A new characterization of symplectic groups $C_2(3^n)$

Behnam Ebrahimzadeh and Reza Mohammadyari

Abstract. We prove that symplectic groups $C_2(3^n)$, where $n = 2^k$ ($k \geq 0$) and $(3^{2n} + 1)/2$ is a prime number, can be uniquely determined by the order of the group and the number of elements with the same order.

1. Introduction

Let $G$ be a finite group, $\pi(G)$ be the set of prime divisors of the order of $G$ and $\pi_e(G)$ be the set of orders of elements in $G$. If $k \in \pi_e(G)$, then we denote the number of elements of order $k$ in $G$ by $m_k(G)$ and the set of the numbers of elements with the same order in $G$ by $nse(G)$. In other words,

$$nse(G) = \{m_k(G) : k \in \pi_e(G)\}.$$ 

Also we denote a Sylow $p$-subgroup of $G$ by $G_p$ and the number of Sylow $p$-subgroups of $G$ by $n_p(G)$. The prime graph $\Gamma(G)$ of group $G$ is a graph whose vertex set is $\pi(G)$, and 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 $\pi_i$, for $i = 1, 2, \ldots, t(G)$. In the case where $G$ is of even order, we assume that $2 \in \pi_1$.

The characterization of groups by $nse(G)$ pertains to Thompson’s problem (see [6]) which Shi posed in [9]. The first time, this type of characterization was studied by Shao and Shi. In [8], they proved that if $S$ is a finite simple group with $|\pi(S)| = 4$, then $S$ is characterizable by $nse(S)$ and $|S|$. Following this result, in [5, 4, 7] it is proved that sporadic simple groups, linear groups $L_2(p)$, where $2^n - 1$ or $2^n + 1$ is a prime number, and Suzuki groups $Sz(q)$,
where \( q - 1 \) is a prime number, can be uniquely determined by the order of the group and \( \text{nse}(G) \). In this paper, we prove that symplectic groups \( C_2(3^n) \), where \( n = 2^k \ (k \geq 0) \) and \( (3^{2n} + 1)/2 \) is a prime number can be uniquely determined by the order of the group and the number of elements with the same order. In fact, we prove the following theorem.

**Main Theorem.** Let \( G \) be a group with \( |G| = |C_2(3^n)| \) and \( \text{nse}(G) = \text{nse}(C_2(3^n)) \), where \( n = 2^k \ (k \geq 0) \) and \( p = (3^{2n} + 1)/2 \) is a prime number. Then \( G \) is isomorphic to \( C_2(3^n) \).

2. Notation and preliminaries

**Lemma 2.1** (see [3]). Let \( G \) be a Frobenius group of even order with kernel \( K \) and complement \( H \). Then

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

**Definition 2.2.** 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 kernels \( K/H \) and \( H \), respectively.

**Lemma 2.3** (see [1]). Let \( G \) be a 2-Frobenius group of even order. Then

(a) \( t(G) = 2 \), \( \pi(H) \cup \pi(G/K) = \pi_1 \) and \( \pi(K/H) = \pi_2 \);  
(b) \( G/K \) and \( K/H \) are cyclic groups satisfying \( |G/K| \) divides \( |\text{Aut}(K/H)| \).

**Lemma 2.4** (see [10]). Let \( G \) be a finite group with \( t(G) \geq 2 \). Then one of the following statements holds:

(a) \( G \) is a Frobenius group;  
(b) \( G \) is a 2-Frobenius group;  
(c) \( G \) has a normal series \( 1 \trianglelefteq H \trianglelefteq K \trianglelefteq G \) such that \( H \) and \( G/K \) are \( \pi_1 \)-groups, \( K/H \) is a non-abelian simple group, \( H \) is a nilpotent group and \( |G/K| \) divides \( |\text{Out}(K/H)| \).

**Lemma 2.5** (see [2]). Let \( G \) be a finite group and \( m \) be a positive integer dividing \( |G| \). If \( L_m(G) = \{g \in G \mid g^m = 1\} \), then \( m \mid |L_m(G)| \).

