S©MR ISSN 1813-3304

СИБИРСКИЕ ЭЛЕКТРОННЫЕ
МАТЕМАТИЧЕСКИЕ ИЗВЕСТИЯ

Siberian Electronic Mathematical Reports
http://semr.math.nsc.ru

Том 10, стр. 31–37 (2013) УДК 512.542
MSC 20D60

ON FINITE GROUPS ISOSPECTRAL TO FINITE SIMPLE UNITARY GROUPS OVER FIELDS OF CHARACTERISTIC 2

M.A. GRECHKOSEEVA, W.J. SHI

ABSTRACT. For every group $U = PSU_n(2^k)$ with $n \geqslant 5$, we find the number of finite groups having the same element orders as U.

Keywords: recognition by spectrum, unitary group, field automorphism.

Dedicated to 70th anniversary of V.D. Mazurov

1. Introduction

The spectrum $\omega(G)$ of a group G is the set of its element orders. Two groups are said to be isospectral if their spectra coincide. A finite group L is recognizable by spectrum if every finite group G with $\omega(G) = \omega(L)$ is isomorphic to L. Denoting by $h(L)$ the number of pairwise non-isomorphic finite groups isospectral to L we can write the property of L to be recognizable as $h(L) = 1$. And L is said to be almost recognizable if $h(L)$ is finite, and irrecognizable otherwise. The recognition by spectrum problem for a group L is to determine whether L is recognizable, almost recognizable or irrecognizable, and a stronger version of this problem is to find $h(L)$. The most recent survey on this subject can be found in [1–3].

This article is concerned with recognition of simple unitary groups $PSU_n(2^k)$. The group $PSU_3(2)$ is soluble and the groups $PSU_4(2)$, $PSU_5(2)$ are irrecognizable [4, 5]. The groups $PSU_3(2^k)$ with $k \geqslant 2$, $PSU_4(2^k)$ with $k \geqslant 2$, and $PSU_6(2)$ are recognizable [6–9]. The rest of the groups $PSU_n(2^k)$ are known to be almost recognizable, but the precise numbers of isospectral groups are still unknown (see

---

GRECHKOSEEVA M.A., SHI W.J., ON FINITE GROUPS ISOSPECTRAL TO FINITE SIMPLE UNITARY GROUPS OVER FIELDS OF CHARACTERISTIC 2.

The first author is supported by the RFBR (grants 11-01-91158 and 12-01-31221). The second author is supported by the NSFC (projects 11171364 and 11111120022).

Received December, 27, 2012, published January, 16, 2013.

Lemma 5). The aim of the article is to find these numbers and to describe the isospectral groups.

Theorem. *Let $U = PSU_n(q)$, where $n \geqslant 5$, $q = 2^k$, and $U \neq PSU_5(2)$. Let $d = (n, q+1)$ and f be the d-part of $((q+1)/d, k)$.*

(i) If $n-1$ is a power of 2 then $h(U) = 1$.

(ii) If $n-1$ is not a power of 2 then $h(U)$ is equal to the number of divisors of f. Furthermore, a finite group G satisfies $\omega(G) = \omega(U)$ if and only if G is isomorphic to the natural extension of U by a field automorphism of order dividing f.

In particular, U is recognizable by spectrum if and only if $(d, (q+1)/d, k) = 1$ or $n-1$ is a power of 2.

In the above theorem and below, $(m_1, m_2, \dots, m_s)$ denotes the greatest common divisor of numbers $m_1, m_2, \dots, m_s$, and for natural numbers r and m, the r-part of m is the smallest divisor t of m such that $(m/t, r) = 1$.

2. Notation and preliminary results

Let G be a finite group. Divisibility relation endows the set $\omega(G)$ by a partial order, and the subset of elements maximal under this order is denoted by $\mu(G)$. Given a prime r, we refer to the highest power of r lying in $\omega(G)$ as to the r-exponent of G.

