sciendo
DOI: 10.2478/awutm-2019-0014

Analele Universităţii de Vest,
Timişoara
Seria Matematică – Informatică
LVII, 2, (2019), 53– 60

Recognition of the Simple Groups ${}^2\mathrm{D}_8((2^\mathrm{n})^2)$

Behnam Ebrahimzadeh

Abstract. One of the important problems in finite groups theory is group characterization by specific property. Properties, such as element orders, set of elements with the same order, the largest element order, etc. In this paper, we prove that the simple groups ${}^2D_8((2^n)^2)$ where, $2^{8n}+1$ is a prime number are uniquely determined by its order and the largest elements order.

AMS Subject Classification (2000). 20D06; 20D60.
Keywords. elements order; largest element order; prime graph.

1 Introduction

For a finite group G, the set of prime divisors of $|G|$ is denoted by $\pi(G)$ and the largest element of the set $\pi_e(G)$ of element orders of G is denoted by $k(G)$. The prime graph $\Gamma(G)$ of group G is a graph whose vertex set is $\pi(G)$, and where two vertices u and v are adjacent if and only if $uv \in \pi_e(G)$. Moreover, assume that $\Gamma(G)$ has $t(G)$ connected components π_i, for $i = 1, 2, \ldots, t(G)$. In the case where $|G|$ is of even order, we assume that $2 \in \pi_1$. Should mention that the other connected components are called the odd components. Let p be a prime. A group G is called a C_{pp} if $p \in \pi(G)$ and p is an isolated vertex of the prime graph of G. In the other words, the centralizers of its elements of order p in G are p-groups.

One of the important problems in finite groups theory is group characterization by specific property. Properties, such as elements order, set of elements with the same order, the largest elements order, etc. In fact, we say the group G is characterized by using the order of the group and the largest elements order, if there exist the group H, so that $k(G) = k(H)$ and $|G| = |H|$ implies that $G \cong H$. In the way, for example the authors in [1–8], [10], [13], [15] proved that the simple groups $L_3(q)$ and $U_3(q)$ where q is some special power of prime, the projective special linear group $L_2(q)$ where $q = p^n < 125$, the simple K_4 -groups of type $L_2(p)$, where p is a prime, also not of the form 2^n-1, the simple sporadic groups, $PGL(2, q)$, Suzuki group $Sz(q)$, where $q - 1$ or $q \pm \sqrt{2q} + 1$ is a prime number, $PSU_3(3^n)$, where $3^{2n} - 3^n + 1$ is a prime number and the simple K_5-groups of type $L_3(p)$, $PSP(8, q)$, where q be odd prime number and the symplectic group $C_4(q)$, where $q > 2$ and $\frac{q^4+1}{2}$ is a prime number by using the order of the group and the largest element order are proved. In this paper, we prove that the simple groups ${}^2D_8((2^n)^2)$, where $2^{8n} + 1$ is a prime number is recognized by the largest element order and the order of the group. In fact, we prove the following main theorem:

Main Theorem. Let G be a group and suppose that $D := {}^2D_8((2^n)^2)$ where $p := 2^{8n} + 1$ is a prime. Then, $|G| = |D|$ and $k(G) < 2p$ if and only if $G \cong D$.

2 Notation and Preliminaries

Lemma 2.1. [9] *Let G be a Frobenius group of even order with kernel K and complement H. Then*

1. *$t(G) = 2$, $\pi(H)$ and $\pi(K)$ are vertex sets of the connected components of $\Gamma(G)$;*
2. *$|H|$ divides $|K| - 1$;*
3. *K is nilpotent.*

Definition 2.1. *A group G is called a 2-Frobenius group if there is a normal series $1 \trianglelefteq H \trianglelefteq K \trianglelefteq G$ such that G/H and K are Frobenius groups with kernel K/H and H respectively.*

Lemma 2.2. [1] *Let G be a 2-Frobenius group of even order. Then*

1. *$t(G) = 2$, $\pi(H) \cup \pi(G/K) = \pi_1$ and $\pi(K/H) = \pi_2$;*
2. *G/K and K/H are cyclic groups satisfying $|G/K|$ divides $|Aut(K/H)|$.*