**Lemma 2.6.** Let \( G \) be a finite group. Then for every \( i \in \pi_e(G) \), \( \varphi(i) \) divides \( m_i(G) \), and \( i \) divides \( \sum_{j \mid i} m_j(G) \). Moreover, if \( i > 2 \), then \( m_i(G) \) is even.

**Proof.** By Lemma 2.5, the proof is straightforward. \( \square \)
Lemma 2.7 (see [11]). Let \( q, k, l \) be natural numbers. Then

1. \( (q^k - 1, q^l - 1) = q^{(k,l)} - 1 \).

2. \( (q^k + 1, q^l + 1) = \begin{cases} q^{(k,l) + 1} & \text{if both } k/(k,l) \text{ and } l/(k,l) \text{ are odd,} \\ (2, q + 1) & \text{otherwise.} \end{cases} \)

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

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

Lemma 2.8. Let \( G \) be a symplectic group \( C_2(3^n) \), where \( p = (3^{2n} + 1)/2 \) is a prime number. Then \( m_p(G) = (p - 1)|G|/(8p) \) and, for every \( i \in \pi_e(G) - \{1,p\} \), \( p \) divides \( m_i(G) \).

Proof. Since \( |G_p| = p \), we deduce that \( G_p \) is a cyclic group of order \( p \). Thus

\[ m_p(G) = \varphi(p)n_p(G) = (p - 1)n_p(G). \]

Now it is enough to show that \( n_p(G) = |G|/(8p) \). By [10], \( p \) is an isolated vertex of \( \Gamma(G) \). Hence \( |C_G(G_p)| = p \) and \( |N_G(G_p)| = xp \) for a natural number \( x \). We know that \( N_G(G_p)/C_G(G_p) \) embeds in \( \text{Aut}(G_p) \), which implies \( x | p - 1 \). Furthermore, by Sylow’s theorem, \( n_p(G) = |G : N_G(G_p)| \) and \( n_p(G) \equiv 1 \) (mod \( p \)). Therefore \( p \) divides \(|G|/(xp) - 1\). Thus \( q^2 + 1/2 \) divides \( q^4(q^4 - 1)(q^2 - 1)/2/(xp) - 1 \). It follows that \( q^2 + 1 \) divides \((2q^6 - 4q^6 + 2q^4 - x)\), hence \( q^2 + 1 \) divides \((q^2 + 1)(2q^6 - 6q^4 + 8q^2 - 8) + (8 - x)\), and since \( x | p - 1 \), we obtain that \( x = 8 \). Let \( i \in \pi_e(G) - \{1,p\} \). Since \( p \) is an isolated vertex of \( \Gamma(G) \), we conclude that \( p \mid i \) and \( pi \notin \pi_e(G) \). Thus \( G_p \) acts fixed point freely on the set of elements of order \( i \) by conjugation and hence \(|G_p| \mid m_i(G) \). So we conclude that \( p \mid m_i(G) \). \( \square \)

3. Proof of the Main Theorem

In this section, we prove the main theorem by the following lemmas. We denote by \( C \) the symplectic group \( C_2(3^n) \), where \( n = 2^k \) (\( k \geq 0 \)) and \( p := (3^{2n} + 1)/2 \) is a prime number. Recall that \( G \) is a group with \(|G| = |C| \) and \( nse(G) = nse(C) \).

Lemma 3.1. We have

\[ m_2(G) = m_2(C), \quad m_p(G) = m_p(C), \quad n_p(G) = n_p(C), \]

\( p \) is an isolate vertex of \( \Gamma(G) \), and \( p \mid m_k(G) \) for every \( k \in \pi_e(G) - \{1,p\} \).