The set of prime divisors of a natural number m is denoted by $\pi(m)$. For a finite group G, we define $\pi(G) = \pi(|G|)$. Given natural numbers m and r, we write m_r to denote the r-part of m, and $m_{r'}$ to denote the number m/m_r. As usual, $[m_1, m_2, \dots, m_s]$ denotes the least common multiple of numbers $m_1, m_2, \dots, m_s$.

Given an integer q and an odd prime r such that $(q, r) = 1$, we write $e(r, q)$ for the multiplicative order of q modulo r, that is, the smallest natural number m satisfying $q^m \equiv 1 \pmod r$. For an odd q, we put $e(2, q) = 1$ if $q \equiv 1 \pmod 4$, and $e(2, q) = 2$ otherwise.

Lemma 1 (Zsygmondy [10])**.** *Let q be an integer whose absolute value is larger than 1. For every natural number k, there is a prime r such that $e(r, q) = k$ except the cases where the pair (q, k) is in $\{(2,1), (3,1), (2,6), (-2,2), (-2,3), (-3,2)\}$.*

A prime r satisfying $e(r, q) = k$ is said to be a primitive prime divisor of $q^k - 1$, and the set of all primitive prime divisors of $q^k - 1$ is denoted by $R_k(q)$. It is easy to verify that $R_k(q) \subseteq R_k(q^m)$ for coprime m and k. The notation $r_k(q)$ is used to denote an element of $R_k(q)$, provided that this set is not empty.

Lemma 2 ([11, Corollary 3])**.** *Let $n \geqslant 3$, q be a power of a prime p, $d = (n, q+1)$, and $\varepsilon = -1$. Then $\omega(PSU_n(q))$ consists of all divisors of the following numbers:*

(i) $\frac{q^n - \varepsilon^n}{d(q+1)}$;

(ii) $\frac{[q^{n_1} - \varepsilon^{n_1}, q^{n_2} - \varepsilon^{n_2}]}{(n/(n_1, n_2), q+1)}$, *where $n_1, n_2 > 0$ and $n_1 + n_2 = n$;*

(iii) $[q^{n_1} - \varepsilon^{n_1}, q^{n_2} - \varepsilon^{n_2}, \dots, q^{n_s} - \varepsilon^{n_s}]$, *where $s \geqslant 3$, $n_1, n_2, \dots, n_s > 0$ and $n_1 + n_2 + \dots + n_s = n$;*

(iv) $p^l \frac{q^{n_1} - \varepsilon^{n_1}}{d}$, *where $l, n_1 > 0$, $p^{l-1} + 1 + n_1 = n$;*

(v) $p^m [q^{n_1} - \varepsilon^{n_1}, \dots, q^{n_s} - \varepsilon^{n_s}]$, *where $s \geqslant 2$, $m, n_1, \dots, n_s > 0$ and $p^{m-1} + 1 + n_1 + \dots + n_s = n$;*

(vi) p^l, *provided that $p^{l-1} + 1 = n$ for $l > 0$.*

Lemma 3 ([12, Corollary 1])**.** *Let m be an odd number and ψ a field automorphism of $PSU_n(q^m)$ of order m. Then*

$$\omega(PSU_n(q^m)\langle\psi\rangle) = \bigcup_{r|m} r \cdot \omega(PSU_n(q^{m/r})).$$

Lemma 4. *Let q and l be natural numbers and $q > 1$.*

(*i*) *If r is an odd prime and r divides $q+1$ or $r = 2$ and $q+1$ is divisible by 4, then $(q^l - (-1)^l)_r = l_r(q+1)_r$.*

(*ii*) *If r and l are coprime, then $\frac{q^l-(-1)^l}{q+1}$ divides $\frac{q^{rl}-(-1)^{rl}}{q^r-(-1)^r}$, and $\frac{q^l-(-1)^l}{(n,q+1)}$ divides $\frac{q^{rl}-(-1)^{rl}}{(n,q^r-(-1)^r)}$ for every natural n.*

Proof. See [13, Lemma 6] and [14, Lemma 8].

