $V = V_1/V_2$ be a chief factor of G and $|V| = r^\gamma$. Since S includes cyclic subgroups H_1 and H_2 of orders $k_3(q)$ and $k_6(q)$ respectively, $(|K|, k_3(q)k_6(q)) = 1$ and r is adjacent to none of the prime divisors of $k_3(q)k_6(q)$, it follows that H_1 and H_2 acts freely on V by conjugation. By Lemma 3.3 we have $\gamma \geqslant \delta + 1$. This is immediately yields that $L = D_4(q)$ and V is the unique chief r-factor of K.

If $\delta = 1$ then V is isomorphic to a Sylow r-subgroup of G, which has order r^2, and so r does not divide $|\overline{G}|$. A simple nonabelian group S is a section of $\operatorname{Aut} V = GL_2(r)$ and is not isomorphic to Alt_5. Therefore r must divide the order of S; a contradiction.

Thus $\delta > 1$. In particular, $q \neq 4$ since otherwise $k_4(q) = q^2 + 1 = 17$. Since V is elementary abelian, $\overline{G}$ contains an element of order $r^{\delta-1}$. Therefore $r^{2\delta}/r^{\delta-1} \geqslant |V| \geqslant r^{\delta+1}$. Hence $|V| = r^{\delta+1}$. The subgroups H_1, H_2 acts freely on V, so $|V| - 1 = r^{\delta+1} - 1$ is divisible by the least common multiple of $k_3(q)$ and $k_6(q)$, which is equal to $(q^4+q^2+1)/(3, q^2-1)$. This contradicts the chain of inequalities $|V| \leqslant ((q^2+1)/(2, q-1))^{(3/2)} < (q^4+q^2+1)/3$ valid for $q \geqslant 5$.

Thus $(k_4(q)k_3(q)k_6(q), |K| \cdot |\overline{G}/S|) = 1$. The lemma is proved.

Proposition 3.2. *Let q be a power of a prime p, L be one of the simple groups $B_n(q)$, where $n \geqslant 2$ and $(n,q) \neq (2,3)$, $C_n(q)$, where $n \geqslant 3$, and $D_n(q)$, where n is even and $n \geqslant 4$. Let G be a finite group with $\omega(G) = \omega(L)$ and $|G| = |L|$. Suppose that the unique nonabelian composition factor S of G is isomorphic to a group of Lie type over a field of characteristic p. Then $L \simeq S = G$.*

Proof. Since the spectra of L and G coincide, we can apply Lemma 2.6.

Let $L = D_n(q)$, where n is even and $n \geqslant 4$. It follows by Lemma 2.4(2),(4) that $S \in \{B_{n-1}(q), C_{n-1}(q), D_n(q)\}$, and if $n = 4$ then alongside the listed possibilities, S can be isomorphic to one of the groups $A_1(q^3)$, $G_2(q)$. Suppose that $S \in \{B_{n-1}(q), C_{n-1}(q)\}$. Then $|L|_p = q^{n(n-1)}$ and $|S|_p = q^{(n-1)^2}$. Furthermore, $|\overline{G}/S|_p \leqslant |\operatorname{Out} S|_p \leqslant \log_p q$. Therefore $|\overline{G}/S|_p \leqslant q$ and hence $|\overline{G}|_p < |L|_p$. So p divides the order of K. It follows by Lemma 3.1 that $|K|_p \geqslant q^{2(n-1)}$, whence $|G|_p \geqslant |K|_p \cdot |S|_p \geqslant q^{(n+1)(n-1)} > q^{n(n-1)} = |L|_p$; a contradiction. It remains therefore to consider the cases when $n = 4$ and S is one of the groups $A_1(q^3)$, $G_2(q)$.

By Lemma 2.7 we can assume that $q > 3$. Estimating the p-part of $|\overline{G}/S|$ in terms of the p-period of L by Lemma 3.1, we derive the inequality $|\overline{G}/S|_p \leqslant q^2$. Since $|A_1(q^3)|_p = q^3$ and $|G_2(q)|_p = q^6$, if $S \simeq A_1(q^3)$ then $q^3 \leqslant |\overline{G}|_p \leqslant q^5$ and if $S \simeq G_2(q)$ then $q^6 \leqslant |\overline{G}|_p \leqslant q^8$. In both cases $|\overline{G}|_p < q^{12} = |L|_p$. So p divides the order of K. It follows by Lemma 3.2 that $k_4(q) = (q^2+1)/(2, q-1)$ must divide the order of S. But $|S| = q^3(q^6-1)/(2,q-1)$ for $S \simeq A_1(q^3)$ and $|S| = q^6(q^2-1)(q^6-1)$ for $S \simeq G_2(q)$, so $(|S|, k_4(q)) = 1$; a contradiction. Thus $S \simeq D_n(q)$ and hence $L \simeq G$.

Let $L = B_2(q)$ and $S \simeq A_1(q^2)$. Since $q > 3$, Lemma 3.1 and [14, Prop. 0.5] imply that $|\overline{G}/S|_p \leqslant q$. Therefore $|\overline{G}|_p \leqslant |S|_p \cdot |\overline{G}/S|_p \leqslant q^3$. Thus p divides the order of K. It follows by Lemma 3.1 that $q^4 = |L|_p$ divides the order K, which is not the case since the order of S is divided by p as well.

Let $L \in \{B_n(q), C_n(q)\}$, $n \geqslant 3$. The groups $B_n(q)$ and $C_n(q)$ for $n \geqslant 3$ have the same orders. Hence if $S \in \{B_n(q), C_n(q)\}$ then $G = S$. On the other hand, it is shown in [35, 36] that $\omega(B_n(q)) \neq \omega(C_n(q))$ provided that $B_n(q) \not\simeq C_n(q)$. Thus if $S \in \{B_n(q), C_n(q)\}$, then $L \simeq S = G$.

Suppose now that $n \geqslant 4$ and $S \simeq {}^2D_n(q)$. Then $|L|_p = q^{n^2}$, $|S|_p = q^{n(n-1)}$. Furthermore, $|\overline{G}/S|_p \leqslant |\operatorname{Out} S|_p \leqslant 2\log_p q$. Hence $|\overline{G}/S|_p \leqslant q$ and so $|\overline{G}|_p < |L|_p$. Thus p divides the order of K. It follows by Lemma 3.1 that $|K|_p \geqslant q^{2n}$ and therefore $|G|_p \geqslant |K|_p \cdot |S|_p \geqslant q^{n(n+1)} > |L|_p$; a contradiction.

Thus to complete the prove, it remains to eliminate the cases when $n = 3$ and $S \in \{A_1(q^3), D_4(q), G_2(q)\}$. If $S \simeq D_4(q)$ then $|G| \geqslant |S| > |L|$, which is impossible. Therefore $S \in \{A_1(q^3), G_2(q)\}$ and by Lemma 2.7 we can assume that $q > 3$. We have $|L|_p = q^9$. Reasoning similarly to the case when $L = D_4(q)$, we derive that $|\overline{G}/S|_p \leqslant q^2$ and so $|\overline{G}|_p < |L|_p$. Thus p divides $|K|$. It follows by Lemma 3.2 that $k_4(q) = (q^2+1)/(2, q-1)$ must divide the order of S, which is not the case. The proposition is proved.

§ 4. Proof of the theorem: Cross-characteristic case

Let L be one the simple groups $B_n(q)$, where $n \geqslant 2$, $(n, q) \neq (2, 3)$, $C_n(q)$, where $n \geqslant 3$, and $D_n(q)$, where $n \geqslant 4$ is even, q be a power of a prime p. Let G be a finite group with $\omega(G) = \omega(L)$ and $|G| = |L|$, S be the unique nonabelian composition factor of G according to Lemma 2.3. By results of the previous section, we can assume that S is a group of Lie type over a field of characteristic not equal to p. In particular, Lemma 2.7 implies that $L \notin \{B_3(q), C_3(q), B_4(q), C_4(q), D_4(q) \mid q = 2, 3\}$.

Let S be a group of Lie type of rank m over a field of order u and characteristic v, where $v \neq p$. Lemma 2.9 asserts that S contains an element whose order is at least a sufficiently large number $h(q)$. It follows by Lemma 1.3 that $h(q)$ does not exceed the number $v/(v-1) \cdot u^{m/2}$ if S is a Ree or Suzuki group; the number $(u+1)/(u-1) \cdot u^m$ if $S \simeq E_8(u)$; and the number $u/(u-1) \cdot u^m$ in other cases. The number u^m can be expressed in terms of the order of a Sylow v-subgroup V of S. The order of V does not exceed the order of a Sylow v-subgroup of G, and so the order of a Sylow v-subgroup of L as well, which is in its turn can be estimated in terms of $f(q)$ and n according to Lemma 1.6. We show that the chain of these estimates results in a contradiction if n is sufficiently large. And if n is small it enables us to substantially narrow the scope of possibilities for S.

Proposition 4.1. *Let L be one of the groups $B_n(q), C_n(q)$, where $n \geqslant 7$, and $D_n(q)$,*

where $n \geqslant 8$ is even; q be a power of a prime p; G be a finite group with $\omega(G) = \omega(L)$ and $|G| = |L|$. Then the unique nonabelian composition factor S of G is not a group of Lie type over a field of characteristic other than p.

