Characterization of simple groups $B_{2m}(3)$ by the set of element orders

Rulin SHEN

Department of Mathematics, Hubei University for Nationalities, Enshi, Hubei, China 445000
E-mail: rulinshen@gmail.com

Received: 3-20-2012; Accepted: 5-5-2011 *Corresponding author
Project supported by the foundation of Educational Department of Hubei Province in China (No. Q20111901) and foundation of Hubei University for Nationalities (No. MY2011T001).

Abstract

Let $\omega(G)$ denote the set of element orders of a finite group $G$. For an arbitrary subset $\omega$ of the set of natural numbers denote by $h(\omega)$ the number of pairwise non-isomorphic finite groups $G$ such that $\omega(G) = \omega$. In this paper we prove that, if $m = 1$, then $h(\omega(B_{2m}(3))) = \infty$, and if $m \geq 2$, then $h(\omega(B_{2m}(3))) = 1$.

Key Words finite simple group, prime graph, spectrum

MSC 2010 20D60

1 Introduction

Denote by $r_n$ the primitive prime divisor of $q^n - 1$ if $r_n | q^n - 1$, but for every $i < n$ we have $r_n$ don’t divide $q^i - 1$. By Zsigmondy theorem [13] there exists $r_n$ always except the cases $(n, q) = (6, 2)$ and $(n, q) = (2, 2^k - 1)$ with nature number $k$. The structure of the group which the number of connected components of prime graph is more than 1 is due to Grunenberg and Kegel as follows.

Theorem 1 (Grunenberg-Kegel). If a finite group $G$ has the disconnected prime graph, then one of the following statements holds:

(1) $s(G) = 2$ and $G$ is a Frobenius group or 2-Frobenius.

(2) there exists a nonabelian simple group $S$ such that $S \leq G = G/N \leq \text{Aut}(S)$, where $N$ is the maximal normal soluble subgroup of $G$. Furthermore, $N$ and $G/S$ are $\pi_1(G)$-subgroups, the graph $GK(G)$ is disconnected, $s(S) \geq s(G)$, and for every $i$ with $2 \leq i \leq s(G)$, there is $j$ with $2 \leq j \leq s(S)$, such that $\mu_i(G) = \mu_j(S)$.

Of course, by well-known Thompson theorem we have $N$ is nilpotent. For the problem of $k$-recognizable of non-abelian simple group $L$, the paper [11] has get the following result.
Theorem 2 (Vasilev-Gorshkov). Let $L$ be a non-abelian simple group satisfying $t(G) \geq 3$ and $t(2, G) \geq 2$. If $\omega(G) = \omega(L)$ for finite group $G$, then the following holds:

1. there is a finite nonabelian simple group $S$ such that $S \leq \overline{G} = G/N \leq \text{Aut}(S)$, where $N$ is the maximal normal soluble subgroup of $G$.

2. for every independent subset $\rho$ of $\pi(G)$ such that $|\rho| \geq 3$, then there is at most one prime divisor of $\rho$ dividing $|N| \cdot |\overline{G}/S|$. In particular, $t(S) \geq t(G) - 1$.

3. For every prime $p \in \pi(G)$ nonadjacent to 2 in prime graph, $p$ don’t divide $|N| \cdot |\overline{G}/S|$. In particular, $t(2, S) \geq t(2, G)$.

For the inequality of the item (2) of Theorem 2, if $L$ has disconnected prime graph, then more stronger result can be obtained as follows.

Lemma 3. Suppose that $L$ and $G$ are same as in Theorem 2. If $L$ has disconnected prime graph and is not one of $A_1(q), A_2(q), A_3(2), A_5(3)$, then $t(S) = t(\overline{G})$.

Proof. First, if $S = \overline{G}$, of course $t(S) = t(\overline{G})$. So we can assume that $S < \overline{G} \leq \text{Aut}(S)$. Since $G K(\overline{G})$ is disconnected and $\overline{G}$ is almost simple group, the simple groups $S$ is determined in [7]. Suppose that $G = S(\alpha)$, where $\alpha$ is a outer automorphism of $S$. If $S$ is sporadic group, then $\pi(\alpha) \leq 2$, so $t(S) = t(\overline{G})$ by the table of [10]. If $S$ is alternating group $A_l$, then $n = p$ or $p + 1$ with $p$ prime by Theorem 3 of [12]. If $n \neq 5, 6, 8$ and $n \geq 7$, then $\pi(\alpha) = 2$ and every prime $p \in \rho(\overline{A_l})$ satisfies $p \geq 5$, so $S(\alpha)$ is a non-abelian simple group in table I. If $\alpha$ is a field automorphism, then $\pi(\alpha) = r$ with $r$ prime number. Denote by $\pi_\alpha$ the set of primes dividing $|C_S(\alpha)|$.