Lemma 5. *Let $U = PSU_n(q)$, where $n \geqslant 5$, $q = 2^k$, and $U \neq PSU_5(2)$. If G is a finite group such that $\omega(G) = \omega(U)$ then $U \leq G \leq \operatorname{Aut} U$.*

Proof. By the main result of [15], we may assume that $U \leq G/K \leq \operatorname{Aut} U$, where K is the soluble radical of G. The full preimage of U in G has the same spectrum as U, and [16, Corollary 1] implies that K is identity.

3. Proof of the theorem

We begin with specifying a matrix representation of unitary groups. We identify $GU_n(q)$ with the subgroup of $GL_n(q^2)$ consisting of matrices $A = (a_{ij})$ such that $(a_{ij}^q)^T = (a_{ij})^{-1}$. Then $SU_n(q)$ is the subgroup of matrices of determinant 1 in $GU_n(q)$; and $PGU_n(q)$ and $PSU_n(q)$ are the images of $GU_n(q)$ and $SU_n(q)$ in the projective group $PGL_n(q^2)$ respectively.

Let $U = PSU_n(q)$, where $q = p^k$ and $n \geqslant 5$. The group $PGU_n(q)$ acts on U by conjugation, and we identify U with $\operatorname{Inn} U$ and $PGU_n(q)$ with the group of inner-diagonal automorphisms of U. Denote by δ the image of the unitary matrix $diag(1, \ldots, 1, \lambda)$, where λ is a primitive $(q+1)$th root of unity in $GF(q^2)$, in $PGU_n(q)$. Denote by φ the field automorphism of U induced by Frobenius map $(a_{ij}) \mapsto (a_{ij}^p)$ of $GU_n(q)$. Then

$$\operatorname{Aut} U = PGU_n(q) \leftthreetimes \langle\varphi\rangle = \langle U, \delta\rangle \leftthreetimes \langle\varphi\rangle$$

with $\delta^\varphi = \delta^p$, $|\langle U, \delta\rangle/U| = (n, q+1)$ and $|\varphi| = 2k$.

Now we are ready to prove the theorem. Let G be a finite group such that $\omega(G) = \omega(U)$. By Lemma 5, we have $U \leq G \leq \operatorname{Aut} U$. Suppose that the index $|G : U|$ is even. By hypothesis, q is even, so we may assume that G contains $\gamma = \varphi^k$. The centralizer $C_U(\gamma)$ is a group of type $C_{n/2}(q)$ or $C_{(n-1)/2}(q)$ according as n is even or odd [17, Proposition 4.9.2 (b)]. Hence one of the numbers $r_n(-q)$ and $r_{n-1}(-q)$ lies in $\pi(C_U(\gamma))$. On the other hand, $2r_n(-q)$, $2r_{n-1}(-q) \notin \omega(U)$. Thus the index $|G : U|$ is odd. The remaining part of the proof does not depend on the characteristic p being 2, so in fact we can prove the following assertion, thus proving the theorem.

Proposition 6. *Let $U = PSU_n(q)$, where $q = p^k$, $n \geqslant 5$, and $d = (n, q+1)$. Suppose that G is a finite group with $U < G \leq \operatorname{Aut} U$ and $|G/U|$ being odd. Then $\omega(G) = \omega(U)$ if and only if $n-1$ is not a power of p and G is conjugate in $\operatorname{Aut} U$ to a subgroup of the group $U \leftthreetimes \langle\phi\rangle$, where $\phi \in \langle\varphi\rangle$ and $|\phi| = ((q+1)/d, k)_d$.*

Proof. Suppose that $\omega(G) = \omega(U)$. Given an element $g \in \operatorname{Aut} U$, we write $\hat{g}$ to denote its image in $\operatorname{Out} U$.