Proof. Assume the opposite. By Lemma 2.9, S contains an element whose order is bounded from below by a polynomial $h(q)$ in q of degree 6.

Let V be a Sylow v-subgroup of S. Let $\sigma(m) = \sigma(m, S)$ be as in Lemma 1.4. The equality $|G| = |L|$ and Lemma 1.6 implies that $|V|$ is at most $f(q)^{3n/2}$. Therefore

$$u^{m/2} \leqslant f(q)^{3n/2\sigma(m)} \tag{4.1}$$

for Ree and Suzuki groups,

$$u^{m} \leqslant f(q)^{3n/2\sigma(m)} \tag{4.2}$$

for other groups. By Lemma 1.3 and the inequalities $(u+1)/(u-1) \leqslant (v+1)/(v-1)$ and $u/(u-1) \leqslant v/(v-1)$, it follows from (4.1) and (4.2) that

$$h(q) \leqslant Cf(q)^{3n/2\sigma(m)}, \tag{4.3}$$

where $C = v/(v-1)$ for $S \not\simeq E_8(u)$ and $C = (v+1)/(v-1)$ for $S \simeq E_8(u)$.

We show that the ratio $n/\sigma(m)$ is at most 2. Then the left-hand side of (4.3) contains a polynomial in q of degree 6, while the right-hand side contains a polynomial in q of degree 3. Thus we derive a contradiction for all sufficiently large q. The case of small q will be handled separately.

To estimate the ratio $n/\sigma(m)$, we use Lemma 2.2(2) and the information on cocliques of prime graphs of finite simple groups from [29, 34].

Since $t(B_n(q)) = t(C_n(q)) = [(3n+5)/4] \geqslant 6$ for $n \geqslant 7$ and $t(D_n(q)) = [(3n+1)/4] \geqslant 6$ for even $n \geqslant 8$, it follows by Lemma 2.2 that $t(S) \geqslant t(L) - 1 \geqslant 5$. In particular, S is either a classical group or a group of one of the types E_m^{ε}, F_4, ${}^2F_4$, and ${}^2G_2$. Observe that $S \not\simeq {}^2G_2(u)$ since every coclique of $GK({}^2G_2(u))$ of size 5 contains the vertex 3, while the prime graph of L always includes a coclique of size 6 and without the vertex 3. Furthermore, S is other than ${}^2D_5(2)$, $F_4(2)$ and ${}^2F_4(8)$ because $t({}^2D_5(2)) = 3$ and $t(F_4(2)) = t({}^2F_4(8)) = 4$.

Suppose that $S \simeq A_m^\varepsilon(u)$. It follows from $t(S) \geqslant 5$ that $m \geqslant 8$. For such m, the independent number of the prime graph of S is equal to $[(m+2)/2]$. Therefore $(m+2)/2 \geqslant [(3n+1)/4]-1 \geqslant (3n-2)/4-1$ and so $n \leqslant (2m+10)/3$. On the other hand, by Lemma 1.4, we have $\sigma(m) = (m+1)/2$. Thus $n/\sigma(m) \leqslant (4m+20)/(3m+3) = 4/3 + 16/(3m+3) \leqslant 4/3 + 16/27 < 2$.

Suppose that S is isomorphic to one of the groups $B_m(u)$, $C_m(u)$, $D_m^\varepsilon(u)$. By $t(S) \geqslant 5$, the rank m is at least 5. Since $t(S) \leqslant [(3m+5)/4]$, it follows that $(3m+5)/4 \geqslant [(3n+1)/4]-1 \geqslant (3n-2)/4-1$. Then $n \leqslant m + 11/3$, i. e., $n \leqslant m+3$. By Lemma 1.4, $\sigma(m) \geqslant m-1$. Therefore $n/\sigma(m) \leqslant (m+3)/(m-1) = 1 + 4/(m-1) \leqslant 2$.

If $S \simeq E_8(u)$ then $t(S) = 12$. Thus $t(L) \leqslant 13$ and so $n \leqslant 18$. Taking into account that $\sigma(m) = 15$, we obtain that $n/\sigma(m) \leqslant 6/5$.

If $S \simeq E_7(u)$ then $t(S) = 8$ and so $n \leqslant 12$. Since $\sigma(m) = 9$, the inequality $n/\sigma(m) \leqslant 4/3$ holds.

If $S \simeq E_6^\varepsilon(u)$, $S \simeq F_4(u)$ or $S \simeq {}^2F_4(u)$ then $t(S) \leqslant 5$, and so $n \leqslant 8$. For all these groups, $\sigma(m) = 6$. Therefore $n/\sigma(m) \leqslant 4/3$.

Thus in all cases under consideration except when $S \simeq E_8(u)$, (4.3) yields $h(q) \leqslant v/(v-1)\cdot f(q)^3$, while in the case $S \simeq E_8(u)$, it yields $h(q) \leqslant (v+1)/(v-1)\cdot f(q)^{9/5}$. We show that the second inequality is stronger than the first one. Indeed, $(v+1)f(q)^{9/5}/(vf(q)^3) = (v+1)/(vf(q)^{6/5}) \leqslant 3/(2f(q)) < 1$ and so the right-hand side of the second inequality is less than the corresponding side of the first one. Hence for all groups S, we have

$$h(q) \leqslant \frac{v}{v-1} f(q)^3. \tag{4.4}$$

LEMMA 4.1. *Let q be a prime power, v be a prime coprime to q, $f(q)$ be the function defined in Lemma* 1.6*, and $h(q)$ be the function defined in Lemma* 2.9(1)*. If $h(q) \leqslant v/(v-1)\cdot f(q)^3$, then $q = 3$ and $v = 2$.*

Proof. Since $h(q) \geqslant (q^7+1)/7(q+1)$, $v/(v-1) \leqslant 2$ and $f(q) \leqslant 2(q+1)$, the inequality in the statement yields

$$q^7 + 1 \leqslant 7(2(q+1))^4,$$

and hence $q \leqslant 5$. If $q \leqslant 5$ then $7 \nmid q^2 - 1$, so $h(q) = (q^7+1)/(q+1)$, and the inequality in

the statement yields

$$q^7 + 1 \leqslant (2(q+1))^4,$$

whence $q \leqslant 3$.

Let $q = 3$ and $v > 3$. Then $f(q) = q = 3$, therefore, $3^7 + 1 \leqslant 2 \cdot 3^3(3+1)$, and so $3^4 \leqslant 2(3+1)$, but this is false. Thus if $q = 3$ then $v = 2$.

Let $q = 2$. Then $v \geqslant 3$ and so $v/(v-1) \leqslant 3/2$. Since $f(q) = q + 1 = 3$, we derive that $2^7 + 1 \leqslant 3/2 \cdot 3^4$, which is false. The lemma is proved.

By the above lemma, the inequality (4.4) leads to a contradiction provided that $(q, v) \neq (3, 2)$. Let $q = 3$ and $v = 2$. Then $f(q) = 8$. Let $S \simeq {}^2F_4(u)$. Then $u \geqslant 32$ and $n/\sigma(m) \leqslant 4/3$. On the other hand, it follows from (4.1) that $u^2 \leqslant f(q)^2 = 2^6$; a contradiction. Let S be isomorphic to one of the groups $E_8(u)$, $E_7(u)$, $E_6^\varepsilon(u)$ and $F_4(u)$. Then $n/\sigma(m) \leqslant 4/3$, and the inequality (4.2) implies that $u^m \leqslant f(q)^2 = 2^6$. Since $S \not\simeq F_4(2)$, we have $S \simeq E_6^\varepsilon(2)$, and so $n \leqslant 8$. The group $E_6(2)$ contains an element of order 31 and the group ${}^2E_6(2)$ contains an element of order 19. Since $e(31, 3) = 15$ and $e(19, 3) = 18$, there are no elements of orders 31 and 19 in L; a contradiction. Let S be a classical group. Recall that if S is a linear or unitary group then $m \geqslant 8$, and if S is a symplectic or orthogonal group then $m \geqslant 5$. Since $n/\sigma(m) \leqslant 2$, it follows from (4.2) that $u^m \leqslant f(q)^3 = 2^9$. Therefore $u = 2$ and $m \leqslant 9$, so $n \leqslant 12$. Since $S \not\simeq {}^2D_5(2)$, S contains an element of order $r_5(2) = 31$ or an element of order $r_{14}(2) = 43$ but L does not contain elements of those orders; a contradiction. The proposition is proved.

We proceed to the case when $n \leqslant 6$. Now $h(q)$ is a polynomial in q of forth or second degree depending on L, and we need more accurate estimate of the order of a Sylow v-subgroup of L. By Lemma 1.6, its order is at most $f(q)^n \cdot v^{\delta(n,v)}$, where $\delta(n, v) = \sum_{l=1}^{\infty}[n/v^l]$. Therefore

$$u^{m/2} \leqslant v^{\delta(n,v)/\sigma(m)} f(q)^{n/\sigma(m)} \tag{4.5}$$

for Ree and Suzuki groups,

$$u^m \leqslant v^{\delta(n,v)/\sigma(m)} f(q)^{n/\sigma(m)} \tag{4.6}$$

for other groups, and in either case

$$h(q) \leqslant Cv^{\delta(n,v)/\sigma(m)} f(q)^{n/\sigma(m)}, \tag{4.7}$$

where, as above, $C = v/(v-1)$ for $S \not\simeq E_8(u)$ and $C = (v+1)/(v-1)$ for $S \simeq E_8(u)$.

