

Alireza Khalili Asboei; Ali Iranmanesh

A characterization of the linear groups  $L_2(p)$

*Czechoslovak Mathematical Journal*, Vol. 64 (2014), No. 2, 459–464

Persistent URL: <http://dml.cz/dmlcz/144009>

## Terms of use:

© Institute of Mathematics AS CR, 2014

Institute of Mathematics of the Czech Academy of Sciences provides access to digitized documents strictly for personal use. Each copy of any part of this document must contain these *Terms of use*.



This document has been digitized, optimized for electronic delivery and stamped with digital signature within the project *DML-CZ: The Czech Digital Mathematics Library* <http://dml.cz>

A CHARACTERIZATION OF THE LINEAR GROUPS  $L_2(p)$ 

ALIREZA KHALILI ASBOEI, Babol, ALI IRANMANESH, Tehran

(Received February 5, 2013)

*Abstract.* Let  $G$  be a finite group and  $\pi_e(G)$  be the set of element orders of  $G$ . Let  $k \in \pi_e(G)$  and  $m_k$  be the number of elements of order  $k$  in  $G$ . Set  $\text{nse}(G) := \{m_k : k \in \pi_e(G)\}$ . In fact  $\text{nse}(G)$  is the set of sizes of elements with the same order in  $G$ . In this paper, by  $\text{nse}(G)$  and order, we give a new characterization of finite projective special linear groups  $L_2(p)$  over a field with  $p$  elements, where  $p$  is prime. We prove the following theorem: If  $G$  is a group such that  $|G| = |L_2(p)|$  and  $\text{nse}(G)$  consists of  $1, p^2 - 1, p(p + \varepsilon)/2$  and some numbers divisible by  $2p$ , where  $p$  is a prime greater than 3 with  $p \equiv 1$  modulo 4, then  $G \cong L_2(p)$ .

*Keywords:* element order; set of the numbers of elements of the same order; linear group

*MSC 2010:* 20D06

## 1. INTRODUCTION

If  $n$  is an integer, then we denote by  $\pi(n)$  the set of all prime divisors of  $n$ . If  $G$  is a finite group, then  $\pi(|G|)$  is denoted by  $\pi(G)$ . We denote by  $\pi_e(G)$  the set of orders of its elements. It is clear that the set  $\pi_e(G)$  is closed and partially ordered by divisibility, and hence it is uniquely determined by  $\mu(G)$ , the subset of its maximal elements. Set  $m_i = m_i(G) := |\{g \in G; \text{the order of } g \text{ is } i\}|$  and  $\text{nse}(G) := \{m_i; i \in \pi_e(G)\}$ . In fact,  $m_i$  is the number of elements of order  $i$  in  $G$  and  $\text{nse}(G)$  is the set of sizes of elements with the same order in  $G$ .

Throughout this paper we denote by  $\varphi$  the Euler's totient function. If  $G$  is a finite group, then we denote by  $P_q$  a Sylow  $q$ -subgroup of  $G$  and by  $n_q(G)$  the number of Sylow  $q$ -subgroup of  $G$ , that is,  $n_q(G) = |\text{Syl}_q(G)|$ . All other notations are standard and we refer to [5], for example.

For the set  $\text{nse}(G)$ , the most important problem is related to Thompson's problem. In 1987, J. G. Thompson put forward the following problem. For each finite group  $G$  and each integer  $d \geq 1$ , let  $G(d) = \{x \in G; x^d = 1\}$ . Define  $G_1$  and  $G_2$  to be of the

same order type if, and only if,  $|G_1(d)| = |G_2(d)|$ ,  $d = 1, 2, 3, \dots$ . Suppose  $G_1$  and  $G_2$  are of the same order type. If  $G_1$  is solvable, is  $G_2$  necessarily solvable? (See [8], Problem 12.37.)

W. J. Shi in [12] made the above problem public in 1989. Unfortunately, no one can solve it or give a counterexample until now, and it remains open. The influence of  $\text{nse}(G)$  on the structure of finite groups was studied by some authors (see [10], [9], [1], [3]).