If $G \cap PGU_n(q) > U$ then the intersection of G and a maximal torus of $PGU_n(q)$ of order $(q^n - (-1)^n)/(q+1)$ is a cyclic group of order $(q^n - (-1)^n)/c(q+1)$ for some $c < d$. However, Lemma 2 implies that $(q^n - (-1)^n)/d(q+1) \in \mu(U)$. Hence $G \cap PGU_n(q) = U$ and G/U is a cyclic group. Let $\alpha = \beta\psi$, where $\beta \in \langle\delta\rangle$ and $\psi \in \langle\varphi\rangle$, generates G modulo U and let $|\psi| = m$. Then $\alpha^m \in G \cap PGU_n(q)$, and therefore $|G/U| = |\hat{\alpha}| = m$.

We claim that $\pi(m) \subseteq \pi(d)$. Otherwise, G contains a field automorphism of odd prime order r with r not dividing d. Denote $q^{1/r}$ by q_0. By Lemma 3, the spectrum of G includes the set $r\omega(PSU_n(q_0))$. If $r = p$ then the p-exponent of G exceeds that of U. Hence $(r, p) = 1$. Denote $e(r, -q)$ by s. Below we will use information on spectra of simple groups from [18] (see also corrections to this article in [19] and [20]).

Suppose that $s = 1$, that is, r divides $q+1$. Then r does not divide n, and therefore $r_n(-q_0) \in R_n(-q)$. Thus by [18, Proposition 4.2], it follows that $rr_n(-q_0) \notin \omega(U)$. On the other hand, $rr_n(-q_0) \in r\omega(PSU_n(q_0)) \subseteq \omega(G)$; a contradiction.

Suppose that $s = 2$ and that r divides the odd number in the set $\{n, n-1\}$. Denote this odd number by l. Since $(l-2, r) = 1$, it follows that $r_{l-2}(-q_0)$ is in $R_{l-2}(-q)$. By Lemma 2, we have that $pr_{l-2} \in \omega(PSU_n(q_0))$. On the other hand, $l-2$ is odd and hence $rpr_{l-2}(-q_0) \notin \omega(U)$; a contradiction. This argument fails if $q_0 = 2$ and $l = 5$, but in this case $r = 5$, $q = 32$ and $e(r, -q) \neq 2$.

Suppose $2 \leqslant s \leqslant n$, and if $s = 2$ then the odd number of the set $\{n, n-1\}$ is coprime to r. We can choose a number t in the set $\{4, \dots, n\}$ such that t and s do not divide each other, $t + s > n$ and $(t, r) = 1$. Then $r_t(-q_0) \in R_t(-q)$ and by [18, Proposition 2.2], we have that $rr_t(-q_0) \notin \omega(U)$. On the other hand, $rr_t(-q_0) \in \omega(G)$; a contradiction.