If the ratio $n/\sigma(m)$ is less than the degree of $h(q)$, the inequality (4.7) holds true only for finitely many values of q. Thus either $\sigma(m)$ is small as compared to n or q takes finitely many values.

LEMMA 4.2. *Let q be a prime power, v be a prime coprime to q, $f(q)$ be the function defined in Lemma* 1.6*, and $h(q) = (q^4+1)/2$.*

(1) *If $h(q) \leqslant v^{\delta(6,v)/2} \cdot v/(v-1) \cdot a(q)^3$ then either $q = 2, 4, 8$, or $v > 2$ and $q = 3, 5, 7$, or $v = 2$ and $q = 3, 5, 7, 9, 11, 13, 17, 31, 127$.*

(2) *If $h(q) \leqslant v^{2\delta(6,v)/5} \cdot v/(v-1) \cdot f(q)^{12/5}$ then either $q = 2, 4$, or $v = 2$ and $q = 3, 5, 7, 9$.*

(3) *If $h(q) \leqslant v^{\delta(6,v)/3} \cdot v/(v-1) \cdot f(q)^2$ or $h(q) \leqslant v^{\delta(4,v)/2} \cdot v/(v-1) \cdot f(q)^2$ then either $q = 2$, or $v = 2$ and $q = 3, 5, 7$.*

Proof. (1) Since $v^{\delta(6,v)/2} \leqslant 4$, $v/(v-1) \leqslant 2$ and $f(q) \leqslant 2(q+1)$, the inequality in the statement implies that $q^4 + 1 \leqslant 16(2(q+1))^3$, whence $q \leqslant 128$.

Suppose that q is not equal to 9 and distinct from the Mersenne and Fermat primes. Then neither $q+1$ nor $q-1$ is a power of 2, so $f(q) \leqslant q+1$ and $q^4 + 1 \leqslant 16(q+1)^3$, and hence $q \leqslant 17$. Thus either $q = 127$ or $q = 31$ or $q \leqslant 17$.

Let $q = 2, 4, 8, 16$. Then $v \geqslant 3$, and so $v^{\delta(6,v)/2} \leqslant 3$, $v/(v-1) \leqslant 3/2$ and $f(q) \leqslant q+1$. We have $q^4 + 1 \leqslant 9(q+1)^3$, which is false for $q = 16$. Thus $q = 2, 4, 8$.

Let $q = 3, 5, 7, 9, 11, 13, 17, 31, 127$ and $v > 2$. Then $v^{\delta(6,v)/2} \leqslant 3$, $v/(v-1) \leqslant 3/2$ and $f(q) \leqslant q$. We have $q^4 + 1 \leqslant 9q^3$, which is false for $q > 7$. Thus $q = 3, 5, 7$.

(2) The inequality in (2) is stronger than that in (1), so the conclusion of (1) holds.

Let $v > 2$ and $q = 2, 3, 4, 5, 7, 8$. Then $v^{2\delta(6,v)/5} \leqslant 3^{4/5}$, $v/(v-1) \leqslant 3/2$. Since $f(q) \leqslant q+1$ for even q and $f(q) \leqslant q$ for odd q, we deduce that even numbers must satisfy the inequality $q^4 + 1 \leqslant 3^{4/5} \cdot 3(q+1)^{12/5}$, while odd ones must satisfy $q^4 + 1 \leqslant 3^{4/5} \cdot 3q^{12/5}$. The first inequality is false for $q = 8$ and the second one is false for $q = 5, 7$, therefore $q = 2, 3, 4$. Let $q = 3$. Then $v \geqslant 5$, so $v^{2\delta(6,v)/5} \leqslant 5^{2/5}$, $v/(v-1) \leqslant 5/4$, and hence $2(q^4+1) \leqslant 5^{2/5} \cdot 5q^{12/5}$,

but this is false for $q = 3$. Thus $q = 2, 4$.

Let $v = 2$. Then $v^{2\delta(6,v)/5} = 2^{8/5}$, $v/(v-1) = 2$ and $f(q) = (q^2-1)_2$, so the inequality $q^4 + 1 \leqslant 2^{8/5} \cdot 4((q^2-1)_2)^{12/5}$ must be true. A direct check shows that it is false for $q = 11, 13, 17, 31, 127$.

(3) Both inequalities in (3) are stronger than the inequality in (2), so the conclusion of (2) holds.

Let $q = 2, 4$. Then $v^{\delta(4,v)/2} \leqslant v^{\delta(6,v)/3} \leqslant 3^{2/3}$, $v/(v-1) \leqslant 3/2$ and $f(q) \leqslant q+1$. We derive that $q^4 + 1 \leqslant 3^{2/3} \cdot 3(q+1)^2$, which is false when $q = 4$.

Let $v = 2$. Then $v^{\delta(6,v)/3} \leqslant v^{\delta(4,v)/2} = 2^{3/2}$, $v/(v-1) = 2$ and $f(q) = (q^2-1)_2$. It follows that $q^4 + 1 \leqslant 2^{3/2} \cdot 4((q^2-1)_2)^2$, whence $q \leqslant 7$. The lemma is proved.

Proposition 4.2. *Let L be one of the groups $B_4(q)$, $C_4(q)$, $B_5(q)$, $C_5(q)$, $B_6(q)$, $C_6(q)$, $D_6(q)$, where q is a power of a prime p, and G be a finite group with $\omega(G) = \omega(L)$ and $|G| = |L|$. Then the unique nonabelian composition factor S of G is not a group of Lie type over a field of characteristic other than to p.*

Proof. Assume the opposite. By Lemma 2.9, $h(q) = (q^4+1)/2$.

I. Let L be one of the groups $B_6(q)$, $C_6(q)$, $B_5(q)$, $C_5(q)$, and $L \neq B_5(2)$. Then $t(L) = 5$. Moreover, $GK(L)$ contains a coclique of size 5a and without the vertices 2 and 3. It follows that $GK(S) \setminus \{2, 3\}$ must contain a coclique of size 4. Therefore S is distinct from ${}^2B_2(u)$, $G_2(u)$, $B_2(u)$, $B_3(u)$, $C_3(u)$, $D_4(u)$, ${}^3D_4(u)$ and $A_m^{\varepsilon}(u)$, where $m \leqslant 5$, and from $B_4(2)$, ${}^2D_4(2)$, ${}^2D_5(2)$, $A_6(2)$, $A_7(2)$ as well. In particular, $\sigma(m) \geqslant 3$, so $n/\sigma(m) \leqslant 2$ and $v^{\delta(n,v)/\sigma(m)} \leqslant v^{\delta(6,v)/3}$. Therefore if $S \not\simeq E_8(u)$ then (4.7) yields $h(q) \leqslant v/(v-1) \cdot v^{\delta(6,v)/3} f(q)^2$, while if $S \simeq E_8(u)$ it yields $h(q) \leqslant (v+1)/(v-1) \cdot v^{\delta(6,v)/15} f(q)^{2/5}$. It easy to verify that the second inequality if stronger than the first one, so in either case

$$h(q) \leqslant \frac{v}{v-1} v^{\delta(6,v)/3} f(q)^2.$$

By Lemma 4.2(3), either $q = 2$, or $v = 2$ and $q = 3, 5, 7$.

Let $q = 2$. Then $f(q) \leqslant 3$, and it follows from (4.5), (4.6) that $u^{m/2} \leqslant 2^{4/3} \cdot 9$ for Ree and Suzuki groups, and that $u^m \leqslant 2^{4/3} \cdot 9$ for other groups. Since $m > 1$, we have $u = 3$ and $m = 2$. This is impossible in view of the restrictions mentioned above and the fact that

${}^2G_2(3)$ is not simple.

Let $v = 2$ and $q = 3, 5, 7$. If $S \simeq {}^2F_4(u)$, where $u \geqslant 8$, then it follows from (4.5) that $2^6 \leqslant u^2 \leqslant 2^{\delta(6,2)/3}(q^2-1)_2^2 \leqslant 2^{4/3}2^8$, whence $u = 8$ and $S \simeq {}^2F_4(8)$. For other groups, (4.6) yields $u^m \leqslant 2^{4/3}2^8$. Since $m > 3$, we infer that either $u = 2$ and $4 \leqslant m \leqslant 9$, or $u = 4$ and $m = 4$. In the last case, in view of the restriction mentioned above, S is isomorphic to one of the groups $B_4(4)$, ${}^2D_4(4)$ and $F_4(4)$.

