International Electronic Journal of Algebra
Volume 16 (2014) 32-52

SOME QUANTITATIVE CHARACTERIZATIONS OF CERTAIN SYMPLECTIC GROUPS OVER THE BINARY FIELD

M. Akbari and A. R. Moghaddamfar

Received: 2 December 2013; Revised: 1 April 2014
Communicated by Arturo Magidin

Abstract. Given a finite group G, denote by $\mathrm{D}(G)$ the degree pattern of G and by $\mathrm{OC}(G)$ the set of all order components of G. Denote by $h_{\mathrm{OD}}(G)$ (resp. $h_{\mathrm{OC}}(G)$) the number of isomorphism classes of finite groups H satisfying conditions $|H| = |G|$ and $\mathrm{D}(H) = \mathrm{D}(G)$ (resp. $\mathrm{OC}(H) = \mathrm{OC}(G)$). A finite group G is called OD-characterizable (resp. OC-characterizable) if $h_{\mathrm{OD}}(G) = 1$ (resp. $h_{\mathrm{OC}}(G) = 1$). Let $C = C_p(2)$ be a symplectic group over the binary field, for which $2^p - 1 > 7$ is a Mersenne prime. The aim of this article is to prove that $h_{\mathrm{OD}}(C) = 1 = h_{\mathrm{OC}}(C)$.

Mathematics Subject Classification 2010: 20D05, 20D06, 20D08
Keywords: Spectrum of a group, prime graph, degree pattern, order component, symplectic group $C_n(q)$, OD(OC)-characterizability of a finite group

1. Introduction

Only finite groups will be considered. Let G be a group, $\pi(G)$ the set of all prime divisors of its order and $\omega(G)$ be the spectrum of G, that is the set of its element orders. The *prime graph* $\mathrm{GK}(G)$ (or *Gruenberg-Kegel graph*) of G is a simple graph whose vertex set is $\pi(G)$ and two distinct vertices p and q are joined by an edge if and only if $pq \in \omega(G)$. Let $t(G)$ be the number of connected components of $\mathrm{GK}(G)$. The vertex set of the ith connected component of $\mathrm{GK}(G)$ is denoted by $\pi_i(G)$ for each $i = 1, 2, \ldots, t(G)$. In the case when $2 \in \pi(G)$, we assume that $2 \in \pi_1(G)$. The classification of finite simple groups with disconnected prime graph was obtained by Williams [13] and Kondratév [4]. Recall that a *clique* in a graph is a set of pairwise adjacent vertices. Note that for all non-abelian simple groups S with disconnected prime graph, all connected components $\pi_i(S)$ for $2 \leqslant i \leqslant t(S)$ are cliques, for instance, see [13]. The *degree* $\deg_G(p)$ of a vertex $p \in \pi(G)$ in $\mathrm{GK}(G)$ is the number of edges incident on p. If $\pi(G) = \{p_1, p_2, \ldots, p_h\}$ with $p_1 < p_2 < \cdots < p_h$, then we define

$$\mathrm{D}(G) = \big(\deg_G(p_1), \deg_G(p_2), \ldots, \deg_G(p_h)\big),$$

which is called the *degree pattern of* G. Given a group G, denote by $h_{\rm OD}(G)$ the number of isomorphism classes of groups with the same order and degree pattern as G. All finite groups, in terms of the function $h_{\rm OD}(\cdot)$, are classified as follows:

Definition 1.1. A group G is called k-fold OD-characterizable if $h_{\rm OD}(G) = k$. Usually, a 1-fold OD-characterizable group is simply called OD-characterizable.

There are scattered results in the literature showing that certain simple groups are k-fold OD-characterizable for $k \in \{1, 2\}$. The most recent version of the list of such simple groups is presented in [8, Tables 2 and 3]. Until now, no examples of simple groups S with $h_{\rm OD}(S) \geqslant 3$ were known. Therefore, we posed the following question:

Problem 1.2. *Is there a non-abelian simple group S with $h_{\rm OD}(S) \geqslant 3$?*

In this article, we focus our attention on the symplectic groups $C_p(2) \cong S_{2p}(2)$, where p is an odd prime. Recall that $C_2(2)$ is not a simple group, in fact, the derived subgroup $C_2(2)'$ is a simple group which is isomorphic with $A_6 \cong L_2(9)$. In addition, we recall that $B_2(3) \cong {}^2A_4(2^2)$, $B_n(2^m) \cong C_n(2^m)$ and $B_2(q) \cong C_2(q)$ (see [2]). Previously, it was determined the values of $h_{\rm OD}(\cdot)$ for some symplectic and orthogonal groups (see [1,6,9]). In the table below, $\pi(n)$ is the set of all prime divisors of n, where n is a natural number.

G	Restrictions on G	$h_{\rm OD}(G)$	Refs.
$B_3(4) \cong C_3(4)$		1	[6]
$B_2(q) \cong C_2(q)$	$\lvert\pi(\frac{q^2+1}{(2,q-1)})\rvert = 1$	1	[1]
$B_{2^m}(q) \cong C_{2^m}(q)$	$\lvert\pi(\frac{q^2+1}{(2,q-1)})\rvert = 1$, q is even	1	[1]
$B_3(5)$, $C_3(5)$,		2	[1]
$B_n(q)$, $C_n(q)$,	$n = 2^m > 2$, $\lvert\pi(\frac{q^n+1}{2})\rvert = 1$, q is an odd prime power	2	[1]
$B_p(3)$, $C_p(3)$,	$\lvert\pi(\frac{3^p-1}{2})\rvert = 1$, p is an odd prime,	2	[1,9]

Given a group G, the order of G can be expressed as a product of some coprime natural numbers $m_i(G)$, $i = 1, 2, \ldots, t(G)$, with $\pi(m_i(G)) = \pi_i(G)$. The numbers $m_1(G), m_2(G), \ldots, m_{t(G)}(G)$ are called the *order components of* G. We set

$$\mathrm{OC}(G) = \{m_1(G), m_2(G), \ldots, m_{t(G)}(G)\}.$$

In a similar manner, we define $h_{\rm OC}(G)$ as the number of isomorphism classes of finite groups with the same set $\rm OC(G)$ of order components. Again, in terms of function $h_{\rm OC}(\cdot)$, the groups G are classified as follows:

Definition 1.3. A finite group G is called k-fold OC-characterizable if $h_{\rm OC}(G) = k$. In the case when $k = 1$ the group G is simply called OC-characterizable.

A Mersenne prime is a prime that can be written as $2^p - 1$ for some prime p. The purpose of this article is to prove the following theorem.

Main Theorem. *Let $C = C_p(2)$ be the symplectic group over the binary field, for which $2^p - 1 > 7$ is a Mersenne prime. Then $h_{\rm OD}(C) = 1 = h_{\rm OC}(C)$.*

It is worth noting that the values of functions $h_{\rm OD}(\cdot)$ and $h_{\rm OC}(\cdot)$ may be different. For instance, suppose $M \in \{B_3(5), C_3(5)\}$. By [13], the prime graph associated with M is connected and so $\mathrm{OC}(M) = \{|M|\} = \{2^9 \cdot 3^4 \cdot 5^9 \cdot 7 \cdot 13 \cdot 31\}$. On the other hand, it is easy to see that the prime graph associated with a nilpotent group is always a clique, hence, we have

$$h_{\rm OC}(M) > \nu_{\rm nil}(|M|) \geqslant \nu_{\rm a}(|M|) = \mathrm{Par}(9)^2 \cdot \mathrm{Par}(4) = 30^2 \times 5 = 4500,$$

where $\nu_{\rm nil}(n)$ (resp. $\nu_{\rm a}(n)$) signifies the number of non-isomorphic nilpotent (resp. abelian) groups of order n and $\mathrm{Par}(n)$ denotes the number of partitions of n. However, by Theorem 1.3 in [1], we know that $h_{\rm OD}(M) = 2$.