Proof. By Lemma 2.6, for every \( 1 \neq r \in \pi_e(G) \), \( r = 2 \) if and only if \( m_r(G) \) is odd. Thus we deduce that \( m_2(G) = m_2(C) \). According to Lemma 2.6, \((m_p(G), p) = 1 \). Thus \( p \mid m_p(G) \) and hence Lemma 2.8 implies that \( m_p(G) \in \{m_1(C), m_2(C), m_p(C)\} \). Moreover, \( m_p(G) \) is even, so we conclude
that $m_p(G) = m_p(C)$. Since $G_p$ and $C_p$ are cyclic groups of order $p$ and $m_p(G) = m_p(C)$, we deduce that $m_p(G) = \varphi(p)n_p(G) = \varphi(p)n_p(C) = m_p(C)$, so $n_p(G) = n_p(C)$.

Now we prove that $p$ is an isolated vertex of $\Gamma(G)$. Assume the contrary. Then there is $t \in \pi(G) - \{p\}$ such that $tp \in \pi_e(G)$. So $m_{tp}(G) = \varphi(tp)n_p(G)k$, where $k$ is the number of cyclic subgroups of order $t$ in $C_G(G_p)$ and since $n_p(G) = n_p(C)$, it follows that

$$m_{tp}(G) = (t - 1)(p - 1)|C/k(8p).$$

If $m_{tp}(G) = m_p(C)$, then $t = 2$ and $k = 1$. Furthermore, Lemma 2.5 yields $p \mid m_2(G) + m_2p(G)$ and since $m_2(G) = m_2(C)$ and $p \mid m_2(C)$, we have $p \mid m_2p(G)$, which is a contradiction. So Lemma 2.8 implies that $p \mid m_{tp}(G)$. Hence $p \mid t - 1$, and since $m_{tp}(G) < |G|$, we have that $t - 1 \leq 8$. In conclusion we deduce that $t \in \{3, 4, 5, 6, 7, 8, 9\}$. Now, since $p \mid m_{tp}(G)$, this is a contradiction.

Let $k \in \pi_e(G) - \{1, p\}$. Since $p$ is an isolated vertex of $\Gamma(G)$, we have that $p \mid k$ and $pk \notin \pi_e(G)$. Thus $G_p$ acts fixed point freely on the set of elements of order $k$ and conjugation and hence $|G_p| \mid m_k(G)$. So we conclude that $p \mid m_k(G)$.

**Lemma 3.2.** The group $G$ is neither a Frobenius group nor a 2-Frobenius group.

**Proof.** Let $G$ be a Frobenius group with kernel $K$ and complement $H$. Then by Lemma 2.1, $t(G) = 2$ and $\pi(H)$ and $\pi(K)$ are vertex sets of the connected components of $\Gamma(G)$, and $|H|$ divides $|K| - 1$. Now by Lemma 3.1, $p$ is an isolated vertex of $\Gamma(G)$. Thus we deduce that (i) $|H| = p$ and $|K| = |G|/p$, or (ii) $|H| = |G|/p$ and $|K| = p$. Since $|H|$ divides $|K| - 1$, we conclude that the last case can not occur. So $|H| = p$ and $|K| = |G|/p$, hence

$$(q^2 + 1)/2 | (q^4 - 1)/(q^2 - 1)/2 - 1.$$  

We conclude that

$$(q^2 + 1) | ((q^2 + 1)(2q^6 - 6q^4 + 8q^2 - 8) + 7.$$  

Thus $q^2 + 1 | 7$ which is impossible.

We now show that $G$ is not a 2-Frobenius group. Let $G$ be a 2-Frobenius group. Then $G$ has a normal series $1 \leq H \leq K \leq G$ such that $G/H$ and $K$ are Frobenius groups by kernels $K/H$ and $H$, respectively. Set $|G/K| = x$. Since $p$ is an isolated vertex of $\Gamma(G)$, we have $|K/H| = p$ and $|H| = |G|/xp$.