Consider the primes non-adjacent to 2 in $GK(L)$. If $n = 6$ then they are the divisors of $k_{12}(q)$ and if $n = 5$ then they are the divisors of $k_5(q)$ for $q = 3, 7$ and divisors of $k_{10}(q)$ for $q = 5$. Therefore by Lemma 2.2, at least one of the numbers $k_{12}(3) = 73$, $k_5(3) = 121$, $k_{12}(5) = 521$, $k_{10}(5) = 601$, $k_{12}(7) = 13 \cdot 181$ and $k_5(7) = 2801$ lies in $\omega(S)$; in particular, $S \notin \{{}^2F_4(8), B_4(4), {}^2D_4(4), F_4(4)\}$. Thus $u = 2$. Since $e(73, 2) = 9$, $e(601, 2) = 25$ and $e(r, 2) \geqslant 110$ for $r \in \{121, 521, 13 \cdot 181, 2801\}$, of all these numbers, $\omega(S)$ can contain only 73, and so the order of S must be divisible by $2^9 - 1$. Hence $L \in \{B_6(3), C_6(3)\}$ and $S \in \{A_8(2), A_9(2), B_9(2), D_9(2), E_6(2), E_7(2), E_8(2)\}$. But then $17 \in \omega(S) \setminus \omega(L)$; a contradiction.

It remains to handle the case $L = B_5(2)$. In this case $\pi(L) = \{2, 3, 5, 7, 11, 17, 31\}$, the graph $GK(L)$ is disconnected, and $\{2, 31, 11\}$ and $\{7, 11, 17, 31\}$ are cocliques in $GK(L)$. Thus $11, 31 \in \pi(S) \subseteq \{2, 3, 5, 7, 11, 17, 31\}$, at least one of 7, 17 also lies in $\pi(S)$, and $GK(S)$ is disconnected. Using [37, Table 1], it is not hard to check that among groups of Lie type over a field of an odd characteristic, there is no group with such properties.

II. Let $L = D_6(q)$. Then $t(L) = 4$. So $t(S) \geqslant 3$, and $S \not\simeq B_2(u)$. Suppose that S is distinct from the groups ${}^2B_2(u)$ and $A_m^\varepsilon(u)$, where $m \leqslant 4$. Then $\sigma(m) \geqslant 3$, and so $n/\sigma(m) \leqslant 2$. Similarly to the case I, it follows that $q = 2$, or $v = 2$ and $q = 3, 5, 7$.

Let $q = 2$. Then $f(q) \leqslant 3$, and it follows from (4.5), (4.6) that $u^{m/2} \leqslant 2^{4/3} \cdot 9$ for Ree and Suzuki groups, and that $u^m \leqslant 2^{4/3} \cdot 9$ for other groups. By assumption $m > 1$, therefore $u = 3$ and $m = 2$. Thus $S \simeq G_2(3)$. Since 31 is not adjacent to 2 in $GK(L)$, Lemma 2.2(3) implies that 31 must divide the order of S, but this is false.

Let $v = 2$ and $q = 3, 5, 7$. If $S \simeq {}^2F_4(u)$, where $u \geqslant 8$, then (4.5) yields $2^6 \leqslant u^2 \leqslant 2^{\delta(6,2)/3}((q^2-1)_2)^2 \leqslant 2^{4/3} \cdot 2^8$, whence $u = 8$ and $S \simeq {}^2F_4(8)$. For other groups, it follows

from (4.6) that $u^m \leqslant 2^{4/3} \cdot 2^8$. Therefore $u \leqslant 16$ and $2 \leqslant m \leqslant 9$. Depending on q, one of the numbers $k_5(3) = 121$, $k_{10}(5) = 521$, $k_5(7) = 2801$ must lie in $\omega(S)$, but this is false.

Suppose that $S \simeq {}^2B_2(u)$, where $u = 2^{2\beta+1} \geqslant 8$. Then $\sigma(m) = 2$, $n/\sigma(m) = 3$, and the inequality (4.7) turns into

$$h(q) \leqslant \frac{v}{v-1} v^{\delta(6,v)/2} f(q)^3.$$

By Lemma 4.2(1), $q = 3, 5, 7, 9, 11, 13, 17, 31, 127$. Assume that $q = 3, 5, 11, 13$. Then $f(q) = 8$, and (4.5) yields $u \leqslant 4 \cdot 8^3 = 2^{11}$. On the other hand, by Lemma 2.2(3), one of the numbers $k_5(3) = 121$, $k_{10}(5) = 521$, $k_5(11) = 3221$, $k_{10}(13) = 11 \cdot 2411$ lies in $\omega(S)$. For the groups $S \simeq {}^2B_2(u)$, where $u \leqslant 2^{11}$, this is false. For $q = 7, 9, 17, 31, 121$ we derive a contradiction in a similar way.

Suppose that $S \simeq A_4^{\varepsilon}(u)$. Then $\sigma(m) = 5/2$, $n/\sigma(m) = 12/5$, and the inequality (4.7) turns into

$$h(q) \leqslant \frac{v}{v-1} v^{2\delta(6,v)/5} f(q)^{12/5}.$$

By Lemma 4.2(2), we infer that either $q = 2, 4$, or $v = 2$ and $q = 3, 5, 7, 9$. Furthermore, the inequality (4.6), which turns into $u^5 \leqslant v^{\delta(6,v)/2} f(q)^3$, must be true. If $q = 2$ then $u \geqslant 3$, $f(q) \leqslant 3$, $v^{\delta(6,v)/2} \leqslant 3$, so $u^5 \leqslant 3^4$, which is impossible. If $q = 4$ then $u \geqslant 3$, $f(q) \leqslant 5$, $v^{\delta(6,v)/2} \leqslant 3$, therefore $u^5 \leqslant 3 \cdot 5^3$, whence $u = 3$. If $S \simeq A_4(3)$ then $121 \in \omega(S) \setminus \omega(L)$ and if $S \simeq {}^2A_4(3)$ then $61 \in \omega(S) \setminus \omega(L)$; a contradiction.

Thus $v = 2$ and $q = 3, 5, 7, 9$. Then $v^{\delta(6,v)/2} = 4$, $f(q) = (q^2-1)_2 \leqslant 16$, therefore $u^5 \leqslant 4 \cdot 16^3 = 2^{14}$, and so $u = 2$ or $u = 4$, i. e., $S \simeq A_4^{\varepsilon}(2)$ or $S \simeq A_4^{\varepsilon}(4)$. By Lemma 2.2(3), one of the numbers $k_5(3) = 121$, $k_{10}(5) = 521$, $k_5(7) = 2801$ and $k_{10}(9) = 1181$ must be in $\omega(S)$, but this is false.

Suppose that S is isomorphic to one of the groups $A_3^{\varepsilon}(u)$, $A_2^{\varepsilon}(u)$ and $A_1(u)$. Consider a coclique $\rho = \{r_{10}, r_8, r_5, r_6\}$ (or $\rho = \{r_{10}, r_8, r_5, r_3\}$ for $L = D_6(2)$) in $GK(L)$. Observe that this coclique does not contain 2 and 3. Since the size of every coclique of $GK(S)$ not containing 2 and 3 is at most three, some number from ρ, say r_i, divides $|K| \cdot |\overline{G}/S|$, and the other three do not divide $|K| \cdot |\overline{G}/S|$ and compose a coclique in $GK(S)$. Every coclique of size three in $GK(S)$ not containing 2 and 3 includes the characteristic v. Therefore $v \in \rho \setminus \{r_i\}$

and v does not divide $|K| \cdot |\overline{G}/S|$. Let $v = r_j$. Since this equality is valid for all primitive divisors of $q^j - 1$, we conclude that $k_j(q) = v^a$ and $k_j(q) \in \omega(S)$. Since $v = r_j > 3$, S does not contain an element of order v^2. So $k_j(q) = v$. On the other hand, $k_j(q)^3$ does not divide the order of L, and hence the order of a Sylow v-subgroup of S is at most v^2. Therefore $S \simeq A_1(u)$. Then every coclique of size three in $GK(S)$ is of the form $\{v, w_1, w_2\}$, where w_1, w_2 are divisors of $(u-1)/(2, u-1)$ and $(u+1)/(2, u-1)$ respectively. Therefore the set $\rho \setminus \{r_i, r_j\}$ contains a divisor of $(u-1)/(2, u-1)$. Denote it by r_k.

Assume that $r = r_i$ divides $|\overline{G}/S|$. Since $r > 3$, G contains a field automorphism of S of order r. The centralizer of such an automorphism in S always contains an element of order v, so $rv \in \omega(G)$; a contradiction since $rv = r_i r_j \notin \omega(L)$.

Suppose that r divides the order of K. Let R be a Sylow r-subgroup of K. By the Frattini argument, $N_G(R)/(N_G(R) \cap K) \simeq G/K \geq S$, so we can assume that R is normal in G. Put $\widetilde{G} = G/R$ and $\widetilde{K} = K/R$. Then $\widetilde{G}/\widetilde{K} \geq S$. In S and hence in $\widetilde{G}/\widetilde{K}$ as well, there is a Frobenius subgroup F with kernel of order u and cyclic complement of order r_k. Let $\widetilde{F}$ denote the preimage of F in $\widetilde{G}$. Since $|F| = ur_k$ is coprime to $|\widetilde{K}|$, it follows by the Shur — Zassenhaus theorem that $\widetilde{F}$ includes a Frobenius subgroup isomorphic to F. The kernel of this group acts on R freely since $rv \notin \omega(G)$. Then it follows by Lemma 1.8 that $rr_k \in \omega(G)$; a contradiction.