In [11], [2], it is proved that the groups  $A_4$ ,  $A_5$ ,  $A_6$ ,  $A_7$  and  $A_8$  are uniquely determined only by  $\text{nse}(G)$ . In [7] the authors show that the simple group  $L_2(q)$  is characterizable by  $\text{nse}(G)$  for each prime power  $4 \leq q \leq 13$ . In this article it is proved that the group  $L_2(p)$  where  $p > 3$  is prime is characterizable by  $\text{nse}(G)$  and the order of the group  $G$ . In fact the main theorem of our paper is as follows:

**Main theorem.** *Let  $p > 3$  be a prime of the form  $p = 4k + \varepsilon$  where  $\varepsilon = \pm 1$ , and suppose that  $G$  is a group with  $|G| = |L_2(p)| = p(p^2 - 1)/2$ . If  $\text{nse}(G)$  consists of 1,  $p^2 - 1$ ,  $p(p + \varepsilon)/2$  and some numbers divisible by  $2p$ , then  $G \cong L_2(p)$ .*

We note that there are finite groups which are not characterizable even by  $\text{nse}(G)$  and  $|G|$ . For example see the Remark in [10].

## 2. PRELIMINARY RESULTS

We first quote some lemmas that are used in deducing the main theorem of this paper.

**Lemma 2.1** ([6]). *Let  $G$  be a finite group and  $m$  be a positive integer dividing  $|G|$ . If  $L_m(G) = \{g \in G; g^m = 1\}$ , then  $m \mid |L_m(G)|$ .*

**Lemma 2.2** ([4], Theorem 1). *Let  $G$  be a finite non-abelian simple group whose order  $|G|$  is divisible by a prime  $p > |G|^{1/3}$ . Then  $G$  is isomorphic either to  $L_2(p)$  where  $p > 3$  is a prime or to  $L_2(p - 1)$  where  $p > 3$  is a Fermat prime.*

**Lemma 2.3.** *The set  $\text{nse}(L_2(p))$  where  $p = 4k + 1$  consists of the numbers 1,  $p^2 - 1$  and  $p(p + 1)/2$  together with all of the numbers of the form  $\varphi(r)p(p - 1)/2$  and all of the numbers  $\varphi(s)p(p + 1)/2$ , where  $r > 2$  is a divisor of  $(p + 1)/2$  and  $s > 2$  is a divisor of  $(p - 1)/2$ .*

**Proof.** The group  $L_2(p)$ , where  $p$  is prime, has two conjugacy classes of size  $(p^2 - 1)/2$ , which is related to elements of order  $p$ . So  $m_p(L_2(p)) = (p^2 - 1)$ . Also, this group has one conjugacy class of size  $p(p + 1)/2$ , which is related to elements of order 2.

So  $m_2(L_2(p)) = p(p+1)/2$ . Suppose that  $1 < r \mid (p+1)/2$ . By [13], Lemma 2.1, we have  $\mu(\text{PGL}_2(p)) = \{p-1, p, p+1\}$ , so  $\mu(L_2(p)) = \{(p-1)/2, p, (p+1)/2\}$ . Then  $r \in \pi_e(L_2(p))$ . To find  $m_r(L_2(p))$ , let  $H$  be a cyclic subgroup of order  $r$  of  $L_2(p) = T$ . We know  $|T : C_T(H)|$  is the size of the conjugacy class of an order  $r$  cyclic subgroup  $H$ . The group  $L_2(p)$  has  $(p-1)/4$  conjugacy classes of order  $p(p-1)$  and  $(p-5)/4$  conjugacy classes of order  $p(p+1)$ . Since  $r > 2$  divides  $p+1$ ,  $|T : C_T(H)| = p(p-1)$ .

Now we will show the number of conjugacy classes of such subgroups  $H$  is  $\varphi(r)/2$ . Since  $r > 2$  divides  $p+1$ , each element of order  $r$  lies in a unique, up to conjugation, subgroup  $R$  of order  $p+1$  of  $L_2(p) = T$ . Now,  $N_T(R) = R \rtimes C_2$ , is a dihedral group of order  $2(p+1)$ . So all elements of order  $r$  of  $R \rtimes C_2$  lie in a unique subgroup of order  $r$  of  $R$ . Therefore there are  $\varphi(r)$  elements of order  $r$  in  $N_T(R)$ . Now every element in  $R$  is conjugate to its inverse, so there are  $\varphi(r)/2$  classes of elements of order  $r$  in  $N_T(R)$ , hence there are  $\varphi(r)/2$  classes of elements of order  $r$  in  $L_2(p)$ . Therefore  $m_r(L_2(p)) = \varphi(r)p(p-1)/2$ .