2. Preliminaries

If a is a natural number, r is an odd prime and $(r, a) = 1$, then by $e(r, a)$ we denote the multiplicative order of a modulo r, that is the minimal natural number n with $a^n \equiv 1 \pmod r$. If a is odd, we put $e(2, a) = 1$ if $a \equiv 1 \pmod 4$, and $e(2, a) = 2$ if $a \equiv -1 \pmod 4$. The following lemma is a consequence of Zsigmondy's Theorem (see [14]).

Lemma 2.1. *Let $a > 1$ be an integer. Then for every natural number n there exists a prime r with $e(r, a) = n$ except for the cases $(n, a) \in \{(1, 2), (1, 3), (6, 2)\}$.*

A prime r with $e(r, a) = n$ is called a *primitive prime divisor* of $a^n - 1$. By Lemma 2.1, such a prime exists except for the cases mentioned in the lemma. We denote by $\mathrm{ppd}(a^n - 1)$ the set of all primitive prime divisors of $a^n - 1$. By our definition, we have $\pi(a - 1) = \mathrm{ppd}(a - 1)$ but for the following sole exception, namely, $2 \notin \mathrm{ppd}(a - 1)$ if $e(2, a) = 2$. In this case, we assume that $2 \in \mathrm{ppd}(a^2 - 1)$.

From the definition it is easy to conclude that: Let $p > 2$ be an integer. Then $\pi(a^p - 1) = \mathrm{ppd}(a^p - 1)$ if and only if p is a prime.

In the following results, we will consider the function $\eta : \mathbb{N} \to \mathbb{N}$, which is defined as follows

$$\eta(m) = \begin{cases} m & \text{if} \quad m \equiv 1 \pmod 2, \\ m/2 & \text{if} \quad m \equiv 0 \pmod 2). \end{cases}$$

Lemma 2.2. ([11]) *Let M be one of the simple groups of Lie type $B_n(q)$ or $C_n(q)$ over a field of characteristic p, and let $r \in \pi(M) \setminus \{p\}$ and $r \in \mathrm{ppd}(q^k - 1)$. Then r and p are non-adjacent if and only if $\eta(k) > n - 1$.*

Lemma 2.3. ([12]) *Let M be one of the simple groups of Lie type $B_n(q)$ or $C_n(q)$ over a field of characteristic p. Let r, s be odd primes with $r, s \in \pi(M) \setminus \{p\}$. Suppose that $r \in \mathrm{ppd}(q^k - 1)$, $s \in \mathrm{ppd}(q^l - 1)$ and $1 \leqslant \eta(k) \leqslant \eta(l)$. Then r and s are non-adjacent if and only if $\eta(k) + \eta(l) > n$ and l/k is not an odd natural number.*

Using Lemmas 2.2 and 2.3, we conclude that the prime graphs $\mathrm{GK}(B_n(q))$ and $\mathrm{GK}(C_n(q))$ coincide (see also [11, Proposition 7.5]), and hence

$$\mathrm{D}(B_n(q)) = \mathrm{D}(C_n(q)).$$

Corollary 2.4. *Let $p > 3$ be a prime and $C = C_p(2)$. Then $\deg_C(3) = |\pi_1(C)| - 1$.*

Proof. Recall that, by [4], we have

$$\pi_1(C) = \pi\left(2(2^p + 1)\prod_{i=1}^{p-1}(2^{2i} - 1)\right) \quad \text{and} \quad \pi_2(C) = \pi(2^p - 1).$$

Now, it follows from Lemma 2.3 that all primitive prime divisors of $2^p - 1$ (and so all primes in $\pi(2^p - 1)$) are non-adjacent to 3. On the other hand, by Lemmas 2.2 and 2.3, we deduce that $\deg_C(3) = |\pi_1(C)| - 1$, as desired. □

The following lemma is crucial to the study of characterizability of symplectic groups $C_p(2)$ by order components.

Lemma 2.5. ([3]) *Let G be a group whose prime graph has more than one component. If H is a normal $\pi_k(G)$-subgroup of G, then $|H| - 1$ is divisible by $m_i(G)$, for all $i \neq k$.*

A group G is called 2-*Frobenius* if there exists a normal series $1 \trianglelefteq H \trianglelefteq K \trianglelefteq G$ of G such that H is the Frobenius kernel of K and K/H is the Frobenius kernel of G/H.

Lemma 2.6. ([7]) *Let S be a simple group with disconnected prime graph* $\mathrm{GK}(S)$, *except $U_4(2)$ and $U_5(2)$. If G is a finite group with* $\mathrm{OC}(G) = \mathrm{OC}(S)$, *then G is neither a Frobenius group nor a 2-Frobenius group.*

Lemma 2.7. ([13]) *Let G be a group with $t(G) \geqslant 2$. Then one of the following hold:*

(1) *G is a Frobenius group;*
(2) *G is a 2-Frobenius group; or*
(3) *G has a normal series $1 \trianglelefteq H \triangleleft K \trianglelefteq G$ such that H is a nilpotent π_1-group, K/H is a non-abelian simple group, G/K is a π_1-group, $|G/K|$ divides $|\mathrm{Out}(K/H)|$ and any odd order component of G is equal to one of the odd order components of K/H.*

Lemma 2.8. ([5]) *The only solution of the equation $p^m - q^n = 1$, where p, q are primes and $m, n > 1$ are integers, is $(p, q, m, n) = (3, 2, 2, 3)$.*

Given a natural number B and a prime number t, we denote by B_t the t-part of B, that is the largest power of t dividing B.

Lemma 2.9. ([10]) *Let $B = (2^2 - 1)(2^4 - 1) \cdots (2^{2n} - 1)$. If t is a prime divisor of B, then $B_t < 2^{3n}$. Furthermore, if $t \geqslant 5$ then $B_t < 2^{2n}$.*

3. Proof of the main theorem

Throughout this section, we will assume that $2^p - 1 > 7$ is a Mersenne prime and $C = C_p(2)$. Suppose that G is a group with the same order and degree pattern as C, that is

$$|G| = |C| = 2^{p^2} \prod_{i=1}^{p} (2^{2i} - 1) \quad \text{and} \quad \mathrm{D}(G) = \mathrm{D}(C).$$

Note that, according to the results summarized in [4], we have $t(C) = 2$, and

$$\pi_1(C) = \pi\left(2(2^p + 1) \prod_{i=1}^{p-1} (2^{2i} - 1)\right) \quad \text{and} \quad \pi_2(C) = \{2^p - 1\}.$$

By our hypothesis, it is easy to see that

$$\pi_2(G) = \pi_2(C) = \{2^p - 1\} \quad \text{and} \quad \pi(G) = \pi(C) = \pi_1(C) \cup \{2^p - 1\}.$$

First of all, we notice that $2^p - 1$ is the largest prime in $\pi(G) = \pi(C)$. Moreover, it follows from Corollary 2.4 that

$$\deg_G(3) = \deg_C(3) = |\pi_1(C)| - 1,$$

and this forces $\pi_1(G) = \pi_1(C)$, and so $t(G) = 2$. Hence, we have

$$\mathrm{OC}(G) = \mathrm{OC}(C) = \left\{ 2^{p^2}(2^p+1)\prod_{i=1}^{p-1}(2^{2i}-1),\quad 2^p-1 \right\},$$

and from Lemma 2.6, the group G is neither a Frobenius group nor a 2-Frobenius group. Finally, Lemma 2.7, reduces the problem to the study of the simple groups. Indeed, by Lemma 2.7, there is a normal series $1 \trianglelefteq H \lhd K \trianglelefteq G$ of G such that:

(1) H is a nilpotent $\pi_1(G)$-group, K/H is a non-abelian simple group and G/K is a $\pi_1(G)$-group. Moreover, we have $K/H \leqslant G/H \leqslant \mathrm{Aut}(K/H)$, and $t(K/H) \geqslant t(G) \geqslant 2$,
(2) $2^p - 1$ is the only odd order component of G which is equal to one of those of the quotient K/H,
(3) $|G/K|$ divides $|\mathrm{Out}(K/H)|$.