III. Let L be one of the groups $B_4(q)$ and $C_4(q)$, $q > 2$. If q is odd, then it follows by [20, Thm. 3] that the unique nonabelian composition factor of each finite group isospectral to L is isomorphic to L or to ${}^2D_4(q)$, so we can assume that $q \geqslant 4$ is even. Since $t(L) = 4$, we have that $t(S) \geqslant 3$, whence $S \not\simeq B_2(u)$. Furthermore, $GK(L)$ is disconnected. By the Gruenberg — Kegel theorem, $n_2(L) = q^4 + 1 \in \omega(S)$ and K is nilpotent.

Suppose that $S \not\simeq A_1(u), A_2^{\varepsilon}(u)$. Then $\sigma(m) \geqslant 2$. Therefore $n/\sigma(m) \leqslant 2$ and $v^{\delta(n,v)/\sigma(m)} \leqslant v^{\delta(4,v)/2}$. Handling, as above, the cases $S \not\simeq E_8(u)$ and $S \simeq E_8(u)$ individually, we derive from (4.7) the inequality

$$h(q) \leqslant \frac{v}{v-1} v^{\delta(4,v)/2} f(q)^2.$$

By Lemma 4.2(3), we conclude that $q \in \{2, 3, 5, 7\}$ but q is even and greater than 3; a

contradiction.

Suppose that $S \simeq A_2^{\varepsilon}(u)$ or $S \simeq A_1(u)$, where u is odd. Consider a coclique $\{r_8, r_6, r_4, r_3\}$ in $GK(L)$. It obviously does not contain 2 and 3. Since every coclique of $GK(S)$ not containing 2 and 3 consists of at most three vertices, one of the numbers r_6, r_4, r_3, say r_i, divides $|K| \cdot |\overline{G}/S|$, and the other two together with r_8 compose a coclique in $GK(S)$. Every coclique of size three in $GK(S)$ not containing 2 and 3 includes the characteristic v. Therefore $v \in \{r_8, r_6, r_4, r_3\}$ and v does not divide $|K| \cdot |\overline{G}/S|$. Let $v = r_j$. Since this equality is valid for all primitive divisors of $q^j - 1$, we infer that $k_j(q) = v^a$ and $k_j(q) \in \omega(S)$. Since $v = r_j > 3$, S does not contain an element of order v^2. Thus $k_j(q) = v$. On the other hand, $k_j(q)^3$ does not divide the order of L, and so the order of a Sylow v-subgroup of S is at most v^2. Furthermore, $S \simeq A_1(u)$. Then every coclique of size three in $GK(S)$ is of the form $\{v, w_1, w_2\}$, where w_1, w_2 are divisors of $(u-1)/2$ and $(u+1)/2$ respectively. Thus the set $\{r_8, r_6, r_4, r_3\} \setminus \{r_i, r_j\}$ contains a divisor of $(u-1)/2$.

Assume that $r = r_i$ divides $|\overline{G}/S|$. Since $r > 3$, it means that G contains a field automorphism of S of order r. The centralizer of such an automorphism in S always contains an element of order v, so $rv \in \omega(G)$; a contradiction since $rv = r_i r_j \notin \omega(L)$. Thus r divides the order of K. Since K is nilpotent and $GK(G)$ is disconnected, we can assume that K is an elementary abelian r-group, on which S acts such that $C_S(K) = 1$. There is a Frobenius subgroup with kernel of order u and cyclic complement of order $(u-1)/2$ in S, hence $r(u-1)/2 \in \omega(G)$; a contradiction. The proposition is proved.

LEMMA 4.3. *Let $q > 3$ be a prime power, v be a prime coprime to q, $f(q)$ be defined in Lemma* 1.6*, and $h(q) = (q^2+1)/2$. If*

$$h(q) \leqslant v^{\delta(4,v)/3} \cdot v/(v-1) \cdot f(q),$$

then either $q = 4$, or $v = 2$ and $q = 5, 7, 9$.

Proof. Since $v^{\delta(4,v)/3} \leqslant 2$, $v/(v-1) \leqslant 2$ and $f(q) \leqslant 2(q+1)$, the inequality in the statement yields $q^2 + 1 \leqslant 16(q+1)$, whence $q \leqslant 16$.

Suppose that $q \leqslant 16$ and $v > 2$. Then $v^{\delta(4,v)/3} \leqslant 3^{1/3} < 3/2$, $v/(v-1) \leqslant 3/2$ and $f(q) \leqslant q+1$. Therefore $2(q^2+1) < 9(q+1)$, and so $q \leqslant 5$. If $q = 5$ then $f(q) = q$, and the

inequality $50 = 2(q^2+1) < 9q = 45$ must be true; a contradiction. Thus $q = 4$.

Suppose that $q \leqslant 16$ and $v = 2$. If $q = 11, 13$ then $f(q) = 8$ and so $122 \leqslant q^2 + 1 \leqslant 8f(q) = 64$; a contradiction. Thus $q = 5, 7, 9$ and the lemma is proved.

Proposition 4.3. *Let L be one of the simple groups $B_2(q)$, $B_3(q)$, $C_3(q)$, $D_4(q)$, where q is a power of a prime p, $L \neq B_2(3)$, and G be a finite group with $\omega(G) = \omega(L)$ and $|G| = |L|$. Suppose that the unique nonabelian composition factor S of G is isomorphic to a group of Lie type over a field of a characteristic other that p.*

(1) *If $L = B_2(q)$, where $q > 3$, then S is isomorphic to one of the groups $A_1(u)$, $A_2^{\varepsilon}(u)$.*

(2) *If $L \in \{B_3(q), C_3(q)\}$ then S is isomorphic to one of the groups $A_m^{\varepsilon}(u)$, where $m \leqslant 4$, $B_2(u)$, and ${}^2B_2(u)$.*

(3) *If $L = D_4(q)$ then S is isomorphic to one of the groups $A_m^{\varepsilon}(u)$, where $m \leqslant 6$, $B_m(u)$ and $C_m(u)$, where $m \leqslant 3$, $D_4^{\varepsilon}(u)$, $G_2(u)$, ${}^2B_2(u)$, ${}^2G_2(u)$, and ${}^3D_4(u)$.*

Proof. In this case $h(q) = (q^2+1)/2$. Furthermore, by Lemma 2.7 we can assume that $q > 3$.

(1) Let $L = B_2(q)$, where $q > 3$. The graph $GK(L)$ has two connected components and $n_2(L) = (q^2+1)/(2, q-1)$. Thus the graph of S is disconnected and $(q^2+1)/(2, q-1) \in \omega(S)$.

Suppose that $S \not\simeq A_1(u), A_2^{\varepsilon}(u)$. Then $\sigma(m) \geqslant 2$ and (4.7) yields

$$h(q) \leqslant \frac{v}{v-1} v^{\delta(2,v)/2} f(q) \leqslant \frac{v}{v-1} v^{\delta(4,v)/3} f(q).$$

By Lemma 4.3, either $q = 4$, or $v = 2$ and $q = 5, 7, 9$. In fact, the first of the previous inequalities holds neither for $q = 4$ nor for $(v, q) = (2, 9)$.

Let $v = 2$ and $q = 5$. Then $(q^2+1)/2 = 13$ and $\pi(L) = \{2, 3, 5, 13\}$, so S is a group of Lie type over a field of characteristic 2 and $13 \in \pi(S) \subseteq \{2, 3, 5, 13\}$. It follows from [37, Table 1] that the only groups satisfying these conditions are ${}^2F_4(2)'$ and ${}^2A_2(4)$. But $S \not\simeq {}^2A_2(u)$ by assumption and S is distinct from the Tits group by Lemma 2.5.

Let $v = 2$ and $q = 7$. Then $(q^2+1)/2 = 25$ and $\pi(L) = \{2, 3, 5, 7\}$, therefore S is a group of Lie type over a field of characteristic 2, $\pi(S) \subseteq \{2, 3, 5, 7\}$ and $25 \in \omega(S)$. It follows from [37, табл. 1] that the only groups satisfying the first two conditions are $A_2(4)$, $A_3(2)$, $B_3(2)$, and $D_4(2)$. But none of these groups contains an element of order 25.

(2) Let $L = B_3(q)$ or $L = C_3(q)$, where $q > 3$. Suppose that the claim is false. Then $\sigma(m) \geqslant 3$ and (4.7) yields

$$h(q) \leqslant \frac{v}{v-1} v^{\delta(3,v)/3} f(q) \leqslant \frac{v}{v-1} v^{\delta(4,v)/3} f(q).$$

By Lemma 4.3, either $q = 4$, or $v = 2$ and $q = 5, 7, 9$.

Let $q = 4$. If $S \simeq {}^2G_2(u)$, where $u \geqslant 27$, then it follows from (4.5) that $27 \leqslant u \leqslant 3^{\delta(3,3)/4}(q+1)^{3/4} = 3^{1/4} \cdot 5^{3/4}$; a contradiction. For other groups, (4.6) yields $3^2 \leqslant u^m \leqslant 3^{1/4} \cdot 5^{3/4}$; a contradiction.