Lemma 2.3. [14] *Let G be a finite group with $t(G) \geq 2$. Then one of the following statements holds:*

1. *G is a Frobenius group;*
2. *G is a 2-Frobenius group;*
3. *G has a normal series $1 \trianglelefteq H \trianglelefteq K \trianglelefteq G$ such that H and G/K are π_1-groups, K/H is a non-abelian simple group, H is a nilpotent group and $|G/K|$ divides $|Out(K/H)|$.*

Lemma 2.4. [16] *Let q, k, l be natural numbers. Then*

1. $(q^k - 1, q^l - 1) = q^{(k,l)} - 1$.
2. $(q^k + 1, q^l + 1) = \begin{cases} q^{(k,l)} + 1 & \text{if both } \frac{k}{(k,l)} \text{ and } \frac{l}{(k,l)} \text{ are odd,} \\ (2, q+1) & \text{otherwise.} \end{cases}$
3. $(q^k - 1, q^l + 1) = \begin{cases} q^{(k,l)} + 1 & \text{if } \frac{k}{(k,l)} \text{ is even and } \frac{l}{(k,l)} \text{ is odd,} \\ (2, q+1) & \text{otherwise.} \end{cases}$

In particular, for every $q \geq 2$ and $k \geq 1$ the inequality $(q^k - 1, q^k + 1) \leq 2$ holds.

Example 2.1. Let R be $\mathbb{Z}_7 \times \mathbb{Z}_7 \times \mathbb{Z}_7 \times \mathbb{Z}_7 \times \mathbb{Z}_7$. Let the symmetric group of degree 5, S_5, act on R by permuting the coordinates. That is, for $\sigma \in S_5$, we define $(x_1, x_2, x_3, x_4, x_5)^\sigma = (x_{1\sigma^{-1}}, x_{2\sigma^{-1}}, x_{3\sigma^{-1}}, x_{4\sigma^{-1}}, x_{5\sigma^{-1}})$. We use this action to determine the semidirect product of R by S_5. Call it S. Now $D = \{(x, x, x, x, x) \mid x \in \mathbb{Z}_7\}$ is a normal subgroup of S and we let G be the factor group S/D. Now let H be R/D and K be $(R/D)((A_5)D/D)$. Then, we have a normal series $1 \trianglelefteq H \trianglelefteq K \trianglelefteq G$ so that K/H is isomorphic to the simple group A_5. Further, $C_G(0,0,0,0,1) = S_4 \times < (0,0,0,0,1) > \cong S_4 \times \mathbb{Z}_7$. Here S_4 is the "natural" S_4 as a subgroup of S_5 (that is the subgroup fixing a point). It follows that $\pi_1 = \{2, 3, 7\}$ and $\pi_2 = \{5\}$ are the connected components of $\Gamma(G)$. Note that $Out(A_5)$ has order 2, so $|G/K| = 2$ divides $|Out(K/H)|$. However, $k(K/H) = 5$ while $k(G) = 21$.

Lemma 2.5. *Suppose that $a > 1$ is an integer and let $N_a := \prod_{i=1}^{7}(a^{2i} - 1)$. Then*

1. $N_a \equiv -8(\mod (a^8 + 1))$. *Thus, $a^8 + 1$ does not divide N_a,*
2. $\frac{N_a}{a^8 - 1} \equiv -8(a^4 - 1)(\mod (a^8 - 1))$. *Thus, $(a^8 - 1)^2$ does not divide N_a,*

3. *Suppose that $i \geq 1$ is an integer which is not divisible by 7. Then $(\frac{a^7+1}{a+1}, a^{2i}-1)$ divides 7. Thus, if $a \geq 2$ is a power of 2, then $(\frac{a^7+1}{a+1}, a^{2i}-1) = 1$.*