Thus $\pi(m) \subseteq \pi(d)$. Suppose that $\hat{\alpha}$ is not conjugate to $\hat{\psi}$ in $\operatorname{Out} U$. For convenience, we may assume that $\psi = \varphi^{2(m-1)k/m}$ so as to have $\delta^{\psi^{-1}} = \delta^{q_0^2}$, where $q_0 = q^{1/m}$. Then
$$(\psi)^\delta = \delta^{-1}\delta^{\psi^{-1}}\psi = \delta^{q_0^2-1}\psi,$$
and we deduce that $\hat{\beta} \notin \langle\hat{\delta}^{q_0^2-1}\rangle$, or equivalently, $\beta \notin \langle\delta^{(q_0^2-1,d)}\rangle$. Hence $|\beta|$ does not divide $|\delta^{(q_0^2-1,d)}|$, and so there is a prime r such that
$$|\beta|_r > \frac{(q+1)_r}{(q_0^2-1,d)_r}.$$
In particular, $(q_0^2-1,d)_r > 1$ and $|\beta|_r > (q+1)_r/d_r$. Since r divides $q_0^2 - 1$, by Lemma 4, we have $(q^2-1)_r/(q_0^2-1)_r = m_r$. Now the equalities
$$\alpha^m = (\beta\psi)^m = \beta\beta^{\psi^{-1}}\dots\beta^{\psi^{1-m}} = \beta^{1+q_0^2+\dots+q_0^{2(m-1)}} = \beta^{(q^2-1)/(q_0^2-1)}$$
show that $|\alpha|_r = |\beta|_r$. Moreover, since $\alpha^m \in U$, we derive that $\beta^{(q^2-1)/(q_0^2-1)} \in \langle\delta^d\rangle$, which implies
$$|\beta|_r \leqslant \frac{(q+1)_r}{d_r} \cdot m_r.$$
Hence r divides m. In particular, r is odd and r divides $q_0 + 1$. Since α centralizes a subgroup of U isomorphic to $SU_{n-1}(q_0)$, there is an element of order $r_{n-1}(-q_0)|\alpha|_r$ in G. The numbers m and $n-1$ are coprime, so $r_{n-1}(-q_0) \in R_{n-1}(-q)$. Then it follows from Lemma 2 that the number $r_{n-1}(-q_0)|\alpha|_r$ can lie in $\omega(U)$ only if it

divides $(q^{n-1}-(-1)^{n-1})/d$. However, $(q^{n-1}-(-1)^{n-1})_r/d_r=(n-1)_r(q+1)_r/d_r=$ $=(q+1)_r/d_r<|\alpha|_r$.

Thus $\hat{\alpha}$ is conjugate to $\hat{\psi}$, as required. Moreover, arguing as above, it is easy to show that m divides $(q+1)/d$ (otherwise, there is a prime divisor r of m such that $m_r r_{n-1}(-q_0)\in\omega(G)\setminus\omega(U)$). It remains to establish that $n-1$ is not a power of p. If $n=p^l+1$ for some l then by Lemma 2 we have that $p^{l+1}\in\mu(U)$. But the same lemma asserts that $p^{l+1}\in\omega(PSU_n(q_0))$, and now Lemma 3 implies that $mp^{l+1}\in\omega(G)$; a contradiction.

Now we prove the converse implication. It suffices to consider the maximal case where $G=U\leftthreetimes\langle\phi\rangle$ with $|\phi|=((q+1)/d,k)_d$. Notice that the number $((q+1)/d,k)_d$ is odd. By Lemma 3, the spectrum of G is the union of the sets $m\omega(PSU_n(q^{1/m}))$ over all divisors m of $((q+1)/d,k)_d$.

Fix a number m dividing $((q+1)/d,k)_d$ and let $q_0=q^{1/m}$. First we check that for every $r\in\pi(m)$ and every natural number l

$$(q^l-(-1)^l)_r\geqslant m_r(q_0^l-(-1)^l)_r, \tag{1}$$

and if $(l,m)=1$ then for every divisor h of n

$$(q^l-1)_r/(h,q-1)_r\geqslant m_r(q_0^l-1)_r/(h,q_0-1)_r. \tag{2}$$

Using Lemma 4, we derive that

$$(q^l-(-1)^l)_r=m_r(q_0^{m_{r'}l}-(-1)^{m_{r'}l})_r. \tag{3}$$

This implies (1) and also the equality $(q+1)_r=m_r(q_0^{m_{r'}}+1)_r$. By hypothesis, m divides $(q+1)/d$, so $(q+1)_r>(q_0^{m_{r'}}+1)_r\geqslant d_r$. This means that for every divisor h of n we have

$$(h,q+1)_r=h_r=(h,q_0^{m_{r'}}+1)_r. \tag{4}$$

Now (3) and (4) show that

$$\frac{(q^l-(-1)^l)_r}{(h,q+1)_r}=m_r\frac{(q_0^{m_{r'}l}-(-1)^{m_{r'}l})_r}{(h,q_0^{m_{r'}}+1)_r}. \tag{5}$$

By Lemma 4, if $(l,m)=1$ then $m_r(q_0^l-(-1)^l)_r/(h,q_0+1)_r$ divides the right-hand side of (5), so we have (2).