For odd order components of K/H see [4,13]. Now, we will continue the proof step by step.

Step 3.1. *$K/H \ncong {}^2A_3(2), {}^2F_4(2)', {}^2A_5(2), E_7(2), E_7(3), A_2(4), {}^2E_6(2)$ nor one of the sporadic simple groups.*

Note that either the odd order components of above groups are not equal to a Mersenne prime $2^p - 1 > 7$ or their orders do not divide the order of G.

In the following, $\mathbb{A}_n$ denotes the alternating group on n letters.

Step 3.2. *$K/H \ncong \mathbb{A}_n$, where n and $n-2$ are both prime numbers.*

In this case, it follows that $n = 2^p - 1$. Now, simple computations show that

$$|\mathbb{A}_n|_2 = \left(\frac{n!}{2}\right)_2 = 2^{\left(\left[\frac{n}{2}\right]+\left[\frac{n}{2^2}\right]+\cdots\right)-1} = 2^{2^p-p-2}.$$

If $p > 5$, then $2^p - p - 2 > p^2$ and hence the 2-part of $|\mathbb{A}_n|$ does not divide the 2-part of $|G|$, i.e. 2^{p^2}, which is a contradiction. In the case when $p = 5$, then $n = 31$ and $|K/H| = (31!)/2$, which does not divide $|G| = |C_5(2)| = 2^{25}\cdot 3^6\cdot 5^2\cdot 7\cdot 11\cdot 17\cdot 31$, which is again a contradiction.

Step 3.3. *$K/H \ncong \mathbb{A}_n$, where $n = q$, $q+1$, or $q+2$ (q is a prime), and one of n, $n-2$ is not prime.*

Here, q is the only odd order component of K/H, and so $q = 2^p - 1$. We now consider the alternating group $\mathbb{A}_q$ which is a subgroup of $K/H \cong \mathbb{A}_n$. Similar arguments as those in the previous step, on the subgroup $\mathbb{A}_q$ instead of $\mathbb{A}_n$, lead us a contradiction.

Step 3.4. *K/H is isomorphic to neither ${}^2E_6(q)$, $q > 2$, nor $E_6(q)$.*

We deal with ${}^2E_6(q)$, $q > 2$, the proof for $E_6(q)$ being quite similar. Suppose that $K/H \cong {}^2E_6(q)$. First of all, we recall that

$$|{}^2E_6(q)| = \frac{1}{(3, q+1)} q^{36}(q^{12} - 1)(q^9 + 1)(q^8 - 1)(q^6 - 1)(q^5 + 1)(q^2 - 1).$$

Considering the only odd order component of ${}^2E_6(q)$, that is $(q^6 - q^3 + 1)/(3, q+1)$, we must have $(q^6 - q^3 + 1)/(3, q + 1) = 2^p - 1$, which implies that $q^9 > 2^p$, or equivalently $q^{36} > 2^{4p}$. Let $q = r^f$. If r is an odd prime, then from Lemma 2.9, we get

$$q^{36} = r^{36f} = |K/H|_r \leqslant |G|_r < 2^{3p},$$

which is a contradiction. Therefore we may assume that $r = 2$. In this case, we have

$$(2^{6f} - 2^{3f} + 1)/(3, 2^f + 1) = 2^p - 1.$$

Now, if $(3, 2^f + 1) = 1$, then we obtain $2^{3f}(2^{3f} - 1) = 2(2^{p-1} - 1)$, from which we deduce that $3f = 1$, a contradiction. In the case where $(3, 2^f + 1) = 3$, an easy calculation shows that

$$2^{3f}(2^{3f} - 1) = 2^2(3 \cdot 2^{p-2} - 1),$$

and so $3f = 2$, which is again a contradiction.

Step 3.5. *$K/H \ncong F_4(q)$, where q is an odd prime power.*

We remark that $q^4 - q^2 + 1$ is the only odd order component of $F_4(q)$, and clearly this forces $q^4 - q^2 + 1 = 2^p - 1$. Then $q^2(q^2 - 1) = 2(2^{p-1} - 1)$, which shows that $2(2^{p-1} - 1)$ is divisible by 4, a contradiction.

Step 3.6. *$K/H \ncong {}^2B_2(q)$, where $q = 2^{2m+1} > 2$.*

Recall that $|{}^2B_2(q)| = q^2(q^2 + 1)(q - 1)$ and the odd order components of ${}^2B_2(q)$ are:

$$q - 1, \quad q - \sqrt{2q} + 1, \quad q + \sqrt{2q} + 1.$$

If $q - 1 = 2^p - 1$, then $q = 2^p$. Now, we consider the primitive prime divisor $r \in \mathrm{ppd}(2^{4p} - 1)$. Clearly $r \in \pi(2^{2p} + 1)$, and so $r \in \pi({}^2B_2(q)) \subseteq \pi(G)$. This is a contradiction.

In the case when

$$q - \sqrt{2q} + 1 = 2^p - 1 \ \ (\text{resp. } \ q + \sqrt{2q} + 1 = 2^p - 1),$$

by simple computations we obtain

$$2^{m+1}(2^m-1)=2(2^{p-1}-1)\ \ (\text{resp. } 2^{m+1}(2^m+1)=2(2^{p-1}-1)),$$

a contradiction.

Step 3.7. *$K/H\ncong E_8(q)$, where $q\equiv 2,3 \pmod 5$.*

The odd order components of $E_8(q)$ in this case are

$$q^8-q^4+1,\qquad \frac{q^{10}+q^5+1}{q^2+q+1},\qquad \frac{q^{10}-q^5+1}{q^2-q+1}.$$

If $q^8-q^4+1=2^p-1$, then we obtain $q^4(q-1)(q+1)(q^2+1)=2(2^{p-1}-1)$. However, the left hand side is divisible by 16, while the right hand side is not divisible by 4, which is impossible.

If $(q^{10}+q^5+1)/(q^2+q+1)=2^p-1$, then after subtracting 1 from both sides of this equation and some simple computations, we obtain

$$q(q-1)(q+1)(q^2+1)(q^3-q^2+1)=2(2^{p-1}-1).$$

Now, if q is odd, then the left hand side is divisible by 16, a contradiction. Moreover, if q is even, then it follows that $q=2$, and if this is substituted in above equation we get $76=2^{p-1}$, a contradiction.

The case $(q^{10}-q^5+1)/(q^2-q+1)=2^p-1$ is quite similar to the previous case and it is omitted.