1. $S = A_l(q')$ with $l$ or $l + 1$ odd prime. If $\alpha$ is a field automorphism, then $\pi_\alpha = \pi(A_l(q'))$, where $q' = q^r$ and $r = l$ or $l + 1$. Since $l \neq r$, then $r > q^r - 1$, so $r \in \pi(A_l(q'))$. Of course, if $r = p'$, then $r \in \pi(A_l(q'))$. We denote $r_i$ and $r_i'$ are primitive prime divisors of $q^r - 1$ and $q^{r'} - 1$, respectively. If $l + 1 \geq 5$, then $\rho(A_l(q')) = \{r_i' \mid \frac{l + 1}{2} < i \leq l + 1\}$. Thus if $r_i \in \rho(A_l(q'))$, then $i > r\left[\frac{l + 1}{2}\right]$. Since $r \geq 5$, we have $i > 5\left[\frac{l + 1}{2}\right] > 2l + 1$, so $\pi_\alpha \cap \rho(A_l(q')) = \phi$. Therefore $t(S) = t(\overline{G})$. If $l \leq 3$, then it is easy to check $S = A_1(q), A_2(q), A_3(2), A_3(3), A_5(5)$ are exceptions by [10]. If $\alpha$ is a graph automorphism, then $r = 2$. Since $2$ does not belong to $\rho(A_l(q'))$ in case of $l \geq 4$, we have $t(S) = t(\overline{G})$.

2. $S = 2A_l(q')$ with $l$ or $l + 1$ odd prime. We may assume $\alpha$ is a field automorphism, then $\pi_\alpha = \pi(2A_l(q'))$, where $q' = q^r$ and $r = l$ or $l + 1$. If $l + 1 \geq 5$, then $\rho(2A_l(q')) = \{r_i' \mid \frac{l + 1}{2} < i \leq l + 1, i \equiv 2(\text{mod} 4)\} \cup \{r_i' \mid \frac{l + 1}{2} < i \leq l + 1, i \equiv 1(\text{mod} 2)\} \cup \{r_i' \mid \frac{l + 1}{2} < i \leq l + 1, i \equiv 0(\text{mod} 4)\}$. Thus if $r_i \in \rho(2A_l(q'))$, then $i > r\left[\frac{l + 1}{2}\right]$. Since $r \geq 5$, we have $i > 5\left[\frac{l + 1}{2}\right] > l + 1$. But if $i > l + 1$, then $r_i$ is not in $\pi(2A_l(q'))$, a contradiction. So we have $\rho(A_l(q')) = \rho(A_l(q')|\alpha)$. Therefore, $t(S) = t(\overline{G})$. If $l \leq 3$, then we can check the exception cases $S = 2A_2(q), 2A_3(3)$.

3. If $S$ is the other possible Lie type simple group in table I–IV of [7], then we know $r$ is 2, 3 or 5, so $r$ does not belong to $\rho(S)$, then $t(S) = t(\overline{G})$.
Lemma 4. If \( \omega(G) = \omega(B_{2m}(3)) \) with prime \( m \geq 2 \), then there is a non-abelian simple group \( S \) such that \( S \leq G/O_r(G) \leq \text{Aut}(S) \), where \( r \in \pi_1(G) \), and the following hold:

1. If \( m \geq 3 \), then \( t(S) = 3 \cdot 2^{m-2} - 3 \cdot 2^{m-2} + 1 \) or \( 3 \cdot 2^{m-2} + 2 \).
2. \( n_i(S) = \frac{3^{m+1}}{2} \). Moreover, if \( m \geq 3 \), then \( S \) is a simple group in Table 1.

Proof. If \( m \geq 3 \), then \( t(B_{2m}(3)) = 3 \cdot 2^{m-2} + 1 \geq 7 \), so \( t(S) \geq 6 \). By Lemma 3, the exception group \( S \) is one of \( A_1(q), A_2(q), A_3(2), A_5(3) \), we have \( t(S) < 6 \), thus \( t(S) = 3 \cdot 2^{m-2} - 3 \cdot 2^{m-2} + 1 \).

For the case of \( m = 2 \), since \( \pi(B_4(3)) = \{2, 3, 5, 7, 13, 41\} \), we have \( S \) in Lemma 4 is a simple \( K_5 \) or \( K_6 \)-group, so we need the information of these in detail.