Also if  $s > 2$  divides  $p-1$ , then by  $\mu(L_2(p))$ ,  $s \in \pi_e(L_2(p))$  and we can prove that  $m_s(L_2(p)) = \varphi(s)p(p+1)/2$ . □

**Lemma 2.4.** *The set  $\text{nse}(L_2(p))$  where  $p = 4k + 3$  consists of the numbers  $1$ ,  $p^2 - 1$  and  $p(p-1)/2$  together with all of the numbers of the form  $\varphi(r)p(p-1)/2$  and all of the numbers  $\varphi(s)p(p+1)/2$ , where  $r > 2$  is a divisor of  $(p+1)/2$  and  $s > 2$  is a divisor of  $(p-1)/2$ .*

*Proof.* The proof is similar to the proof of Lemma 2.3. □

Let  $p > 3$  be a prime of the form  $p = 4k + \varepsilon$  where  $\varepsilon = \pm 1$ . By Lemma 2.3 and 2.4, we note that if  $\text{nse}(G) = \text{nse}(L_2(p))$ , then  $\text{nse}(G)$  consists of  $1$ ,  $p^2 - 1$  and  $p(p + \varepsilon)/2$  and some numbers divisible by  $2p$ .

Let  $m_n$  be the number of elements of order  $n$ . We note that  $m_n = k\varphi(n)$ , where  $k$  is the number of cyclic subgroups of order  $n$  in  $G$ . Also we note that if  $n > 2$ , then  $\varphi(n)$  is even. If  $n \mid |G|$ , then by Lemma 2.1 and the above notation we have

$$(*) \quad \begin{cases} \varphi(n) \mid m_n, \\ n \mid \sum_{d \mid n} m_d. \end{cases}$$

In the proof of the main theorem, we often apply (\*) and the above comments.

### 3. PROOF OF THE MAIN THEOREM

Let  $G$  be a group such that  $|G| = |L_2(p)|$  and  $\text{nse}(G)$  consists of 1,  $p^2 - 1$  and  $p(p + \varepsilon)/2$  and some numbers divisible by  $2p$  where  $p = 4k + \varepsilon$  ( $\varepsilon = \pm 1$ ) is prime. The following lemmas reduce the problem to a study of groups with the same order as  $L_2(p)$ .

**Lemma 3.1.**

- (a)  $m_p(G) = m_p(L_2(p)) = (p^2 - 1)$  and  $n_p(G) = (p + 1)$ .
- (b)  $m_2 = p(p + \varepsilon)/2$ .

*Proof.* (a) By (\*),  $1 + m_p(G)$  is divisible by  $p$ , so  $m_p(G) \equiv -1 \pmod{p}$ . The only number in  $\text{nse}(G)$  that  $m_p(G) \equiv -1 \pmod{p}$  is  $p^2 - 1$ , so we must have  $m_p(G) = (p^2 - 1)$ . Since  $p^2 \nmid |G|$ ,  $m_p(G) = \varphi(p)n_p(G) = (p - 1)n_p(G) = (p^2 - 1)$ , so  $n_p(G) = (p + 1)$ .

(b) Since  $|G| = (1/2)(p - 1)p(p + 1)$ ,  $2 \mid |G|$  so  $m_2 \neq 1$ . Since  $2 \mid (1 + m_2)$ ,  $m_2$  is an odd number. On the other hand, the only odd number in  $\text{nse}(G)$  apart from 1 is  $p(p + \varepsilon)/2$  so  $m_2 = p(p + \varepsilon)/2$ . □

**Lemma 3.2.** *For each Sylow  $p$ -subgroup  $P$  of  $G$  we have  $P = C_G(P)$ . Since  $|P| = p$  this is equivalent to saying that there is no prime  $r \in \pi(G)$  for which  $rp \in \pi_e(G)$ .*

*Proof.* First we prove that for every  $r \in \pi(G)$  distinct from  $p$ ,  $p \mid m_r$ . If  $r = 2$ , then since  $m_r$  is odd and exceeds 1, we have  $m_r = p(p + \varepsilon)/2$  is divisible by  $p$ , as claimed. If  $r$  is not 2, then since  $r$  divides  $1 + m_r$  and  $r \neq p$  we cannot have  $m_r = 1$  or  $p^2 - 1$ . All other numbers in  $\text{nse}(G)$  are divisible by  $p$ . Thus  $p \mid m_r$ .