Step 3.8. *$K/H\ncong E_8(q)$, where $q\equiv 0,1,4 \pmod 5$.*

The odd order components of $E_8(q)$ in this case are

$$\frac{q^{10}+1}{q^2+1},\quad q^8-q^4+1,\quad \frac{q^{10}+q^5+1}{q^2+q+1},\quad \frac{q^{10}-q^5+1}{q^2-q+1}.$$

Consider the first case. Let $(q^{10}+1)/(q^2+1)=2^p-1$. Subtracting 1 from both sides of this equality, we get

$$q^2(q^2-1)(q^4+1)=2(2^{p-1}-1),$$

which implies $2(2^{p-1}-1)$ is divisible by 4, a contradiction.

Similarly, if $q^8-q^4+1=2^p-1$, we obtain $q^4(q-1)(q+1)(q^2+1)=2(2^{p-1}-1)$, which shows that $2(2^{p-1}-1)$ is divisible by 16, a contradiction. Similar arguments work if $(q^{10}+q^5+1)/(q^2+q+1)=2^p-1$ or $(q^{10}-q^5+1)/(q^2-q+1)=2^p-1$, and we omit the details.

Step 3.9. *$K/H\ncong {}^2F_4(q)$, where $q=2^{2m+1}>2$.*

The odd order components of ${}^2F_4(q)$ are:

$$q^2+\sqrt{2q^3}+q+\sqrt{2q}+1 \quad \text{and} \quad q^2-\sqrt{2q^3}+q-\sqrt{2q}+1.$$

Therefore, we have

$$q^2+\sqrt{2q^3}+q+\sqrt{2q}+1=2^p-1 \quad \text{or} \quad q^2-\sqrt{2q^3}+q-\sqrt{2q}+1=2^p-1.$$

However, if 2^{2m+1} is substituted in these equations we obtain

$$2^{m+1}(2^{3m+1}\pm 2^{2m+1}+2^m\pm 1)=2(2^{p-1}-1),$$

which is a contradiction.

Step 3.10. *$K/H \ncong F_4(q)$, where $q=2^m$.*

The odd order components of $F_4(q)$ are q^4+1 and q^4-q^2+1, hence $q^4+1=2^p-1$ or $q^4-q^2+1=2^p-1$. Now, it is easy to see that in both cases, 2^{2m} divides $2(2^{p-1}-1)$, a contradiction.

Step 3.11. *$K/H \ncong {}^2G_2(q)$, where $q=3^{2m+1}>3$.*

The odd order components of ${}^2G_2(q)$ are $q+\sqrt{3q}+1$ and $q-\sqrt{3q}+1$. If $q-\sqrt{3q}+1=2^p-1$, then $q^3>2^{3p}$, while Lemma 2.9 shows that $q^3<2^{3p}$, which is a contradiction. If $q+\sqrt{3q}+1=2^p-1$, then

$$2^p-2=2(2^{(p-1)/2}-1)(2^{(p-1)/2}+1)=3^{m+1}(3^m+1). \qquad (1)$$

First of all, we recall that $(2^{(p-1)/2}-1, 2^{(p-1)/2}+1)=1$. Now we consider two cases separately:

(i) If 3^{m+1} divides $2^{(p-1)/2}-1$, then

$$3^m+1<3^{m+1}\leqslant 2^{(p-1)/2}-1<2^{(p-1)/2}+1.$$

Hence, we obtain

$$3^{m+1}(3^m+1)<2(2^{(p-1)/2}-1)(2^{(p-1)/2}+1),$$

a contradiction.

(ii) If 3^{m+1} divides $2^{(p-1)/2}+1$, then $2^{(p-1)/2}+1=k\cdot 3^{m+1}$ where k is a natural number. Now, from Eq.(1), it follows that

$$2k(2^{(p-1)/2}-1)=3^m+1,$$

and consequently $3^m\geqslant 2^{(p+1)/2}-1$. Therefore we have

$$2^{(p+1)/2}-1\leqslant 3^m<3^{m+1}\leqslant 2^{(p-1)/2}+1,$$

a contradiction.

Step 3.12. *$K/H \not\cong G_2(q)$, where $q = 3^m$.*

Recall that the odd order components of $G_2(q)$ are $q^2 - q + 1$ and $q^2 + q + 1$. If $q^2 - q + 1 = 2^p - 1$ then $q^6 > 2^{3p}$, while one can follow from Lemma 2.9 that $q^6 < 2^{3p}$, which is a contradiction. If $q^2 + q + 1 = 2^p - 1$, then $q(q+1) \equiv 2 \pmod 4$, which forces m is even. But then, it is obvious that $2^p - 2 = q(q+1) \equiv 2 \pmod 8$, a contradiction.

Step 3.13. *$K/H \not\cong {}^2D_r(3)$, where $r = 2^m + 1$ is a prime number and $m \geqslant 1$.*

Recall that

$$|{}^2D_r(3)| = \frac{1}{(4, 3^r + 1)} 3^{r(r-1)}(3^r + 1) \prod_{i=1}^{r-1}(3^{2i} - 1),$$

and the odd order components of ${}^2D_r(3)$ are

$$(3^{r-1} + 1)/2 \quad \text{and} \quad (3^r + 1)/4.$$

In the case when $(3^{r-1} + 1)/2 = 2^p - 1$, adding 1 to both sides of this equality, we obtain

$$3(3^{r-2} + 1) = 2^{p+1},$$

which is a contradiction. If $(3^r+1)/4 = 2^p-1$, then $r \geqslant 5$ because $p \geqslant 5$. Moreover, on the one hand, from last equation we obtain $3^r = 2^{p+2} - 5 > 2^{p+1}$, which implies that

$$3^{r(r-1)} > 2^{(p+1)(r-1)} > 2^{4(p+1)}.$$

On the other hand, it follows from Lemma 2.9 that

$$3^{r(r-1)} = |K/H|_3 \leqslant |G|_3 < 2^{3p},$$

which is a contradiction.

Step 3.14. *$K/H \not\cong B_n(q)$, where $n = 2^m \geqslant 4$ and $q = r^f$ is an odd prime power.*

Note that

$$|B_n(q)| = \frac{1}{(2, q-1)} q^{n^2} \prod_{i=1}^{n}(q^{2i} - 1),$$

and the only odd order component of $B_n(q)$ is $(q^n + 1)/2$. If $(q^n + 1)/2 = 2^p - 1$, then $q^n = 2^{p+1} - 3 > 2^p$ and clearly q is not divisible by 2 and 3. Since $p \geqslant 5$ and $n \geqslant 4$, it is easy to see that

$$q^{n^2} > q^{3n} > 2^{3p} > 2^{2p}.$$

On the other hand, by Lemma 2.9, we obtain

$$q^{n^2} = |K/H|_r \leqslant |G|_r < 2^{2p},$$

which is a contradiction.

Step 3.15. *$K/H \ncong B_r(3)$.*

The only odd order component of $B_r(3)$ is $(3^r-1)/2$. If $(3^r-1)/2 = 2^p-1$, then $2^{p+1}-3^r = 1$. However, this equation has no solution by Lemma 2.8, which is impossible.

Step 3.16. *$K/H \ncong {}^3D_4(q)$.*

We recall that q^4-q^2+1 is the only odd order component of ${}^3D_4(q)$, and so $q^4-q^2+1 = 2^p-1$. But then, $q^2(q^2-1) = 2(2^{p-1}-1)$, which shows that $2(2^{p-1}-1)$ is divisible by 4, a contradiction.