Proof. i) First note that $a^8 \equiv -1(\mod (a^8+1))$, so we can write

$$N_a = \prod_{i=1}^{7}(a^{2i}-1) \equiv (a^2-1)(a^4-1)(a^6-1)(-2)(-a^2-1)(-a^4-1)(-a^6-1)$$
$$\equiv -(a^4-1)(a^8-1)(a^{12}-1)(-2) \equiv 2(a^4-1)(-2)(-a^4-1)$$
$$\equiv 4(a^8-1) \equiv -8(\mod (a^8+1))$$

ii) Note that $a^8 \equiv 1(\mod (a^8-1))$, so

$$\frac{Na}{a^8-1} \equiv ((a^2-1)(a^4-1)(a^6-1))^2 \equiv ((2-a^2-a^6)^2(a^4-1)^2$$
$$\equiv (6-4a^2+2a^4-4a^6)(2-2a^4) \equiv 8(1-a^4)(\mod (a^8-1).$$

It follows that if $(a^8-1) \mid \frac{N-1}{a^8-1}$, then $a^4+1 \mid 8$, a contradiction.
iii) Suppose that $i = 1, 2, 3$ then $(a+1)(\frac{a^7+1}{a+1}) - a^{7-2i}(a^{2i}-1) = a^{7-2i}+1$. Now, by Lemma 2.4 $(a^{2i}-1, a^{7-2i}+1) = a+1$. Now, clearly, $(\frac{a^7+1}{a+1}, a+1) \mid 7$, so $(\frac{a^7+1}{a+1}, a^{2i}-1) \mid 7$. Similarly, if $i \geq 4$ and 7 does not divide i, then $a^{2i-7}(a+1)(\frac{a^7+1}{a+1}) - (a^{2i}-1) = a^{2i-7}+1$. Now as above $(a^{2i}-1, a^{2i-7}+1) = a+1$, since 7 does not divide i, which implies that $(\frac{a^7+1}{a+1}, a^{2i}-1) \mid 7$, as above. Note that if a is a power of 2, then $a \equiv 1, 2, 4(\mod (7))$, so 7 does not divide $\frac{a^7+1}{a+1}$, and thus, $(\frac{a^7+1}{a+1}, a^{2i}-1) = 1$. Thus if 7 does not divide a, then $a^6 \equiv 1(\mod (7))$ and so $a^7 \equiv a(\mod (7))$, so 7 does not divide $\frac{a^7+1}{a+1}$. □

3 Proof of the Main Theorem

In this section, we prove the main theorem. To do this, we denote groups ${}^2D_8(q^2)$ by D, where $q = 2^n$ and $p = 2^{8n}+1$ is a prime number. We notice that $|{}^2D_8(q^2)| = q^{56}(q^8+1)\prod_{i=1}^{7}(q^{2i}-1)$ and $k({}^2D_8(q^2)) = (q+1)(q^7-1)$ (see [11]).
Note that $|{}^2D_8((2^n)^2)| = 2^{56n}(2^{8n}+1)N_{2^n} = q^{56}(q^8+1)N_q$. The above lemma thus implies that q^8+1 does not divide N_q and $(q^8-1)^2$ does not divide $|{}^2D_8((q)^2)|$.

Theorem 3.1. *Let G be a group and suppose that $D := {}^2D_8((2^n)^2)$ where $p := 2^{8n} + 1$ is a prime. Then, $|G| = |D|$ and $k(G) < 2p$ if and only if $G \cong D$.*

Proof. Throughout the proof we let $q := 2^n$ and $p := 2^{8n} + 1 = q^8 + 1$. Note that $8n$ must be a power of 2, so we let $8n := 2^s$ for some $s \geq 3$. Note that $p \mid |G|$, but p^2 does not.
($\Leftarrow$) Now we know that $k(D) = (q+1)(q^7-1)$. Thus, if $G \cong D$, then we have $|G| = |D|$ and $k(G) = k(D) = (q+1)(q^7-1) = q^8+q^7-q-1 < 2(q^8+1) = 2p$, since $2p - (q+1)(q^7-1) = (q^8-q^7)+(q+3) > 0$, as required.
($\Rightarrow$) The proof proceeds in a series of steps.

1.) p is an isolated vertex of $\Gamma(G)$.
Proof. Suppose that there is a prime $r \in \pi(G)$ so that $r \neq p$ and $pr \in \pi_e(G)$. Now $pr \geq 2p$ and so, $k(G) \geq 2p$, a contradiction.