By Lemma 2.3, $|G/K|$ divides $|\text{Aut}(K/H)|$. Thus $x \mid p - 1$ and since, by Lemma 2.7, $(p - 1, q - 1) = 1$, we have $(q^2 - 1/2, q^2 + 1/2) = 1$. Now, since $|G/K|/(p - 1)$, we deduce that $q^2 + 1/2p$. The group $H$ is nilpotent. Therefore, $H_t \times K/H$ is a Frobenius group with kernel $H_t$ and complement.
Now we consider \((q, 2, 3)\) of Lemma 2.4 occurs. So \(G\) has a normal series \(1 ≤ H ≤ K ≤ G\) such that \(H\) and \(G/K\) are \(\pi_1\)-groups, and \(K/H\) is a non-abelian simple group. Since \(p\) is an isolated vertex of \(\Gamma(G)\), we have \(p \mid |K/H|\). According to the classification of the finite simple groups we know that the possibilities are: alternating groups \(A_n\), where \(n > 5\); 26 sporadic finite simple groups; simple groups of Lie type. We deal with the above cases separately.

**Step 1.** Let \(K/H \cong A_n\), where \(n ≥ 5\), \(n = p', p' + 1, p' + 2\). For this purpose, we consider \((q^2 + 1)/2 = p'\). Then we deduce \(p' + 1 = (q^2 + 3)/2\). Now \(p' + 1 \mid |A_n| \mid |G|\), but we can see easily that \(\frac{q^2 + 1}{2} \mid |G|\), which is a contradiction. Now we consider \((q^2 + 1)/2 = p' - 2\), so \(p' = (q^2 + 4)/2\). Since \(p' \mid |A_n| \mid |G|\), but we can see easily that \(\frac{q^2 + 4}{2} \mid |G|\), we obtain a contradiction.

**Step 2.** If \(K/H\) is a sporadic group, then we consider \((q^2 + 1)/2 = 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 59, 71\), where this number is the order of components of sporadic groups. If, for example, \((q^2 + 1)/2 = 5\), then we deduce \(q^2 = 9\), and hence \(q = 3\). Now, since \(M_{11} \mid |G|\), this is a contradiction. For the other groups we have a contradiction, similarly.

**Step 3.** Here we suppose that \(K/H\) is isomorphic to a group of Lie type. For this purpose, we consider the following cases.

**Case 1.** Let \(K/H \cong B_n(q')\), where \(n ≥ 2\), or \(C_n(q')\), where \(n ≥ 3\). If \(K/H \cong B_n(q')\), where \(n ≥ 2\), then we consider \((q^2 + 1)/2 = (q^n + 1)/2\) so \(q^n = q^n\). On the other hand,

\[
|B_n(q')| = \frac{1}{(2, q - 1)} q^{n^2} \prod_{i=1}^{n} (q^{2i} - 1) \mid q^4(q^4 - 1)(q^2 - 1)
\]

and also we know that each \(p\)-part of \(K/H\) divides \(p\)-part of \(G\). Since \(p = (q^2 + 1)/2\), we have \(q^2 = 2p - 1\). Now, since \(|B_n(q')| \mid |G|\), we conclude that

\[
4p(p - 1)(p - 2)(2p - 1)^2 = q^{n^2} \prod_{i=1}^{n} (q^{2i} - 1).
\]

Thus we have \(p \mid q^{n^2}\) or \(p \mid \prod_{i=1}^{n} (q^{2i} - 1)\). On the other hand, \(q^{n^2} \mid p - 1\) or \(p - 2\) or \((2p - 1)\). If \(p \mid q^{n^2}\), then \(p \mid q^t\), and so \(p \mid \prod_{i=1}^{n} (q^{2i} - 1)\). In other words, \(p \mid q^{2t} - 1\), where \(1 ≤ t ≤ n\). From \(q^{n^2} \mid p - 1\) it follows that

\[
q^{n^2} ≤ p - 1 ≤ p ≤ q^{2t} - 1 ≤ q^{2n} - 1 ≤ q^{2n}.
\]
As a result $q^{n^2} \leq q^{2n}$, so $n^2 \leq 2n$, $n \leq 2$, but this is a contradiction. Similarly, there is a contradiction for other cases.