Step 3.17. *$K/H \ncong G_2(q)$, where $2 < q \equiv \pm 1 \pmod 3$.*

In this case, the odd order components of $G_2(q)$ are q^2+q+1 and q^2-q+1. Let $q = r^f$. If $q^2+q+1 = 2^p-1$, then $q(q+1) = 2(2^{p-1}-1)$, which shows that $q > 2$ is not a power of 2. Moreover, since $q-1 \geqslant 2$, we obtain

$$q^3-1 = (q-1)(q^2+q+1) \geqslant 2(2^p-1),$$

and so $q^3 \geqslant 2^{p+1}-1 > 2^p$, which yields that $q^6 > 2^{2p}$. However, since

$$|G_2(q)| = q^6(q^2-1)(q^6-1),$$

from Lemma 2.9, we conclude that

$$q^6 = |K/H|_r \leqslant |G|_r < 2^{2p},$$

which is a contradiction.

The case when $q^2-q+1 = 2^p-1$ is similar and left to the reader.

Step 3.18. *$K/H \ncong {}^2D_n(3)$, where $n = 2^m+1$ which is not a prime and $m \geqslant 2$.*

The odd order component of ${}^2D_n(3)$ is $(3^{n-1}+1)/2$. If $(3^{n-1}+1)/2 = 2^p-1$, then $2^{p+1} = 3(3^{n-2}+1)$, a contradiction.

Step 3.19. *$K/H \ncong {}^2D_r(3)$, where $r \geqslant 5$ is a prime and $r \neq 2^m+1$.*

Here, we have

$$|{}^2D_r(3)| = \frac{1}{(4, 3^r+1)} 3^{r(r-1)}(3^r+1)\prod_{i=1}^{r-1}(3^{2i}-1).$$

The only odd order component of ${}^2D_r(3)$ is $(3^r+1)/4$, and so $(3^r+1)/4 = 2^p - 1$. An easy computation shows that $3^r = 2^{p+2} - 5 > 2^{p+1}$. Moreover, we note that $r - 1 \geqslant 4$, and so

$$3^{r(r-1)} \geqslant 3^{4r} > 2^{4(p+1)}.$$

On the other hand, by Lemma 2.9, we obtain

$$3^{r(r-1)} = |K/H|_3 \leqslant |G|_3 < 2^{3p},$$

which is a contradiction.

Step 3.20. *$K/H \ncong {}^2D_n(2)$, where $n = 2^m + 1$, $m \geqslant 2$.*

The only odd order component of ${}^2D_n(2)$ is $2^{n-1}+1$. Therefore, we obtain $2^{n-1} + 1 = 2^p - 1$, which is impossible.

Step 3.21. *$K/H \ncong {}^2D_n(q)$, where $n = 2^m \geqslant 4$ and $q = r^f$.*

Recall that

$$|{}^2D_n(q)| = \frac{1}{(4, q^n+1)} q^{n(n-1)}(q^n+1)\prod_{i=1}^{n-1}(q^{2i}-1),$$

and the only odd order component of ${}^2D_n(q)$ is $(q^n+1)/(2, q+1)$. Therefore, $(q^n+1)/(2,q+1) = 2^p - 1$. Assume first that $(2, q+1) = 1$. In this case, we obtain $q^n = 2(2^{p-1} - 1)$, a contradiction. Assume next that $(2, q+1) = 2$. Again, using simple calculations we obtain $q^n = 2^{p+1} - 3 > 2^p$ and so q cannot be a power of 2. Moreover, since $n - 1 \geqslant 3$, $q^{n(n-1)} \geqslant q^{3n} > 2^{3p}$. Now, Lemma 2.9 shows that

$$q^{n(n-1)} = |K/H|_r \leqslant |G|_r < 2^{3p},$$

which is a contradiction.

Step 3.22. *$K/H \ncong D_{r+1}(q)$, where $q = 2, 3$.*

Since, the only odd order component of $D_{r+1}(q)$ is $(q^r-1)/(2, q-1)$, we have $(q^r - 1)/(2, q-1) = 2^p - 1$. If $(2, q-1) = 1$, then $r = p$ and $q = 2$, and we have

$$|K/H| = |D_{p+1}(2)| = \frac{1}{(4, 2^{p+1}-1)} 2^{p(p+1)}(2^{p+1}-1)\prod_{i=1}^{p}(2^{2i}-1),$$

this shows that $|K/H|_2 = 2^{p(p+1)}/(4, 2^{p+1}-1)$ does not divide $|G|_2 = 2^{p^2}$, which is a contradiction. In the case when $(2, q-1) = 2$, we have the equation $2^{p+1} - 3^r = 1$, which has no solution for $p \geqslant 5$, by Lemma 2.8. This is again a contradiction.

Step 3.23. *$K/H \ncong D_r(q)$, where $q = 2, 3, 5$ and $r \geqslant 5$.*

We recall that the only odd order component of $D_r(q)$ is $(q^r-1)/(q-1)$. We distinguish three cases separately.

(*i*) $q=2$. In this case, we have $2^r-1=2^p-1$, and so $r=p$ and

$$|K/H|=|D_p(2)|=2^{p(p-1)}(2^p-1)\prod_{i=1}^{p-1}(2^{2i}-1).$$

Note that $|\mathrm{Out}(D_p(2))|=2$ and $D_p(2)\leqslant G/H\leqslant \mathrm{Aut}(D_p(2))$. Now, considering the order of groups, we get $|H|=2^\alpha(2^p+1)$ where $p-1\leqslant\alpha\leqslant p$. Let $r\in \mathrm{ppd}(2^{2p}-1)$ and $Q\in \mathrm{Syl}_r(H)$. Clearly $r\in\pi(2^p+1)$, Q is a normal $\pi_1(G)$-subgroup of G and $|Q|$ divides 2^p+1. Now, from Lemma 2.5, it follows that $|Q|-1$ is divisible by $m_2(G)=2^p-1$, and so $|Q|-1\geqslant 2^p-1$ or equivalently $|Q|\geqslant 2^p$. This forces $|Q|=2^p+1$. But then $m_2(G)=2^p-1$ does not divide the value $|Q|-1=2^p$, which is a contradiction.

(*ii*) $q=3$. In this case, from the equality $(3^r-1)/2=2^p-1$, we deduce that $2^{p+1}-3^r=1$. However, this equation has no solution when $p\geqslant 5$ by Lemma 2.8, a contradiction.

(*iii*) $q=5$. Here $(5^r-1)/4=2^p-1$, and so $5^r=2^{p+2}-3>2^{p+1}$. As before, since $r-1\geqslant 4$, we obtain $5^{r(r-1)}>5^{4r}>2^{4(p+1)}$. On the other hand, by Lemma 2.9, we have

$$5^{r(r-1)}=|K/H|_5\leqslant |G|_5<2^{2p},$$

which is a contradiction.

Step 3.24. *$K/H\ncong C_r(3)$.*

The only odd order component of $C_r(3)$ is $(3^r-1)/2$. Thus, if $(3^r-1)/2=2^p-1$, then $2^{p+1}-3^r=1$. However, this equation has no solution by Lemma 2.8, which is impossible.