2.) G is not a Frobenius group.
Proof. Suppose that G is a Frobenius group with kernel K and complement H. Now by Lemma 2.1(a) we have $t(G) = 2$; $\pi(H)$ and $\pi(K)$ are connected components of $\Gamma(G)$. Since p is an isolated vertex of $\Gamma(G)$ and $\{p\}$ is a connected component of $\Gamma(G)$, either $\pi(H) = \{p\}$ or $\pi(K) = \{p\}$.
i.) Assume that $|H| = p$. Then, $|K| = |G|/p$ and since $|H| \mid (|K|-1)$, we have $p \mid (|G|/p - 1)$. This says that $q^8 + 1 = p \mid q^{56}N_q - 1$. But as $q^{56} = (q^8)^7 \equiv -1(\mod (p))$, by the Lemma 2.5(i) $q^{56}N_q \equiv 8(\mod (p))$, contradiction.
ii.) If $|K| = p$, then $|G|/p \mid (p-1)$, and thus, $|G| \leq p(p-1)$, again a contradiction.

3.) G is not a 2-Frobenius group.
Proof. Suppose that G is a 2-Frobenius group. Then, by Lemma 2.2 there is a normal series $1 \trianglelefteq H \trianglelefteq K \trianglelefteq G$ so that G/H and K are Frobenius groups with kernels K/H and H, respectively. And also,$t(G) = 2$; $\pi(G/K) \cup \pi(H) = \pi_1$ and $\pi(K/H) = \pi_2$, G/K and K/H are cyclic groups satisfying $|G/K)| \mid |Aut(K/H)|$. Since p is an isolated vertex of $\Gamma(G)$, we must have that $\pi_2 = \{p\}$. (Recall p^2 doesn't divide $|G|$.) Thus, it follows that $|K/H| = p$ and that $|G/K| \mid (p-1) = 2^{8n}$. Now $|G| = |H||K/H||G/K| = |H| \cdot p \cdot 2^r$ for some $r \leq 8n$. It follows that $|H| = 2^{56n-r}N_q$. Since K is a Frobenius group with kernel H, we must have $p \mid (|H|-1)$. But $|H| - 1 = 2^{56n-r}N_p - 1 \equiv -2^{56n-r+3} - 1(\mod (p)$. Hence, $(2^{56n-r+3}+1, 2^{8n}+1) = 2^{8n}+1$. By the lemma in the paper we need $8n \mid (56n - r + 3)$ and so $8n \mid (r-3)$, a contradiction as $r \leq 8n$.