Now we show that  $rp \notin \pi_e(G)$  for every  $r \in \pi(G)$  distinct from  $p$ . Suppose  $rp \in \pi_e(G)$ . By (\*) we have  $rp \mid (1 + m_r + m_p + m_{rp})$ . We know that  $p \mid (1 + m_p) = p^2$  and  $p \mid m_r$ , so  $p \mid m_{rp}$ . We know that if  $P$  and  $Q$  are Sylow  $p$ -subgroups of  $G$ , then  $P$  and  $Q$  are conjugate, which implies that  $C_G(P)$  and  $C_G(Q)$  are conjugate in  $G$ . Therefore  $m_{rp} = \varphi(rp)n_p k$  where  $k$  is the number of cyclic subgroups of order  $r$  in  $C_G(P)$ . Since  $n_p = p + 1$  and  $\varphi(rp) = (r - 1)(p - 1)$  we have  $(p^2 - 1) \mid m_{rp}$ . On the other hand  $p \mid m_{rp}$  from the above, so  $p(p^2 - 1) \mid m_{rp}$ . This is a contradiction because  $|G| = (1/2)p(p^2 - 1)$ . Therefore there is no prime  $r \in \pi(G)$  for which  $rp \in \pi_e(G)$ . □

**Lemma 3.3.** *There exist normal subgroups  $N$  and  $H$  of  $G$  such that  $H/N$  is a simple group with order divisible by  $p$ .*

*Proof.* Let  $N$  normal in  $G$  be as large as possible with order not divisible by  $p$ . Then  $N < G$ , so we can choose a minimal normal subgroup  $H/N$  of  $G/N$ . Then

$H/N$  is of order divisible by  $p$  but not  $p^2$ . It must be a direct product of simple groups, so it is simple.  $\square$

**Lemma 3.4.**  $|N|$  is either 1 or  $p + 1$ , and if  $|N| = p + 1$ , then  $H/N$  has order  $p$  and  $p$  is a Mersenne prime.

*Proof.* Suppose  $|N| > 1$ . Let  $P$  be a Sylow  $p$ -subgroup of  $H$ . By  $C_N(P) = 1$  note that the action of  $P$  in  $N - \{1\}$  is fixed-point free, so  $|N| \geq p + 1$ . Now we have that  $N \cap N_G(P) = 1$ . It follows that  $|N|$  divides  $|G : N_G(P)| = p + 1$ , so  $|N| = p + 1$ , and we have  $NN_G(P) = G$ . It follows that  $NP$  is normal in  $G$ , and since  $H/N$  is simple, we see that  $H/N$  has order  $p$ . Also  $N$  is nilpotent. Choose  $r$  so that  $N$  has a nontrivial Sylow  $r$ -subgroup  $R$ . Then by the Frattini argument,  $H = NN_H(R)$ . Hence some Sylow  $p$ -subgroup  $Q$  of  $H$  normalizes  $R$  and acts fixed-point free, so  $|R| \geq p + 1$  and hence  $R = N$ . Thus  $p + 1$  is a power of  $r$ , and we have  $r = 2$ . Therefore  $p$  is Mersenne prime.  $\square$

**Lemma 3.5.** The case where  $|N| = p + 1$  is impossible.

*Proof.* Suppose  $|N| = p + 1$ . Then  $|G : N| = p(p - 1)/2$  which is odd since  $p$  is Mersenne. Thus the normal subgroup  $N$  contains all the elements of order 2 in  $G$ . This contradicts Lemma 3.1(b).  $\square$