Now we are ready to verify that for every $a\in\omega(PSU_n(q_0))$, there is $b\in\omega(U)$ such that ma divides b. By hypothesis, $n-1$ is not a power of p, so we may assume that a is one of the numbers $f(q_0)$ listed in (i)–(v) of Lemma 2. For convenience, we write ε in place of -1.

Let

$$f(q_0)=\frac{q_0^n-\varepsilon^n}{(q_0+1)(n,q_0+1)}.$$

Denote by r the smallest prime in $\pi(m)$. Then $(m,r-1)=1$. Hence r divides $q_0+1=(q_0^m+1,q_0^{r-1}-1)$. There is an element of order $q^{n/r}-\varepsilon^{n/r}$ in U. This order is divisible by $f(q_0)$. Furthermore, by Lemma 4 and (1), we see that

$$(q^{n/r}-\varepsilon^{n/r})_r=\frac{(q^n-\varepsilon^n)_r}{r}\geqslant\frac{m_r(q_0^n-\varepsilon^n)_r}{r}\geqslant\frac{m_r(q_0^n-\varepsilon^n)_r}{(q_0+1)_r}\geqslant m_rf(q_0)_r$$

and

$$(q^{n/r}-\varepsilon^{n/r})_u=(n/r)_u(q+1)_u=n_u(q+1)_u=(q^n-\varepsilon^n)_u\geqslant m_u(q_0^n-\varepsilon^n)_u\geqslant m_uf(q_0)_u$$

for every $u\in\pi(m)$, $u\neq r$. Thus $mf(q_0)$ divides $q^{n/r}-\varepsilon^{n/r}$.

Let
$$f(q_0)=\frac{[q_0^{n_1}-\varepsilon^{n_1},q_0^{n_2}-\varepsilon^{n_2}]}{(h,q_0+1)},$$
where $n_1+n_2=n$ and $h=n/(n_1,n_2)$. Suppose that n_1 and m have a common prime divisor r. Then r also divides n_2. Replacing n_1 by n_2 if necessary, we may assume that $(q^{n_1}-\varepsilon^{n_1})_r\leqslant(q^{n_2}-\varepsilon^{n_2})_r$. There is an element of order $[q^{n_1/r}-\varepsilon^{n_1/r},q^{n_2}-\varepsilon^{n_2}]$ in U. This order is divisible by $f(q_0)$. Applying Lemma 4 and (1), we deduce that
$$\begin{aligned}[q^{n_1/r}-\varepsilon^{n_1/r},q^{n_2}-\varepsilon^{n_2}]_r\geqslant[q_0^{n_1}-\varepsilon^{n_1},m(q_0^{n_2}-\varepsilon^{n_2})]_r=\\=m_r[q_0^{n_1}-\varepsilon^{n_1},q_0^{n_2}-\varepsilon^{n_2}]_r\geqslant m_rf(q_0)_r\end{aligned}$$
and
$$\begin{aligned}[q^{n_1/r}-\varepsilon^{n_1/r},q^{n_2}-\varepsilon^{n_2}]_u\geqslant[m(q_0^{n_1}-\varepsilon^{n_1}),m(q_0^{n_2}-\varepsilon^{n_2})]_u=\\=m_u[q_0^{n_1}-\varepsilon^{n_1},q_0^{n_2}-\varepsilon^{n_2}]_u\geqslant m_uf(q_0)_u\end{aligned}$$
for every $u\in\pi(m)$, $u\neq r$.