Step 3.25. *$K/H\ncong C_n(q)$, where $n=2^m\geqslant 2$.*

Note that

$$|C_n(q)|=\frac{1}{(2,q-1)}q^{n^2}\prod_{i=1}^{n}(q^{2i}-1),$$

and the only odd order component of $C_n(q)$ is $(q^n+1)/(2,q-1)$. Therefore, $(q^n+1)/(2,q-1)=2^p-1$. If $(2,q-1)=1$, then $q^n=2(2^{p-1}-1)$, which yields that $q=p=2$ and $n=1$, a contradiction. If $(2,q-1)=2$, then $q^n=2^{p+1}-3>2^p$, which implies that q is not a power of 2 and 3. Let $q=r^f$. When $n\geqslant 4$, it is easy to see that

$$q^{n^2}>q^{3n}>2^{3p}>2^{2(p+1)}.$$

But, from Lemma 2.9, we obtain

$$q^{n^2} = |K/H|_r \leqslant |G|_r < 2^{2p},$$

a contradiction. Assume now that $n = 2$. In this case, we have $q^2 = 2^{p+1} - 3$, or equivalently

$$(q-1)(q+1) = 2^2(2^{p-1} - 1).$$

However, the left hand side is divisible by 8, while the right hand side is divisible by 4, a contradiction.

Step 3.26. *$K/H \ncong A_1(q)$, where $q = 2^m > 2$.*

The odd order components of $A_1(q)$ are $q+1$ and $q-1$. If $q+1 = 2^p - 1$, then $q = 2(2^{p-1} - 1)$, a contradiction. If $q - 1 = 2^p - 1$, then $q = 2^p$. Moreover, since $A_1(q) \leqslant G/H \leqslant \mathrm{Aut}(A_1(q))$, it is easy to see that the order of H is divisible by $(2^2-1)(2^4-1)\cdots(2^{2(p-1)}-1)$. Let $r \in \mathrm{ppd}(2^{2(p-1)}-1)$ and $Q \in \mathrm{Syl}_r(H)$. Clearly Q is a normal $\pi_1(G)$-subgroup of G and $|Q|$ divides $2^{p-1}+1$. On the other hand, from Lemma 2.5, $|Q|-1$ is divisible by $2^p - 1$ which implies that $|Q| \geqslant 2^p$. This is a contradiction.

Step 3.27. *$K/H \ncong A_1(q)$, where $3 \leqslant q \equiv \pm 1 \pmod 4$ and $q = r^f$.*

Assume first that $3 \leqslant q \equiv 1 \pmod 4$. In this case, the odd order components of $A_1(q)$ are $(q+1)/2$ and q. If $(q+1)/2 = 2^p - 1$, then $r^f = q = 2^{p+1} - 3$. First of all, we claim that f is an odd number. Otherwise, we have

$$(r^{f/2} - 1)(r^{f/2} + 1) = 2^2(2^{p-1} - 1).$$

But then, the left hand side is divisible by 8, while the right hand side is divisible by 4, which is a contradiction. Furthermore, by easy computations we observe that

$$|A_1(q)| = \frac{1}{2}q(q^2-1) = 2^2(2^{p+1}-3)(2^{p-1}-1)(2^p-1).$$

On the other hand, we have $|G/K| \cdot |H| = |G|/|A_1(q)|$, from which we deduce that

$$|G/K|_2 \cdot |H|_2 = \frac{|G|_2}{|A_1(q)|_2} = 2^{p^2-2}.$$

But since $|G/K|$ divides $|\mathrm{Out}(A_1(q))| = 2f$ and f is odd, $|G/K|_2$ is at most 2. Hence, if $S_2 \in \mathrm{Syl}_2(H)$, then $|S_2| = 2^{p^2-2}$ or $|S_2| = 2^{p^2-3}$. We notice that S_2 is a normal subgroup of G, because H is nilpotent. Now, it follows from Lemma 2.5 that $2^p - 1$ divides $2^{p^2-2} - 1$ or $2^{p^2-3} - 1$, which is a contradiction. If $q = 2^p - 1$, we get a contradiction by Lemma 2.8.

Assume next that $3 \leqslant q \equiv -1 \pmod 4$. In this case, the odd order components of $A_1(q)$ are $(q-1)/2$ and q. If $(q-1)/2 = 2^p - 1$, then $2^{p+1} - r^f = 1$. Noting

Lemma 2.8, we deduce that $f = 1$, and hence $r = 2^{p+1} - 1$ is a Mersenne prime, which is a contradiction because $p + 1$ is not a prime.

The case when $q = 2^p - 1$ is similar to the previous paragraph.

Step 3.28. *$K/H \not\cong A_r(q)$, where $(q-1)\big|(r+1)$.*

Recall that

$$|K/H| = |A_r(q)| = \frac{1}{(r+1, q-1)} q^{r(r+1)/2} \prod_{i=2}^{r+1} (q^i - 1).$$

The only odd order component of $A_r(q)$ is $(q^r - 1)/(q - 1)$, and so

$$(q^r - 1)/(q - 1) = 2^p - 1.$$

As a simple observation we see that $q^r - 1 \geqslant (q^r - 1)/(q - 1) = 2^p - 1$ and so $q^r \geqslant 2^p$. Let $q = t^f$, where t is a prime number and f is a natural number.

(i) Suppose first that $r \geqslant 7$. Then $q^{r(r+1)/2} > q^{3(r+1)} \geqslant 2^3 q^{3r} \geqslant 2^{3(p+1)}$. Now, if t is an odd prime, then by Lemma 2.9 we obtain

$$q^{r(r+1)/2} = |K/H|_t \leqslant |G|_t < 2^{3p},$$

which is a contradiction. Therefore, we may assume that $t = 2$. In this case, we have

$$(2^{fr} - 1)/(2^f - 1) = 2^p - 1,$$

from which one can deduce that $f = 1$ and $r = p$. Thus

$$|G/K| \cdot |H| = \frac{2^{p^2} \prod_{i=1}^{p} (2^{2i} - 1)}{2^{\frac{p(p+1)}{2}} \prod_{i=2}^{p+1} (2^i - 1)}.$$

Since $|G/K|$ divides $|\mathrm{Out}(K/H)| = |\mathrm{Out}(A_p(2))| = 2$, we conclude that $|H|$ is divisible by $2^p + 1$. Let $s \in \mathrm{ppd}(2^{2p} - 1) \subseteq \pi(2^p + 1)$ and $Q \in \mathrm{Syl}_s(H)$. Clearly $|Q|\big|2^p + 1$. Since H is a normal $\pi_1(G)$-subgroup of G which is nilpotent, Q is also a normal $\pi_1(G)$-subgroup of G. Now, by Lemma 2.5, $m_2(G) = 2^p - 1$ divides $|Q| - 1$, and so $|Q| \geqslant 2^p$. But, this forces $|Q| = 2^p + 1$. However, this contradicts the fact that $m_2(G) \| Q| - 1$.

(ii) Suppose next that $r = 5$. If q is even, then from $(q^5 - 1)/(q - 1) = 2^p - 1$, we obtain $q(q^3 + q^2 + q + 1) = 2(2^{p-1} - 1)$, which implies that $q = 2$ and $r = p = 5$. Therefore, by easy calculations we see that

$$|G/K| \cdot |H| = \frac{2^{10} \prod_{i=1}^{5} (2^i + 1)}{2^6 - 1},$$

which is not a natural number, a contradiction. If q is odd, then we get

$$q(q+1)(q^2+1) = q^4 + q^3 + q^2 + q = 2^p - 2,$$

however $q(q+1)(q^2+1) \equiv 0 \pmod 4$, while $2^p - 2 \equiv 2 \pmod 4$, a contradiction.

(iii) Finally suppose that $r = 3$. Then $q(q+1) = 2(2^{p-1} - 1)$. First of all, we note that q is not even, otherwise $p = 3$, which is impossible. In addition, we have

$$q(q+1) = 2(2^{(p-1)/2} - 1)(2^{(p-1)/2} + 1). \qquad (2)$$

Now we consider two cases separately:

(a) If q divides $2^{(p-1)/2} - 1$, then

$$q \leqslant 2^{(p-1)/2} - 1, \quad q + 1 < 2^{(p-1)/2} + 1.$$

Hence, we obtain

$$q(q+1) < 2(2^{(p-1)/2} - 1)(2^{(p-1)/2} + 1),$$

a contradiction.