**Lemma 3.6.**  $G$  is isomorphic to  $L_2(p)$ .

*Proof.* By Lemma 3.5 and 3.6,  $|N| = 1$ . We have  $H$  non-abelian since otherwise  $G$  has a normal Sylow  $p$ -subgroup. Since  $|G| = (1/2)(p - 1)p(p + 1)$ , by Lemma 2.2,  $H$  is either  $L_2(p)$  or  $L_2(p - 1)$ , where  $p$  is Fermat. In the second case  $|H| = \frac{1}{2}(p - 2) \times (p - 1)p$ , so  $p - 2$  divides  $|H|$ . Since  $|H|$  divides  $\frac{1}{2}(p - 1)p(p + 1)$ , we deduce that  $p - 2$  divides  $\frac{1}{2}(p - 1)p(p + 1)$  so  $p - 2$  divides  $p + 1$ , and this forces  $p = 5$ . Then  $H = L_2(4)$  which is isomorphic to  $L_2(5)$ , so we definitely have that  $H$  is  $L_2(p)$ , and thus  $G$  is isomorphic to  $L_2(p)$ .  $\square$

The proof of the main theorem is now complete.

**Acknowledgment.** The authors would like to thank the referee for valuable comments.

## References

- [1] *A. K. Asboei, S. S. S. Amiri, A. Iranmanesh, A. Tehranian*: A characterization of symmetric group  $S_r$ , where  $r$  is prime number. *Ann. Math. Inform.* *40* (2012), 13–23.
- [2] *A. K. Asboei, S. S. S. Amiri, A. Iranmanesh, A. Tehranian*: A new characterization of  $A_7$  and  $A_8$ . in *An. Ştiinţ. Univ. “Ovidius” Constanţa Ser. Mat* *21* (2013), 43–50.
- [3] *A. K. Asboei, S. S. S. Amiri, A. Iranmanesh, A. Tehranian*: A new characterization of sporadic simple groups by nse and order. *J. Algebra Appl.* *12* (2013), Paper No. 1250158.
- [4] *R. Brauer, W. F. Reynolds*: On a problem of E. Artin. *Ann. Math.* *68* (1958), 713–720.
- [5] *J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, R. A. Wilson*: Atlas of Finite Groups. Maximal subgroups and ordinary characters for simple groups. Clarendon Press, Oxford, 1985.
- [6] *G. Frobenius*: Verallgemeinerung des Sylow’schen Satzes. *Berl. Ber.* (1895), 981–993. (In German.)
- [7] *M. Khatami, B. Khosravi, Z. Akhlaghi*: A new characterization for some linear groups. *Monatsh. Math.* *163* (2011), 39–50.
- [8] *V. D. Mazurov, E. I. Khukhro*, eds.: The Kourovka Notebook. Unsolved Problems in Group Theory. Including archive of solved problems. Institute of Mathematics, Russian Academy of Sciences, Siberian Div., Novosibirsk, 2006.
- [9] *C. Shao, Q. Jiang*: A new characterization of Mathieu groups. *Arch. Math., Brno* *46* (2010), 13–23.
- [10] *C. Shao, W. Shi, Q. Jiang*: Characterization of simple  $K_4$ -groups. *Front. Math. China* *3* (2008), 355–370.
- [11] *R. Shen, C. Shao, Q. Jiang, W. Shi, V. Mazurov*: A new characterization of  $A_5$ . *Monatsh. Math.* *160* (2010), 337–341.
- [12] *W. Shi*: A new characterization of the sporadic simple groups. *Group Theory. Proceedings of the Singapore group theory conference 1987* (K. N. Cheng et al., eds.). Walter de Gruyter, Berlin, 1989, pp. 531–540.
- [13] *L. Zhang, X. Liu*: Characterization of the projective general linear groups  $PGL(2, q)$  by their orders and degree patterns. *Int. J. Algebra Comput.* *19* (2009), 873–889.

*Authors’ addresses*: Alireza Khalili Asboei (corresponding author), Department of Mathematics, Farhangian University, Shariati Mazandaran, Babol, Iran, and Department of Mathematics, College of Engineering, Buin Zahra Branch, Islamic Azad University, Buin Zahra, Iran, e-mail: [khaliliasbo@yahoo.com](mailto:khaliliasbo@yahoo.com); Ali Iranmanesh, Department of Mathematics, Faculty of Mathematical Sciences, Tarbiat Modares University, P. O. Box: 14115-137, Tehran, Iran, e-mail: [iranmanesh@modares.ac.ir](mailto:iranmanesh@modares.ac.ir).