Suppose now that $(n_1,m)=1$. Then $(n_2,m)=1$ as well. Hence by Lemma 4, we see that $f(q_0)$ divides $f(q)$. Moreover, (2) implies
$$f(q)_m=\frac{[q^{n_1}-\varepsilon^{n_1},q^{n_2}-\varepsilon^{n_2}]_m}{(h,q+1)_m}\geqslant\frac{m[q_0^{n_1}-\varepsilon^{n_1},q_0^{n_2}-\varepsilon^{n_2}]_m}{(h,q_0+1)_m}=mf(q_0)_m.$$
Thus in both cases $mf(q_0)\in\omega(U)$.

Let
$$f(q_0)=p^l\frac{q_0^{n_1}-1}{(n,q_0+1)},$$
where $l>0$, $p^{l-1}+1+n_1=n$. Suppose that n_1 and m have common prime divisors. Denote the smallest of those by r. Consider the number $p^l(q^{n_1/r}-1)$ lying in $\omega(U)$. This number is divisible by $f(q_0)$. By (1) we have
$$(q^{n_1/r}-\varepsilon^{n_1/r})_r=\frac{(q^{n_1}-\varepsilon^{n_1})_r}{r}\geqslant\frac{m_r(q_0^{n_1}-\varepsilon^{n_1})_r}{r}$$
and
$$(q^{n_1/r}-\varepsilon^{n_1/r})_u=(q^{n_1}-\varepsilon^{n_1})_u\geqslant m_u(q_0^{n_1}-\varepsilon^{n_1})_u\geqslant m_uf(q_0)_u$$
for every $u\in\pi(m)$, $u\neq r$. Observe that $(n_1,m,r-1)=1$ by choice of r. Hence if r divides $q_0^{n_1}-\varepsilon^{n_1}$ then r divides $q_0+1=(q_0^{n_1}-\varepsilon^{n_1},q_0^m+1,q_0^{r-1}-1)$ as well, and so $m_r(q_0^{n_1}-\varepsilon^{n_1})_r/r\geqslant m_rf(q_0)_r$. And if r does not divide $q_0^{n_1}-\varepsilon^{n_1}$, then $m_rf(q_0)_r=m_r\leqslant(q^{n_1/r}-\varepsilon^{n_1/r})_r$ since m divides $q+1$. Thus $mf(q_0)$ divides $p^l(q^{n_1/r}-\varepsilon^{n_1/r})$.

Suppose that $(n_1,m)=1$. Then Lemma 4 asserts that $f(q_0)$ divides $f(q)$. Applying (2), we have that
$$f(q)_m=\frac{(q^{n_1}-\varepsilon^{n_1})_m}{(n,q+1)_m}\geqslant\frac{m(q_0^{n_1}-\varepsilon^{n_1})_m}{(n,q_0+1)_m}=mf(q_0)_m.$$
Thus $mf(q_0)$ divides $f(q)$.

Finally, let $f(q_0)=p^l[q_0^{n_1}-\varepsilon^{n_1},q_0^{n_2}-\varepsilon^{n_2},\dots,q_0^{n_s}-\varepsilon^{n_s}]$, where $l\geqslant0$. A direct application of (1) shows that $mf(q_0)$ divides $f(q)$.

The proposition and the theorem are proved.

References

[1] W.J. Shi, *On the order and the element orders of finite groups: results and problems*, Ischia Group Theory 2010-Proceedings of the Conference (edited by Bianchi Mariagrazia et al.), World Scientific Publishing, 2011, 313–333.