(b) If q divides $2^{(p-1)/2} + 1$, then $2^{(p-1)/2} + 1 = kq$ for some natural number k. Now from Eq.(2), it follows that

$$2k(2^{(p-1)/2} - 1) = q + 1.$$

If $k = 1$, then $p = q = 5$. Hence $13 \in \pi(K/H) = \pi(A_3(5))$, however $13 \notin \pi(G) = \pi(C_5(2))$, a contradiction. Thus, $k \geqslant 2$ and we obtain

$$2(2^{(p+1)/2} - 2) - 1 \leqslant q < q + 1 \leqslant kq = 2^{(p-1)/2} + 1,$$

which is a contradiction.

Step 3.29. *$K/H \ncong A_{r-1}(q)$, where $(r, q) \neq (3, 2), (3, 4)$.*

Again, we recall that

$$|K/H| = |A_{r-1}(q)| = \frac{1}{(r, q-1)} q^{r(r-1)/2} \prod_{i=2}^{r} (q^i - 1),$$

and the only odd order component of $A_{r-1}(q)$ is $(q^r - 1)/(q-1)(r, q-1)$. Hence, we must have

$$(q^r - 1)/(q-1)(r, q-1) = 2^p - 1,$$

which implies that

$$q^r - 1 \geqslant (q^r - 1)/(q-1)(r, q-1) = 2^p - 1,$$

or equivalently $q^r \geqslant 2^p$. Let $q = t^f$, where t is a prime and f is a natural number. In what follows, we consider several cases separately.

(*i*) $r \geqslant 7$. In this case, we obtain

$$q^{r(r-1)/2} \geqslant q^{3r} \geqslant 2^{3p},$$

and Lemma 2.9 implies that $t = 2$. Now, Lemma 2.1 shows that $q = 2$ and $r = p$, and hence we obtain

$$|G/K| \cdot |H| = \frac{2^{p^2} \prod_{i=1}^{p}(2^{2i}-1)}{2^{\binom{p}{2}} \prod_{i=2}^{p}(2^i-1)} = 2^{\frac{p(p+1)}{2}} \prod_{i=1}^{p}(2^i+1).$$

On the other hand, $|G/K|$ divides $|\mathrm{Out}(K/H)| = 2$. From this we deduce that $|H|$ is divisible by $2^p + 1$. Let $s \in \mathrm{ppd}(2^{2p}-1) \subseteq \pi(2^p+1)$ and $Q \in \mathrm{Syl}_s(H)$. Evidently Q is a normal subgroup of G and $|Q|$ divides 2^p+1. Now, it follows from Lemma 2.5 that $m_2(G) = 2^p - 1 \big| |Q| - 1$, which is impossible.

(*ii*) $r = 5$. Assume first that $(5, q-1) = 1$. In this case, we have

$$\frac{q^5-1}{q-1} = q^4 + q^3 + q^2 + q + 1 = 2^p - 1,$$

or equivalently

$$q(q+1)(q^2+1) = 2(2^{p-1}-1). \tag{3}$$

If q is even, then we conclude that $q = 2$ and $r = p = 5$, and the proof is quite similar as (*i*). If q is odd, then the left-hand side of Eq.(3) is congruent to $0 \pmod 4$, while the right-hand side of Eq.(3) is congruent to $2 \pmod 4$, a contradiction.

Assume next that $(5, q-1) = 5$. In this case, we have

$$q^4 + q^3 + q^2 + q + 1 = 5(2^p - 1),$$

or equivalently

$$(q-1)(q^3 + 2q^2 + 3q + 4) = 10(2^{p-1} - 1).$$

In the case when q is even, one can easily deduce that $q = 2$, and so $13 = 5(2^{p-1}-1)$, a contradiction. Moreover, if q is odd, then from the equality $q(q+1)(q^2+1) = 5 \cdot 2^p - 6$ it is easily seen that the left-hand side of this equation is congruent to $0 \pmod 4$, while the right-hand side is congruent to $2 \pmod 4$, a contradiction.

(*iii*) $r = 3$. In this case, we have $(q^3-1)/(q-1)(3, q-1) = 2^p - 1$. First of all, if q is even, then we obtain $p = 3$, which is not the case. Thus, we can assume that q is odd.

If $(3, q-1) = 1$, then

$$q(q+1) = 2(2^{(p-1)/2} - 1)(2^{(p-1)/2} + 1). \tag{4}$$

If q divides $2^{(p-1)/2} - 1$, then

$$q \leqslant 2^{(p-1)/2} - 1, \quad q + 1 < 2^{(p-1)/2} + 1.$$

Hence, we obtain

$$q(q+1) < 2(2^{(p-1)/2} - 1)(2^{(p-1)/2} + 1),$$

a contradiction. If q divides $2^{(p-1)/2}+1$, then $2^{(p-1)/2}+1 = kq$. Now, from Eq.(4), it follows that

$$2k(2^{(p-1)/2} - 1) = q + 1.$$

When $k = 1$, we conclude that $p = 5$ and $q = 5$. But then, we have

$$|K/H| = |A_2(5)| = 2^5 \cdot 3 \cdot 5^3 \cdot 31,$$

while $|G| = |C_5(2)| = 2^{25} \cdot 3^6 \cdot 5^2 \cdot 7 \cdot 11 \cdot 17 \cdot 31$; this is a contradiction because $|K/H|_5 > |G|_5$. If $k \geqslant 2$, then $q \geqslant 2(2^{(p+1)/2} - 2) - 1$. Therefore, we have

$$2(2^{(p+1)/2} - 2) - 1 \leqslant q < q + 1 \leqslant 2^{(p-1)/2} + 1,$$

a contradiction.

If $(3, q-1) = 3$, then $q(q+1) = 2^2(3 \cdot 2^{p-2} - 1)$, which implies that $(q+1)_2 = 4$ and so $(q-1)_2 = 2$. Moreover, under these conditions, one can easily deduce that f is odd, otherwise $8|q-1$ where

$$q - 1 = t^f - 1 = (t^{f/2} - 1)(t^{f/2} + 1),$$

which is a contradiction. Thus, we have $|A_2(q)|_2 = 2^4$, while

$$|G/K|_2 \cdot |H|_2 = \frac{|G|_2}{|A_2(q)|_2} = 2^{p^2-4}.$$

Since $|G/K|$ divides $2f(3, q-1)$ and f is odd, $|G/K|_2 \leqslant 2$. Therefore a Sylow 2-subgroup of H has order either 2^{p^2-4} or 2^{p^2-5}. Applying Lemma 2.5 we deduce that $2^p - 1|2^{p^2-4} - 1$ or $2^p - 1|2^{p^2-5} - 1$. Now, one can easily check that the second divisibility is possible only for $p = 5$. But then, we get $q(q+1) = 2^2 \cdot 23$, which is a contradiction.

Step 3.30. *$K/H \ncong {}^2A_r(q)$, where $(q+1)\big|(r+1)$ and $(r, q) \neq (3, 3)$, $(5, 2)$.*

In this case, we have

$$|K/H| = |{}^2A_r(q)| = \frac{1}{(r+1, q+1)} q^{r(r+1)/2} \prod_{i=2}^{r+1} \left(q^i - (-1)^i\right),$$

and the only odd order component of ${}^2A_r(q)$ is $(q^r+1)/(q+1)$. Therefore, we get

$$(q^r+1)/(q+1) = 2^p - 1.$$

An argument similar to that in the previous cases shows that

$$q^r - 1 > (q^r+1)/(q+1) = 2^p - 1,$$

and so $q^r > 2^p$. Let $q = t^f$, where t is a prime and f is a natural number. We now consider three cases separately.