**Case 2.** Let $K/H \cong D_n(q')$, where $n \geq 4$ or $2D_n(q')$ with $n \geq 4$. Then we consider $(q^2 + 1)/2 = (q^n - 1)/(q - 1)$. On the other hand,

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

and also we know that each $p$-part of $K/H$ divides $p$-part of $G$. Since $|D_n(q')| \mid |G|$, it follows that

$$4p(p - 1)(p - 2)(2p - 1)^2 = \frac{1}{q^n(q - 1)} q^{m(n-1)}(q^m - 1) \prod_{i=1}^{n-1} (q^{2i} - 1).$$

Now we have

$$p \mid q^{m(n-1)} \text{ or } p \mid q^m - 1 \text{ or } p \mid \prod_{i=1}^{n-1} (q^{2i} - 1).$$

On the other hand, $q^{m(n-1)} \mid p - 1$ or $p - 2$ or $(2p - 1)$. If $p \mid q^{m(n-1)}$, then $p \nmid q'$, so $p \mid \prod_{i=1}^{n-1} (q^{2i} - 1)$. In other words, $p \mid q^{2i} - 1$, where $1 \leq t \leq n - 1$. Since $q^{m(n-1)} \mid p - 1$, we have

$$q^{m(n-1)} \leq p - 1 \leq p \leq q^{2t} - 1 \leq q^{2n} - 1 \leq q^{2n}. $$

As a result $q^{m(n-1)} \leq q^{2n}$, so $n(n-1) \leq 2n$, $n \leq 3$, but this is a contradiction ($n \geq 4$). There is a contradiction for other cases. Similarly, $K/H \not\cong 2D_n(q)$.

**Case 3.** Let $K/H \cong A_n(q')$, where $n \geq 2$. Then we consider

$$\frac{q^2 + 1}{2} = \frac{q^{m+1} + 1}{(q^m + 1)(q + 1, n + 1)},$$

and so

$$q^2 + 1 = \frac{q^{m+1} + 1}{(q^m + 1)(q + 1, n + 1)} < q^{m+1} + 1, \quad q^2 < q^{m+1}. $$

Since $n \geq 2$, we get

$$q^{m(n+1)/2} > q^{4n/2} \geq q^{2n} > q^m > 2^{4n}.$$ 

But, on the other hand, we have

$$q^{m(n+1)/2} = |K/H| \leq |G| \leq 2^{3n},$$

which is a contradiction.

**Case 4.** Let $K/H \cong E_6(q), E_7(q), E_8(q)$, where $n \geq 2$, or let $K/H \cong F_4(q)$. If $K/H \cong E_8(q')$, then we consider $(q^2 + 1)/2 = q^8 - q^4 + 1$. On the other hand,

$$|E_8(q')| = q^{120}(q^{90} - 1)(q^{24} - 1)(q^{20} - 1)(q^{18} - 1)(q^{14} - 1)$$
Since $|E_6(q')| \not| |G|$, this is a contradiction. For other cases we have similarly a contradiction.

Case 5. Let $K/H \cong G_2(q')$, where $q' \equiv \pm 2 \pmod{5}$. Then we consider $(q^2 + 1)/2 = q'(q' \mp 1)$. Since $(q', q' \mp 1) = 1$, we obtain $q^2 - 1 = 2q'(q' \pm 1)$, and
\[
(2^{m+1}, 2^m \pm 1) = 1, \quad \text{we deduce that}
\]
\[
(q - 1)(q + 1) = 2^{m+1}(2^m \pm 1).
\]
In other words,
\[
(3^n - 1)(3^n + 1) = 2^{m+1}(2^m \pm 1).
\]
Consequently, $3^n - 1 = 2^n \pm 1$ and $3^n + 1 = 2^{m+1}$, which is a contradiction.