[2] M.A. Grechkoseeva, W.J. Shi, A.V. Vasil'ev, *Recognition by spectrum for finite simple groups of Lie type*, Front. Math. China, **3**, No. 2 (2008), 275–285. MR2395222

[3] V.D. Mazurov, *Groups with a prescribed spectrum*, Izv. Ural. Gos. Univ. Mat. Mekh., **36** (2005), 119–138 [in Russian]. MR2190946

[4] W.J. Shi, *On the simple K_3-groups*, J. Southwest China Normal Univ.(N. S.), **13**, No. 3(1988), 1–4 [in Chinese]. Zbl 0731.20011

[5] V.D. Mazurov, *Recognition of finite groups by a set of orders of their elements*, Algebra and Logic, **37**, No. 6 (1998), 371–379. MR1680412

[6] V.D. Mazurov, M.C. Xu, H.P. Cao, *Recognition of the finite simple groups $L_3(2^m)$ and $U_3(2^m)$ by their element orders*, Algebra and Logic, **39**, No. 5 (2000), 324–334. MR1805756

[7] W.J. Shi, *A characterization of $U_3(2^n)$ by their element orders*, J. Southwest China Normal Univ.(N. S.), **25**, No. 4 (2000), 353–360. MR1784865

[8] V.D. Mazurov, G.Y. Chen, *Recognizability of the finite simple groups $L_4(2^m)$ and $U_4(2^m)$ by the spectrum*, Algebra and Logic, **47**, No. 1 (2008), 49–55. MR2408572

[9] W.J. Shi, H.L. Li, *A characterization of M_{12} and $PSU(6,2)$*, Acta Math. Sinica, **32**, No. 6 (1989), 758–764 [in Chinese]. MR1052219

[10] K. Zsigmondy, *Zur Theorie der Potenzreste*, Monatsh. Math. Phys., **3** (1892), 265–284. MR1546236

[11] A.A. Buturlakin, *Spectra of finite linear and unitary groups*, Algebra and Logic, **47**, No. 2 (2008), 91–99. MR2438007

[12] A.V. Zavarnitsine, *Recognition of the simple groups $U_3(q)$ by element orders*, Algebra and Logic, **45**, No. 2 (2006), 106–116. Zbl 1117.20010

[13] A.V. Zavarnitsine, *Recognition of the simple groups $L_3(q)$ by element orders*, J. Group Theory, **7**, No. 1 (2004), 81–97. MR2030231

[14] M.A. Grechkoseeva, *Recognition by spectrum for finite linear groups over fields of characteristic* 2, Algebra and Logic, **47**, No. 4 (2008), 229–241. MR2484562

[15] M.A. Grechkoseeva, *Quasirecognizability of simple unitary groups over fields of even order*, Sib. Electron. Math. Rep., **7** (2010), 435–444. MR2770864

[16] M.A. Grechkoseeva, *On element orders in covers of finite simple classical groups*, J. Algebra, **339** (2011), 304–319. MR2811323

[17] D. Gorenstein, R. Lyons, R. Solomon, *The classification of the finite simple groups. Number 3* (Mathematical Surveys and Monographs, **40.3**), Providence, RI, American Mathematical Society, 1998. MR1490581

[18] A.V. Vasil'ev, E.P. Vdovin, *An adjacency criterion for the prime graph of a finite simple group*, Algebra and Logic, **44**, No. 6 (2005), 381–406. MR2213302

[19] A.V. Vasil'ev, E.P. Vdovin, *Cocliques of maximal size in the prime graph of a finite simple group*, Algebra and Logic, **50**, No. 4 (2011), 291—322. MR2893582

[20] Huaiyu He, Wujie Shi, *A note on the ajacency criterion for the prime graph and characterization of $C_p(3)$*, Algebra Colloq., **19**, No. 3 (2012), 553—562. Zbl pre06073857

Maria Alexandrovna Grechkoseeva,
Sobolev Institute of Mathematics,
pr. Koptyuga, 4,
630090, Novosibirsk, Russia
E-mail address: gma@math.nsc.ru

Wujie Shi,
Department of Mathematics, Chongqing University of Arts and Sciences,
Yongchuan,
6402160, Chongqing, P.R. China
E-mail address: wjshi@suda.edu.cn