(i) $r \geqslant 7$. Then $q^{r(r+1)/2} > q^{3(r+1)} \geqslant 2^3 q^{3r} > 2^{3(p+1)}$, which forces by Lemma 2.9 that $t = 2$. Thus $(2^{fr}+1)/(2^f+1) = 2^p - 1$, and, consequently, $f = 1$, $r = 3$ and $p = 2$, which is a contradiction.

(ii) If $r = 5$, then $(q^5+1)/(q+1) = 2^p - 1$. Arguing as in the case (i), we conclude that $t = 2$ and $f = 1$, whence $12 = 2^p$, a contradiction.

(iii) If $r = 3$, then $(q^3+1)/(q+1) = 2^p - 1$. It follows that $q(q-1) = 2(2^{p-1}-1)$, and so $q = p = 2$, which is impossible.

Step 3.31. $K/H \ncong {}^2A_{r-1}(q)$.

In this case, we have

$$|K/H| = |{}^2A_{r-1}(q)| = \frac{1}{(r, q+1)} q^{r(r-1)/2} \prod_{i=2}^{r} \left(q^i - (-1)^i\right),$$

and the only odd order component of ${}^2A_{r-1}(q)$ is $(q^r+1)/(q+1)(r, q+1)$. Thus

$$\frac{q^r+1}{(q+1)(r, q+1)} = 2^p - 1,$$

As before, we deduce that $q^r \geqslant 2^p$. Let $q = t^f$, where t is a prime and f is a natural number. We now consider three cases separately.

(i) $r \geqslant 7$. It follows that $q^{r(r-1)/2} \geqslant q^{3r} > 2^{3p}$, which implies that $t = 2$ by Lemma 2.9. Now, we obtain

$$\frac{2^{fr}+1}{(2^f+1)(r, 2^f+1)} = 2^p - 1,$$

which contradicts Lemma 2.1 because $2^p - 1$ is the largest prime in $\pi(G)$.

(*ii*) $r = 5$. In this case we have $q^5 + 1 = (q + 1)(2^p - 1)(5, q + 1)$. Assume first that q is even, that is $q = 2^f$. If $(5, q + 1) = 1$, then we obtain $2^{5f} = 2^{f+p} + 2^p - 2^f - 2$, which is impossible. If $(5, q + 1) = 5$, then $2^{5f} = 5(2^{f+p} + 2^p - 2^f) - 6$, which is again a contradiction. Assume next that q is odd. Noting that $q(q-1)(q^2+1) = (2^p-1)(5, q+1)-1$, it is easily seen that the left hand side is congruent to $0 \pmod 4$, while the right hand side is congruent to $2 \pmod 4$, a contradiction.

(*iii*) $r = 3$. In this case, we have $(q^3+1)/(q+1)(3, q+1) = 2^p-1$. If $(3, q+1) = 1$, then we obtain

$$q(q-1) = 2^p - 2 = 2(2^{(p-1)/2} - 1)(2^{(p-1)/2} + 1).$$

If q divides 2, than $p = 2$, a contradiction. If q divides $2^{(p-1)/2} - 1$ or $2^{(p-1)/2} + 1$, then

$$q(q-1) < 2^p - 2 = 2(2^{(p-1)/2} - 1)(2^{(p-1)/2} + 1),$$

a contradiction. Therefore we may assume that $(3, q + 1) = 3$. If q is even, then we conclude that $q = 4$, which is a contradiction. We now suppose that q is odd. Since $q(q-1) = 2^2(3 \cdot 2^{p-2} - 1)$, it follows that $(q-1)_2 = 4$, and so $(q + 1)_2 = 2$. Moreover, under these hypotheses, one can easily deduce that f is odd, otherwise $8|q - 1 = t^f - 1 = (t^{f/2} - 1)(t^{f/2} + 1)$, which is a contradiction. On the other hand, $|G/K|$ divides $f(3, q+1)$ and since f is odd, $|G/K|_2 = 1$. Therefore a Sylow 2-subgroup of H has order 2^{p^2-4}. Again, using Lemma 2.5, we see that $2^p - 1|2^{p^2-4} - 1$, which implies that $p = 2$. This is a contradiction.

Step 3.32. $K/H \ncong C_r(2)$.

The only odd order component of $C_r(2)$ is $2^r - 1$. Thus $2^r - 1 = 2^p - 1$. It follows that $r = p$, $G/K = 1$ and $H = 1$, which means $G \cong C$. This completes the proof of the theorem. □

Acknowledgment. We would like to thank Professor Arturo Magidin and the referee for the careful reading of this manuscript and for many insightful suggestions and remarks.

References

[1] M. Akbari and A. R. Moghaddamfar, *Simple groups which are 2-fold OD-characterizable*, Bull. Malays. Math. Sci. Soc., 35(1) (2012), 65–77.

[2] R. W. Carter, Simple groups of Lie type, Wiley, London, 1972.

[3] G. Y. Chen, *A new characterization of sporadic simple groups*, Algebra Colloq., 3(1) (1996), 49–58.

[4] A. S. Kondratév, *On prime graph components of finite simple groups*, Mat. Sb., 180(6) (1989), 787–797.

[5] P. Mihăilescu, *Primary cyclotomic units and a proof of Catalan's conjecture*, J. Reine Angew. Math., 572 (2004), 167–195.

[6] A. R. Moghaddamfar, *Recognizability of finite groups by order and degree pattern*, Proceedings of the International Conference on Algebra 2010, 422–433.

[7] A. R. Moghaddamfar, *A comparison of the order components in Frobenius and 2-Frobenius groups with finite simple groups*, Taiwanese J. Math., 13(1) (2009), 67–89.

[8] A. R. Moghaddamfar and S. Rahbariyan, *OD-Characterization of some projective special linear groups over the binary field and their automorphism groups*, Comm. Algebra (to appear).

[9] A. R. Moghaddamfar, A. R. Zokayi and M. R. Darafsheh, *A characterization of finite simple groups by the degrees of vertices of their prime graphs*, Algebra Colloq., 12(3) (2005), 431–442.

[10] H. G. Shi and G. Y. Chen, ${}^2D_{p+1}(2)(5 \leqslant p \neq 2^m - 1)$ *can be characterized by its order components*, Kumamoto J. Math., 18 (2005), 1–8.

[11] A. V. Vasilév and E. P. Vdovin, *An adjacency criterion in the prime graph of a finite simple group*, Algebra Logic, 44(6) (2005), 381–406.

[12] A. V. Vasilév and E. P. Vdovin, *Cocliques of maximal size in the prime graph of a finite simple group*, Algebra Logic, 50(4) (2011), 291–322.

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

[14] K. Zsigmondy, *Zur theorie der potenzreste*, Monatsh. Math. Phys., 3(1) (1892), 265–284.

M. Akbari and **A. R. Moghaddamfar**
Department of Mathematics,
K. N. Toosi University of Technology,
P. O. Box 16315-1618,
Tehran, Iran
e-mails: m.akbari@dena.kntu.ac.ir (M. Akbari)
moghadam@kntu.ac.ir; moghadam@ipm.ir (A. R. Moghaddamfar)