Let $v = 2$ and $q = 5, 7, 9$. If $S \simeq {}^2F_4(u)$, where $u \geqslant 8$, then it follows from (4.5) that $64 \leqslant u^2 \leqslant 2^{\delta(3,2)/4}((q^2-1)_2)^{3/4} \leqslant 2^{1/2} \cdot 8$; a contradiction. For other groups, (4.6) yields $2^2 \leqslant u^m \leqslant 2^{1/2} \cdot 8$, whence $u = 2$ and $m = 2, 3$. Therefore $S \simeq B_3(2)$. By Lemma 2.8, at least one of the numbers $k_4(q)$ and $k_3(q)$ lies in $\omega(S)$. This is false since $k_4(5) = k_3(9) = 13$, $k_3(5) = 31$, $k_4(7) = 25$, $k_3(7) = 19$ and $k_4(9) = 41$.

(3) Let $L = D_4(q)$ and $q > 3$. Suppose that the claim is false. Then $m \geqslant 4$ and $\sigma(m) \geqslant 4$. It follows from (4.7) that

$$h(q) \leqslant \frac{v}{v-1} v^{\delta(4,v)/4} f(q) \leqslant \frac{v}{v-1} v^{\delta(4,v)/3} f(q).$$

By Lemma 4.3, either $q = 4$, or $v = 2$ and $q = 5, 7, 9$.

Let $q = 4$. Then (4.6) yields $3^4 \leqslant u^m \leqslant 3^{\delta(4,3)/4}(q+1) = 3^{1/4} \cdot 5$; a contradiction.

Let $v = 2$ and $q = 5, 7, 9$. If $S \simeq {}^2F_4(u)$, where $u \geqslant 8$, then it follows from (4.5) that $64 \leqslant u^2 \leqslant 2^{\delta(4,2)/4}(q^2-1)_2 \leqslant 2^{3/4} \cdot 16$; a contradiction. For other groups (4.6) yields $u^m \leqslant 2^{3/4} \cdot 16$, whence $u = 2$ and $m = 4$. Therefore $S \simeq B_4(2)$ and $17 \in \omega(S)$, contrary to the fact that $17 \notin \omega(D_4(q))$ for $q = 5, 7, 9$. The proposition is proved.

§ 5. Proof of the theorem: Completion

As in the previous section, S is a finite group over a field of order $u = v^\beta$, where v is a prime other than p. Propositions 4.1–4.3 implies that it remains to handle the following possibilities:

(1) If $L = B_2(q)$, where $q > 3$, then S is isomorphic to one of the groups $A_1(u)$, $A_2^\varepsilon(u)$.

(2) If $L \in \{B_3(q), C_3(q)\}$ then S is isomorphic to one of the groups $A_m^\varepsilon(u)$, where $m \leqslant 4$, $B_2(u)$, and ${}^2B_2(u)$.

(3) If $L = D_4(q)$ then S is isomorphic to one of the groups $A_m^\varepsilon(u)$, where $m \leqslant 6$, $B_m(u)$ and $C_m(u)$, where $m \leqslant 3$, $D_4^\varepsilon(u)$, $G_2(u)$, ${}^2B_2(u)$, ${}^2G_2(u)$, and ${}^3D_4(u)$.

If $L = B_2(4)$ then $\pi(S) \subseteq \pi(L) = \{2, 3, 5, 17\}$. Furthermore, 17 is not adjacent to 2 in $GK(L)$, whence $17 \in \pi(S)$. It follows from [37, Table 1] that S must be isomorphic to $A_1(16)$ or $A_1(17)$. The first variant is impossible by Proposition 3.2. If $S \simeq A_1(17)$ then $9 \in \omega(S) \setminus \omega(L)$; a contradiction. Thus if $L = B_2(q)$ then we can assume that $q > 4$.

Suppose that p does not divide the order of the soluble radical K of G. We show that $|P|^3 > |S|$ for a Sylow p-subgroup P of S.

If $L = B_2(q)$ then $|L| = q^4(q^2-1)(q^4-1)/(2, q-1)$ and the p-period of L is equal to p for $p > 3$ and to p^2 for $p \in \{2, 3\}$. Since $q > 4$, by Lemma 3.1 we have $|\overline{G}/S|_p \leqslant q$. Therefore $|P|^2 \geqslant (q^3)^2 > (q^2-1)(q^4-1) \geqslant |S|/|P|$. Thus $|P|^3 > |S|$ as claimed.

If $L = B_3(q)$ or $L = C_3(q)$ then $|L| = q^9(q^2-1)(q^4-1)(q^6-1)/(2, q-1)$ and the p-period of L is at most q^2 (recall that $q > 3$). Therefore $|P|^2 \geqslant (q^7)^2 > (q^2-1)(q^4-1)(q^6-1) \geqslant |S|/|P|$, and we again derive the claimed inequality.

If $L = D_4(q)$ then $|L| = q^{12}(q^2-1)(q^4-1)^2(q^6-1)/(4, q^4-1)$ and the p-period is at most q^2 again. The chain of inequalities $|P|^2 \geqslant (q^{10})^2 > (q^2-1)(q^4-1)^2(q^6-1) \geqslant |S|/|P|$ yields $|P|^3 > |S|$.

Thus if p does not divide the order of K then by Lemma 1.7, S is isomorphic to either $A_1(u)$ or ${}^2A_2(3)$ for $p = 2$ or ${}^2A_4(2)$ for $p = 3$.

If $S \simeq {}^2A_2(3)$ then $p = 2$, and so $q \geqslant 4$. If $L = B_2(q)$ then an element of order $n_2(L) = q^2 + 1 \geqslant 17$ must lie in S, while the largest element of $\omega(S)$ is equal to 12. Similarly, if L is one of the groups $B_3(q)$, $C_3(q)$, $D_4(q)$ then elements of orders $k_3(q) = (q^2+q+1)/(3, q-1)$ and $k_6(q) = (q^2-q+1)/(3, q+1)$ lie in S. This is again a contradiction since $\max\{k_3(q), k_6(q)\} \geqslant q^2 - q + 1 \geqslant 13$.

If $S \simeq {}^2A_4(2)$ then $p = 3$, and so $q \geqslant 9$. Observe that the largest element order of S is equal to 18. Reasoning similarly to the previous paragraph, we derive a contradiction proving that S contains an element of order at least $(q^2+1)/2 \geqslant 41$ when $L = B_2(q)$ and

an element of order at least $q^2 - q + 1 \geqslant 73$ otherwise.

Suppose that S is isomorphic to $A_1(u)$. Since $p \neq v$, a Sylow p-subgroup P of S is cyclic. On the other hand, estimating the p-part of the order of $\overline{G}/S$ according to Lemma 3.1, we have $|P| \geqslant q^3 \geqslant p^3$ for $L = B_2(q)$ and $|P| \geqslant q^7 \geqslant p^7$ otherwise. This is a contradiction since $p^3 \notin \omega(L)$ for $L = B_2(q)$ and $p^7 \notin \omega(L)$ otherwise.

Thus p does not divide the order of K.

I. Suppose that $L = B_2(q)$. Lemma 3.1 implies that the order of a Sylow p-subgroup of K is equal to $q^{4\gamma}$, so it follows from $|L|_p = q^4$ that p does not divide the order of $\overline{G}$. Furthermore, $|K|_p = q^4$ and hence a Sylow p-subgroup P of K is elementary abelian. In particular, it follows that p cannot be equal to 2 and 3, for otherwise the p-period of L is larger than that of G.

Consider the remaining possibilities for S according to (1). Suppose that $S \simeq A_2^{\varepsilon}(u)$. Exploiting [26, Tables 1a-1c], we conclude that either $S \simeq A_2(2)$ and $n_2(L) = (q^2+1)/2 \in \{3, 7\}$, or $S \simeq A_2(4)$ and $n_2(L) = (q^2+1)/2 \in \{3, 5, 7\}$, or $n_2(L) = (q^2+1)/2 = n_2(S) = (u^2 + \varepsilon u + 1)/(3, u - \varepsilon 1)$. Since $q \geqslant 5$, the first two possibilities can be obviously dismissed. For brevity, set $a = n_2(L) = n_2(S)$. Clearly, the order of S divides the order of the factor group $\overline{G} = G/K$, and so $|S|$ divides $|L|_{p'} = (q^2-1)^2 \cdot (q^2+1)/2 = (q^2-1)^2 \cdot a$. Therefore $|S|/a \leqslant (q^2-1)^2 < (2a)^2$. On the other hand, $|S| = u^3(u^2-1)(u^3 - \varepsilon 1)/(3, u - \varepsilon 1)$, and so $|S|/a = u^3(u^2-1)(u - \varepsilon 1)$. If $u > 3$ then we derive an immediate contradiction since $|S|/a > 4(u^2+u+1)^2 \geqslant (2a)^2$. The group ${}^2A_2(2)$ is not simple. The case when $S \simeq A_2(2)$ has been already eliminated. If $S \simeq {}^2A_2(3)$ then $n_2(S) = 7$ is not equal to $(q^2+1)/2$ for any q. Finally, if $S \simeq A_2(3)$ then $n_2(S) = 13 = (q^2+1)/2 = n_2(L)$ and hence $L = B_2(5)$, which is impossible, since $3^3 = |S|_3 > 3^2 = |L|_3$.