4.) We show that $G \cong D$.
Proof. By Lemma 2.3(iii), the group G has a normal series $1 \trianglelefteq H \trianglelefteq K \trianglelefteq G$ such that H and G/K are π_1-groups, K/H is a non-abelian simple group, H is nilpotent. It should be $|G/K|$ divides $|Out(K/H)|$. Note that since $p \mid |K/H|$ and p is an isolated vertex of $\Gamma(K/H)$, it follows that K/H is a simple C_{pp}-group with $p = 2^{8n} + 1$. Now by [12] we have that K/H must be one of the following .
i.) $Alt(p)$, $Alt(p+1)$, $Alt(p+2)$,
ii.) $A_1(r)$, $r = 2^{8n}$, p^k, $2 \cdot p^k \pm 1$ which is a prime, $8n \geq k \geq 1$, (Note here we must have $k = 1$),
iii.) $B_a(2^b)$, $ab = 8n$, $a \geq 2$,
iv.) $F_4(2^{2n})$,
v.) ${}^2D_{8n+1}(2)$,
vi.) ${}^2D_{a/2}(2^b)$; $ab = 16n$.
We go through all these cases.
i.) Suppose K/H is isomorphic to $Alt(p)$, $Alt(p+1)$, or $Alt(p+2)$. Note that $|K/H| \mid |G|$, since $p = 2^{8n} + 1 = 2^{2^s} + 1$, then $2^{e-1} \mid |K/H|$ where $e = 2^{2^s-1} \cdot 2^{2^s-2} \ldots 2^1 = 2^{2^s(2^s-1)/2} = 2^{2^{s-1}(2^s-1)} = 2^{4n(8n-1)} = 2^{32n^2-4n}$. Since $2^{32n^2-4n-1} > 56n$, we have a contradiction.
ii.) Suppose that K/H is isomorphic to $A_1(r)$ with $r = 2^{8n} = p-1$; p; $2p \pm 1$, for these last two possibilities r must be a prime. First, note that $|A_1(2^{8n})| = q^8(q^{16}-1)(q^8-1)$. It follows that $(q^8-1)^2$ divides $|G|$ and hence, $(q^8-1)^2$ divides N_q, a contradiction by Lemma 2.5. If $r = 2p+1$ is a prime, then K/H has an element of order $r > 2p$, contrary to assumption. Also, notice that if $r = 2p-1$, then r is not a prime as $r = 2(2^{8n}+1)-1 = 2^{8n+1}+1$ and $8n+1$ is not a power of 2. Now if $r = p$, then $2^{8n-1}+1 = \frac{(p+1)}{2}$ divides N_q. Now $2^{8n-1}+1$ divides $\prod_{i=1}^{7}(2^{2ni}-1, 2^{8n}-1)$. Using the result of Lemma 2.4(iii) we get $2^{8n-1}+1$ divides $3^9 \cdot 11 \cdot 43$. An easy check shows that this only happens when $n = 1$; $q = 2$. It is easy to check that in this case $|K/H|$ does not divide $|G|$, a contradiction.
iii.) Suppose that K/H is isomorphic to $B_a(2^b)$, $ab = 8n$, $a \geq 2$. Now we know that $|B_a(2^b)| = (2^b)^{a^2} \prod_{i=1}^{a}((2^b)^{2i} - 1)$. We see that the power of 2 which divides $|B_a(2^b)|$ is $(2^b)^{a^2} = 2^{(ab)a} = 2^{(8n)a}$. It follows that $a \leq 7$. Since n is a power of 2, we see that either $a = 2$ or $a = 4$. If $a = 2$, then $|B_2(2^{4n})| = q^{16}(q^8-1)(q^{16}-1)$. It follows that $(q^8-1)^2$ divides $|G|$ and so $(q^8-1)^2$ divides N_q, a contradiction by Lemma 2.5(ii). If $a = 4$, then $|B_4(2^{2n})| = q^{32}(q^4-1)(q^8-1)(q^{12}-1)(q^{16}-1)$, and again we get $(q^8-1)^2$ divides N_q, a contradiction.
iv). Suppose that K/H is isomorphic to $F_4(2^{2n})$. Again, it follows that

$(q^8-1)^2$ divides $|K/H|$ and hence, divides $|G|$ again a contradiction.
v). Suppose that K/H is isomorphic to $^2D_{8n+1}(2)$. Now the power of 2 which divides $|K/H|$ is $2^{(8n+1)8n}$ which is a contradiction, as $(8n+1)8n > 56n$. The only possibility remaining is that K/H is isomorphic to $^2D_{a/2}(2^b)$ where $a \geq 8$ and $ab = 16n$. Recall that $8n = 2^s$. It follows that the power of 2 which divides $|K/H|$ is $(2^b)^{a/2(a/2-1)} = 2^{8n(a/2-1)}$. Now we must have $a/2 - 1 \leq 7$, so $a \leq 16$. It follows that either $a = 8$ or $a = 16$. Now if $a = 8$, then note that $|^2D_4(2^{2n})| = q^{24}(q^8+1)(q^4-1)(q^8-1)(q^{12}-1)$. Let r be a prime so that $r \mid \frac{q^7+1}{q+1}$. It is easy to see that r does not divide $|^2D_4(2^{2n})|$, as follows that $|G/K| \mid |Out(^2D_4(2^{2n}))|$ is a power of 2. It follows that $r \mid |H|$. Let R be a Sylr(G). Then it is clear that $R \leq H$. As H is nilpotent, then $R \trianglelefteq G$. Suppose x is an element of G of order $p = q^8 + 1$. Now x acts as an automorphism of R, but as $|R| \mid \frac{q^7+1}{q+1}$, $|R| < |x|$ and it follows that x must centralize R. This means that G contains an element of order $pr > 2p$, a contradiction. Thus, the only possibility is that $a = 16$ and K/H is isomorphic to $^2D_8(2^n) \cong D$. It follows that $|G| = |K/H|$ and thus, that $H = 1$ and $G = K$. Thus, $G \cong D$, as required. □

Acknowledgement

The authors express their sincere thanks to the referee for the valuable comments which highly improved the original manuscript.