Case 6. Let $K/H \cong B_2(q')$, where $q' = 2^{2r+1}$, $r \geq 1$. Then we consider $(q^2 + 1)/2 = q' + \sqrt{2q'} + 1$. As a result $q^2 - 1 = 2^m + 1(2^m \pm 1)$. Since $(2^m + 1, 2^m \pm 1) = 1$, we deduce that
\[
(q - 1)(q + 1) = 2^m + 1(2^m \pm 1).
\]
As a result $q^2 = 1 = q' + \sqrt{2q'} + 1$, so we deduce
\[
(q - 1)(q + 1) = 2^s + 1(2^{2s+1} + 2^s + 1).
\]
It follows that $3^n - 1 = 2^s + 1$ and $3^n + 1 = (2^{2s+1} + 2^s + 1)$, where we can see easily a contradiction.

Case 7. Let $K/H \cong E_6(q')$, where $q' = 2^{2s+1}$, $s \geq 1$. Then we consider
\[
\frac{q^2 + 1}{2} = q'^2 + \sqrt{2q'} + q' + \sqrt{2q'} + 1.
\]
As a result $q^2 - 1 = q' + \sqrt{2q'} + 1$, so we deduce
\[
(q - 1)(q + 1) = 2^s + 1(2^{2s+1} + 2^s + 1).
\]
It follows that $3^n - 1 = 2^s + 1$ and $3^n + 1 = (2^{2s+1} + 2^s + 1)$, where we can see easily a contradiction.

Case 8. Let $K/H \cong E_6(q)$, where $q = 2^{t+1}$, $t \geq 1$. Then we consider
\[
\frac{q^2 + 1}{2} = q'^6 - q'^3 + 1,
\]
so $q^2 < q'^6 - q'^3 + 1 < q'^6$. Hence $q'^{36} > 3^{12n}$.

On the other hand,
\[
2E_6(q') = \frac{1}{(3, q' + 1)} q'^{36}(q'^{12} - 1)(q'^9 + 1)
\times (q'^6 - 1)(q'^6 - 1)(q'^6 + 1)(q^2 - 1).
\]
Now, we obtain $q = r^s$. Therefore, by Lemma 2.4,
\[
q'^{36} = r^{36s} = |K/H| r \leq |G|r \leq 2^{3n},
\]
which is a contradiction.

Case 9. Let $K/H \cong D_q(q')$. Then we consider $(q^2 + 1)/2 = q'^4 - q'^2 + 1$, as a result
\[
(3^n - 1)(3^n + 1) = 2q^2(q^2 - 1).
\]
Hence $2q^2 = 3^n + 1$ and $q^2 - 1 = 3^n - 1$, which is a contradiction.
Case 10. Let $K/H \cong L_{n+1}(q')$. Then we consider

$$\frac{q^2 + 1}{2} = \frac{q'^{n+1} - 1}{(q' - 1)(q' - 1, n + 1)}$$

so

$$q'^{n+1} - 1 > \frac{q'^{n+1} - 1}{(q - 1)(q - 1, n + 1)} = q^2 + 1.$$ 

As a result $q^2 < q'^{n+1}$, so

$$q^n(n+1)/2 > q^{4(n+1)/2} > q^{2n} > 3^{8n}.$$ 

On the other hand, by Lemma 2.4 we have

$$q^n(n+1)/2 = |K/H|_r \leq |G|_r \leq 2^{3n},$$

which is a contradiction.

Hence $K/H \cong C_2(3^m)$, in conclusion $|K/H| = |C_2(3^m)|$. We know that $H \leq K \leq G$. Since $p$ is an isolated vertex of $\Gamma(G)$, we deduce that $p \mid |K/H|$. Hence $\frac{q^2 + 1}{2} = \frac{(q' + 1)/2}$. As a result $q = q'$, so $n = m$. Now, since $|K/H| = |C|$ and $1 \leq H \leq K \leq G$, we conclude that $H = 1$ and $G = K \cong C$. □

References


Department of Mathematics, Buin Zahra Branch, Islamic Azad University, Buin Zahra, Iran
E-mail address: behnam.ebrahimzadeh@gmail.com
E-mail address: rezamohammadyari@gmail.com