Let $S \simeq A_1(u)$. Then $a = n_2(L) = (q^2+1)/2$ is equal to one of the numbers v, $(u-1)/(2, u-1)$, $(u+1)/(2, u-1)$. Since S includes a Frobenius group with kernel of order u and complement of order $(u-1)/(2, u-1)$, each prime divisor of $(u-1)/(2, u-1)$ is adjacent in $GK(G)$ to every prime divisor of the order of K other than v. By assumption, p is not equal to v and divides the order of K. Therefore $a \neq (u-1)/(2, u-1)$. Suppose that $a = v$. Since $(a, |L|/a) = 1$, we have $u = v = a$ and, in particular, $v \neq 2$. It is

shown in the previous paragraph that $|S|/a$ must divide $(q^2-1)^2$. On the other hand, $(u+1)/2 = (q^2+3)/4$ is coprime to q^2-1 since $(q^2-1, q^2+3) = 4$; a contradiction. If $(q^2+1)/2 = (u+1)/2$ then $v = p$, a contradiction. If $(q^2+1)/2 = u+1$ then $u = 2^\beta$ and $q^2 = 2^{\beta+1}+1$, which is impossible since $q > 3$. Thus the case $L = B_2(q)$ is examined completely.

II. Let L be one of the groups $B_3(q)$, $C_3(q)$, $D_4(q)$. It follows by Lemma 3.2 that $(k_4(q)k_3(q)k_6(q), |K| \cdot |\overline{G}/S|) = 1$.

Let $S \simeq A_1(u)$. Since a cyclic group of order $(u-1)/(2,u-1)$ arises as the complement of a Frobenius subgroup of S and $p \in \pi(K)$, each prime divisor of $(u-1)/(2,u-1)$ is adjacent to p in $GK(G)$. Therefore $k_3(q)$ and $k_6(q)$ are coprime to $u-1$, and so one of them divides u. Thus a Sylow v-subgroup of S must be cyclic. Hence $u = v$. In particular, $v > 3$. Since $r_4(q)$ is not adjacent to $r_3(q)$ and $r_6(q)$, the number $k_4(q)$ divides $(v-1)/2$. In particular, this implies that a Hall $\pi(k_4(q))$-subgroup of S and so a Hall $\pi(k_4(q))$-subgroup of L as well are cyclic. Therefore L cannot be $D_4(q)$. Hence $L = B_3(q)$ or $L = C_3(q)$. The fact that p divides K and Lemma 3.1 yield $|K|_p = q^6$, and thus $|S|_p \geqslant q$. Since p is not adjacent to $r_3(q)$ and $r_6(q)$, the number q divides $(v-1)/2$. Therefore $q(q^2+1)/(2,q-1)$ divides $(v-1)/2$. Hence $q(q^2+1) \leqslant v-1 < v \leqslant \max\{k_3(q), k_6(q)\} \leqslant q^2+q+1$, which is impossible. Thus $S \not\simeq A_1(u)$.

Since $S \not\simeq A_1(u)$, a Sylow v-subgroup of S cannot be cyclic, and so a Sylow v-subgroup of G cannot be cyclic either. Therefore v does not divide $k_3(q)$, $k_6(q)$. Suppose that v divides $k_4(q)$. Then L must be equal to $D_4(q)$. Furthermore, $(6, k_4(q)) = 1$, and so $v \geqslant 5$. Put $v^\gamma = (k_4(q))_v$. Since $(k_4(q), |K| \cdot |\overline{G}/S|) = 1$, we have $|S|_v = |L|_v = (k_4(q)^2)_v = v^{2\gamma}$, i. e., the order of a Sylow v-subgroup is equal to the squared v-period of S. Examining all variants accordingly (3), it easy to check that this is impossible. Thus v does not divide $k_4(q)$ in the case $L = D_4(q)$ either. Therefore v divides q^2-1.

Denote a Sylow v-subgroup of S by V. Since $S \not\simeq A_1(u)$, Lemma 1.5 yields $|V|^{8/3} > |S|$. It follows that $|V|^2 > |S|/|V|$.

Let $L = B_3(q)$ or $L = C_3(q)$. It follows by Lemma 3.1 that $|K|_p = q^6$. Therefore $|\overline{G}|_p = q^3$. Applying Lemma 3.1 one more time, we infer that $|\overline{G}/S|_p \leqslant q$ if p is odd or $q > 4$

and that $|\overline{G}/S|_p \leqslant 8$ if $q = 4$. Let $L \neq B_3(4)$. The order of S is divisible by the number $t = q^2k_4(q)k_3(q)k_6(q) = q^2(q^2+1)(q^4+q^2+1)/(2, q-1)(3, q^2-1)$, which is coprime to v and divides $|L| = q^9(q^2-1)^3(3, q^2-1) \cdot t$. So $|V| \leqslant ((q^2-1)_v)^3$ if $v \neq 3$ and $|V| \leqslant 3((q^2-1)_3)^3$ if $v = 3$.

If v and q are odd, then $(q^2-1)_v \leqslant (q+1)/2$. Hence $|V|^2 \leqslant 9((q+1)/2)^6 < t \leqslant |S|/|V|$; a contradiction.

If q is even then v is odd, so $(q^2-1)_v \leqslant q+1$. If $v \neq 3$ then $|V|^2 \leqslant (q+1)^6 < t \leqslant |S|/|V|$; a contradiction. If $v = 3$ then $|V|^2 \leqslant 9(q+1)^6 < t \leqslant |S|/|V|$ for $q > 4$.

If $v = 2$ then q is odd. Suppose first that $q \neq 2^\delta \pm 1$. Then $(q^2-1)_2 \leqslant 2(q+1)/3$ and $|V|^2 \leqslant (2(q+1)/3)^6 < t \leqslant |S|/|V|$, which is impossible. Let $q = 2^\delta + 1$. Then q is a Fermat prime or 9 and $(q^2-1)_2 = 2(q-1)$. We have $|V|^2 \leqslant (2(q-1))^6 < t \leqslant |S|/|V|$ for $q > 5$. Let $q = 2^\delta - 1$. Then q is a Mersenne prime and $(q^2-1)_2 = 2(q+1)$. We have $|V|^2 \leqslant (2(q+1))^6 < t \leqslant |S|/|V|$ for $q > 7$.

Thus it remains to consider the situation when L is one of the five groups $B_3(4) = C_3(4)$, $B_3(5)$, $C_3(5)$, $B_3(7)$, $C_3(7)$. Moreover, in all the cases except the first one we can assume that $v = 2$.

If $L = B_3(4)$ then $k_3(4) = 7$, $k_6(4) = 13$, $k_4(4) = 17$ lie in $\omega(S)$. By [37, Table 1], if S satisfies the conditions $\pi(S) \subseteq \pi(L) = \{2, 3, 5, 7, 13, 17\}$ and $|S|_r = |L|_r = r$ for $r \in \{7, 13, 17\}$ but is not isomorphic to L then $S \simeq A_2(16)$, which is impossible since $v \neq p$ by assumption.

If $L \in \{B_3(5), C_3(5)\}$ then $k_3(5) = 31$, $k_6(5) = 7$, $k_4(5) = 13$ lie in $\omega(S)$. It follows from [37, Table 1] that a group S satisfying $\{7, 13, 31\} \subseteq \pi(S) \subseteq \pi(L) = \{2, 3, 5, 7, 13, 31\}$ must be a group over a field of characteristic 5; a contradiction.

If $L \in \{B_3(7), C_3(7)\}$ then $k_3(7) = 19$, $k_6(7) = 43$, $k_4(7) = 25$ lie in $\omega(S)$. It follows from [37, Table 1] that a group S satisfying $\{5, 19, 43\} \subseteq \pi(S) \subseteq \pi(L) = \{2, 3, 5, 7, 19, 43\}$ and $|S|_5 = |L|_5 = 5^2$ must itself lie in $\{B_3(7), C_3(7)\}$; a contradiction.

Let $L = D_4(q)$. Lemma 3.1 implies that $|K|_p = q^{6\gamma}$, where $\gamma \in \{1, 2\}$. It follows that $|V| \leqslant ((q^2-1)_v)^4$, if $v \neq 3$ and $|V| \leqslant 3((q^2-1)_3)^4$ if $v = 3$.

If $|K|_p = q^6$ then $|S|/|V|$ is divisible by $t = q^4(q^2+1)^2(q^4+q^2+1)/(2, q-1)^2(3, q^2-1)$,

which is greater than $|V|^2$ in all cases except when $q = 7$ and $v = 2$.

If $|K|_p = q^{12}$ then $|S|/|V|$ is divisible by $t = (q^2+1)^2(q^4+q^2+1)/(2, q-1)^2(3, q^2-1)$. Observe that in this case $|\overline{G}|$ is not divisible by p since $|L|_p = q^{12}$. In particular, p cannot be equal to 2.