References

[1] **G. Y. Chen**, On the structure of Frobenius groups and 2-Frobenius groups, *J. Southwest China Normal University*, **20** (5), (1995), 485-487

[2] **G. Y. Chen, L. G. He, and J. H. Xu**, A new characterization of sporadic simple groups, *Italian Journal of Pure and Applied Mathematics*, **30**, (2013), 373-392

[3] **G. Y. Chen and L. G. He**, A new characterization of $L_2(q)$ where $q = p^n < 125$, *Italian Journal of Pure and Applied Mathematics*, **38**, (2011), 125-134

[4] **G. Y. Chen and L. G. He**, A new characterization o Simple K_4 -group with type $L_2(p)$, *Advances in Mathematics (China)*, (2012), doi: 10.11845/sxjz.165b

[5] **B. Ebrahimzadeh, A. Iranmanesh, A. Tehranian, and H. Parvizi Mosaed**, A Characterization of the Suzuki groups by order and the Largest elements order, *Journal of Sciences, Islamic Republic of Iran*, **27** (4), (2016), 353-355

[6] **B. Ebrahimzadeh and R. Mohammadyari**, A new characterization of projective special unitary groups $PSU_3(3^n)$, *Discussiones Mathematicae General Algebra and Applications*, **39**, (2019), 35-41

[7] **B. Ebrahimzadeh, M. Y. Sadeghi, A. Iranmanesh, and A. Tehranian**, A new characterization of symplectics groups $PSP(8, q)$, *An. Ştiinţ. Univ. Al. I. Cuza Iaşi. Mat. (N.S.)*, **LXVI** (1), (2020), 93-99

[8] **B. Ebrahimzadeh, R. Mohammadyari, and M. Y. Sadeghi**, A New Characterization of the simple groups $C_4(q)$, by its order and the largest order of elements, *Acta et Commentationes Universitatis Tartuensis de Mathematica*, **23** (2), (2019)

[9] **D. Gorenstein**, *Finite groups*, Harper and Row, New York, 1980

[10] **L. G. He and G. Y. Chen**, A new characterization of $L_3(q)$ $(q \leq 8)$ and $U_3(q)$ $(q \leq 11)$, *J. Southwest Univ. (Natur. Sci.)*, **27** (33), (2011), 81-87

[11] **W. M. Kantor and A. Seress**, Large element orders and the characteristic of Lie-type simple groups, *J. Algebra*, **322**, (2009), 802-832

[12] **A. Khosravi and B. Khosravi**, A new characterization of some alternting and symmetric groups, *Int. J. Math. and Math. Sci*, (2003), 2863-2872

[13] **J. Li, W. Shi, and D. Yu**, A characterization of some $PGL(2, q)$ by maximum element orders, *Bull.Korean Math.Soc*, **52** (6), (2015), 2025-2034

[14] **J. S. Williams**, Prime graph components of finite groups, *J. Algebra*, **69** (2), (1981), 487-513

[15] **D. Yu, J. Li, G. Chen, L. Zhang, and W. J. Shi**, A new characterization of simple K_5-groups of type $L_3(p)$, *Bulletin of the Iranian Mathematical Society*, **45** (3), (2019), 771-781

[16] **A. V. Zavarnitsine**, Recognition of the simple groups $L_3(q)$ by element orders, *J. Group Theory*, **7** (1), (2004), 81-97

Behnam Ebrahimzadeh

Young Researchers and Elite Club, Science and Research Branch, Islamic Azad university, Tehran, Iran

E-mail: `behnam.ebrahimzadeh@gmail.com`