If v is odd then $|V|^2 \leqslant 9((q+1)/2)^8 < t \leqslant |S|/|V|$ for $q > 7$.

Let $v = 2$. In this case we need a more accurate estimate on the order of a Sylow v-subgroup of S. By Lemma 1.5, $|V|^{5/3} > |S|/|V|$. Since $v = 2$, it follows that $|V| \leqslant ((q^2-1)_2)^4/4$. Suppose first that $q \neq 2^\delta - 1$. Then $(q^2-1)_2 \leqslant 2(q-1)$ and $|V|^{5/3} \leqslant (2(q-1))^{20/3}/4^{5/3} < t \leqslant |S|/|V|$, but this is false. If $q = 2^\delta - 1$ then q is a Mersenne prime and $(q^2-1)_2 = 2(q+1)$. The chain of the inequalities $|V|^{5/3} \leqslant (2(q+1))^{20/3}/4^{5/3} < t \leqslant |S|/|V|$ holds for $q > 7$.

Thus it remains to handle the cases when $L \in \{D_4(5), D_4(7)\}$.

If $L = D_4(5)$ then $k_3(5) = 31$, $k_6(5) = 7$, $k_4(5) = 13$ lie in $\omega(S)$. It follows from [37, Table 1] that a group S satisfying $\{7, 13, 31\} \subseteq \pi(S) \subseteq \pi(L) = \{2, 3, 5, 7, 13, 31\}$ must be a group over a field of characteristic 5; a contradiction.

If $L = D_4(7)$ then [37, Table 1] yields that a group S satisfying $\{5, 19, 43\} \subseteq \pi(S) \subseteq \pi(L) = \{2, 3, 5, 7, 19, 43\}$ and $|S|_5 = |L|_5 = 5^4$ must itself be isomorphic to $D_4(7)$; a contradiction. The theorem is proved.

References

1. W. Shi, "A new characterization of the sporadic simple groups," in: Group Theory, Proc. 1987 Singapore Group Theory Conf., Berlin-New York, Walter de Gruyter, 531–540 (1989).
2. Unsolved problems in group theory. The Kourovka notebook, 16th edn (Eds. V. D. Mazurov and E. I. Khukhro), Novosibirsk, Sobolev Institute of Mathematics (2006).
3. W. Shi and J. Bi, "A new characterization of the alternating groups," *Southeast Asian Bull. Math.*, **16**, No. 1, 81—90 (1992).
4. W. Shi and J. Bi, "A characterization of Suzuki-Ree groups," *Sci. China, Ser. A*, **34**, No. 1, 14—19 (1991).

5. W. Shi, "The pure quantitative characterization of finite simple groups (I)," *Progr. Nat. Sci.*, **4**, No. 3, 316—326 (1994).

6. W. Shi and J. Bi, "A characteristic property for each finite projective special linear group," in: Groups, Sel. Pap. Aust. Natl. Univ. Group Theory Program, 3rd Int. Conf. Theory Groups Rel. Top., Canberra/Aust. 1989 (Lect. Notes Math. **1456**), Berlin, Springer-Verlag, 1990, 171—180.

7. H. Cao and W. Shi, "Pure quantitative characterization of finite projective special unitary groups," *Sci. China, Ser. A*, **45**, No. 6, 761—772 (2002).

8. M. Xu and W. Shi, "Pure quantitative characterization of finite simple groups ${}^2D_n(q)$ and $D_l(q)$ (l odd)," *Algebra Colloq.*, **10**, No. 3, 427—443 (2003).

9. A. V. Vasil′ev, M. A. Grechkoseeva, and V. D. Mazurov, On finite groups isospectral to simple symplectic and orthogonal groups, *Siberian Math. J.*, **50**, No. 6, 965–981 (2009).

10. J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, and R. A. Wilson, *Atlas of finite groups*, Oxford, Clarendon Press (1985).

11. K. Zsigmondy, "Zur Theorie der Potenzreste," *Monatsh. Math. Phys.*, **3**, 265—284 (1892).

12. M. Roitman, "On Zsigmondy primes," *Proc. Am. Math. Soc.*, **125**, No. 7, 1913—1919 (1997).

13. D. Deriziotis, "Conjugacy classes and centralizers of semisimple elements in finite groups of Lie type," Vorlesungen Fachbereich Math. Univ. Essen, **11** (1984).

14. D. M. Testerman, "A_1-Type overgroups of elements of order p in semisimple algebraic groups and the associated finite groups," *J. Algebra*, **177**, No. 1, 34—76 (1995).

15. D. I. Deriziotis and A. P. Fakiolas, "The maximal tori in the finite Chevalley groups of type E_6, E_7 and E_8," *Commun. Algebra*, **19**, No. 3, 889—903 (1991).

16. D. Deriziotis, "The centralizers of semisimple elements of the Chevalley groups E_7 and E_8," *Tokyo J. Math.*, **6**, No. 1, 191—216 (1983).

17. A. A. Buturlakin and M. A. Grechkoseeva, "The cyclic structure of maximal tori of the finite classical groups," *Algebra and Logic*, **46**, No. 2, 73-89 (2007).

18. A. A. Buturlakin, "Spectra of finite linear and unitary groups," *Algebra and Logic*, **47**, No. 2, 91—99 (2008).

19. A. A. Buturlakin, "Spectra of finite simple symplectic groups and orthogonal groups of odd dimension," Preprint No. 204, Novosibirsk, Inst. Mat. SO RAN (2009) [in Russian].

20. A. V. Vasil′ev, I. B. Gorshkov, M. A. Grechkoseeva, A. S. Kondrat′ev, and A. M. Staroletov, "On recognizability by spectrum of finite simple groups of types B_n, C_n and ${}^2D_n$ for $n = 2^k$," *Trudy Inst. Mat. Mekh. UrO RAN*, **15**, No. 2, 58—73 (2009).

21. M. A. Grechkoseeva, "Recognition by spectrum for finite linear groups over fields of characteristic 2," *Algebra and Logic*, **47**, No. 4, 229—241 (2008).

22. W. Shi, "On a problem of E. Artin," *Acta Math. Sin.*, **35**, No. 2, 262—265 (1992) [in Chinese].

23. V. D. Mazurov, "Characterization of finite groups by sets of element orders," *Algebra and Logic*, **36**, No. 1, 23–32 (1997).

24. J. S. Williams, "Prime graph components of finite groups," *J. Algebra*, **69**, No. 2, 487—513 (1981).

25. A. S. Kondrat′ev, "Prime graph components of finite simple groups," *Math. USSR-Sb.*, **67**, No. 1, 235–247 (1990).

26. V. D. Mazurov, "Recognition of finite simple groups $S_4(q)$ by their element orders," *Algebra and Logic*, **41**, No. 2, 93–110 (2002).

27. A. V. Vasil'ev, "On connection between the structure of a finite group and the properties of its prime graph," *Siberian Math. J.*, **46**, No. 3, 396—404 (2005).

28. A. V. Vasil′ev and I. B. Gorshkov, "On recognition of finite simple groups with connected prime graph," *Siberian. Math. J.*, **50**, No. 2, 233–238 (2009).

29. A. V. Vasiliev and E. P. Vdovin, "An adjacency criterion for the prime graph of a finite simple group," *Algebra and Logic*, **44**, No. 6, 381–406 (2005).

30. M. R. Aleeva, "On finite simple groups with the set of element orders as in a Frobenius or a double Frobenius group," *Math. Notes,* **73**, No. 3, 299–313 (2003).

31. A. V. Zavarnitsine, "A solvable group isospectral to $S_4(3)$," *Siberian Math. J.*, to appear.

32. W. Shi and C. Y. Tang, "A characterization of some orthogonal groups," *Prog. Nat. Sci.*, **7**, No. 2, 155—162 (1997).

33. V. D. Mazurov and A. R. Moghaddamfar, "The recognition of the simple group $S_8(2)$ by its spectrum," *Algebra Colloq.*, **13**, No. 4, 643—646 (2006).

34. A. V. Vasil′ev and E. P. Vdovin, "Cocliques of maximal size in the prime graph of a finite simple group," Preprint No. 225, Novosibirsk, Inst. Mat. SO RAN (2009), http://arxiv.org/abs/0905.1164v1.

35. M. A. Grechkoseeva, "On difference between the spectra of the simple groups $B_n(q)$ and $C_n(q)$," *Siberian Math. J.*, **48**, No. 1, 73—75 (2007).

36. W. Shi, "Pure quantitative characterization of finite simple groups," *Front. Math. China*, **2**, No. 1, 123—125 (2007).

37. A. V. Zavarnitsine, "Finite simple groups with narrow prime spectrum," *Sib. Electr. Math. Rep.*, **6**, 1—12 (2009), http://semr.math.nsc.ru/v6/p1-12.pdf.

Abstract

In the article we give an affirmative answer to Question 12.39 from the Kourovka Notebook. Namely we prove that a finite simple group and a finite group having the same orders and the same sets of element orders are isomorphic.

Key words: finite group, simple group, element orders, recognizability by spectrum and order, symplectic group, orthogonal group.