Lemma 5. Let \( q \) be prime power. Then each finite \( K_5 \)-group is

1. \( L_2(q) \), where \( q \) satisfies \( |\pi(q^2 - 1)| = 4 \);
2. \( L_3(q) \), where \( q \) satisfies \( |\pi((q^2 - 1)(q^3 - 1))| = 4 \);
3. \( U_3(q) \), where \( q \) satisfies \( |\pi((q^2 - 1)(q^3 + 1))| = 4 \);
4. \( O_5(q) \), where \( q \) satisfies \( |\pi(q^4 - 1)| = 4 \);
5. \( S \geq (2^{2n+1}) \), where \( |\pi((2^{2n+1} - 1)(2^{4n+2} + 1))| = 4 \);
6. \( R(q) \), where \( q = 3^{2n+1} \) satisfies \( |\pi(q^2 - 1)| = 3 \) and \( |\pi(q^2 - q + 1)| = 1 \);
7. \( \text{Alt}_{11}, \text{Alt}_{12}, M_{22}, J_3, HS, He, McL, L_4(4), L_4(5), L_4(7), L_5(2), L_5(3), L_6(2), O_7(3), O_8(2), S_6(3), S_8(2), L_4(8), U_4(5), U_4(7), U_4(9), U_5(3), U_6(2), O^c_8(3), O^c_8(2), 3D_4(3), G_2(4), G_2(5), G_2(7), G_2(8) \).

Lemma 6. Let \( q \) be prime power. Then each finite \( K_6 \)-group is

1. \( L_2(q) \), where \( q \) satisfies \( |\pi(q^2 - 1)| = 5 \);
2. \( L_3(q) \), where \( q \) satisfies \( |\pi((q^2 - 1)(q^3 - 1))| = 5 \);
3. \( U_3(q) \), where \( q \) satisfies \( |\pi((q^2 - 1)(q^3 + 1))| = 5 \);
4. \( L_4(q) \), where \( q \) satisfies \( |\pi((q^2 - 1)(q^3 - 1)(q^4 - 1))| = 5 \);
5. \( U_4(q) \), where \( q \) satisfies \( |\pi((q^2 - 1)(q^3 + 1)(q^4 - 1))| = 5 \);
6. \( O_5(q) \), where \( q \) satisfies \( |\pi(q^4 - 1)| = 5 \);
7. \( G_2(q) \), where \( q \) satisfies \( |\pi(q^6 - 1)| = 5 \);
8. \( S \geq (2^{2n+1}) \), where \( |\pi((2^{2n+1} - 1)(2^{4n+2} + 1))| = 5 \);
9. \( R(q) \), where \( q = 3^{2n+1} \) satisfies \( |\pi((q - 1)(q^2 - 1))| = 5 \);
10. \( \text{Alt}_{13}, \text{Alt}_{14}, \text{Alt}_{15}, \text{Alt}_{16}, M_{23}, M_{24}, J_1, Suz, Ru, Co_2, Co_3, F_4(22), HN, L_5(7), L_6(3), L_7(2), O_7(4), O_7(5), O_7(7), O_9(3), S_6(4), S_6(5), S_6(7), S_8(3), U_5(4), U_5(5), U_5(9), U_6(3), U_7(2), F_4(2), O^c_8(4), O^c_8(5), O^c_8(7), O^c_{10}(2), O^c_8(3), 3D_4(4), 3D_4(5) \).
2 Proofs of Cases \( m = 1 \) and \( 2 \)

Firstly, if \( m = 1 \), that is the case of \( B_2(3) \cong U_4(2) \), then \( \omega(B_2(3)) = \{1, 2, 3, 4, 5, 6, 9, 12\} \).

Secondly, if \( m = 2 \), that is the case of \( B_4(3) \cong O_9(3) \), then it is a simple \( K_5 \)-group. If \( \omega(G) = \omega(B_4(3)) \), then there is a non-abelian simple group \( S \) such that \( S \leq G/O_r(G) \leq \text{Aut}(S) \) by lemma 4, so \( S \) is a simple \( K_5 \) or \( K_6 \)-group and \( \pi(S) \leq \pi(B_4(3)) = \{2, 3, 5, 7, 13, 41\} \). Note that \( n_4(S) = 41 \). If \( S \) is a \( K_5 \)-group, then the values of \( n_i(S) \) for \( i \geq 2 \) are given in \([6]\). If \( S \) is one of item (1) of Lemma 5 and 6, then \( n_i(L_2(q)) = r \) or \( \frac{q^4+1}{2q^2-1} \), where \( q = r \) and \( q \equiv \epsilon(\mod 4) \). So \( r = 41 \) and \( |\pi(q^2-1)| = 4, 5, \) or \( \frac{q^4+1}{2q^2-1} = 41 \) and \( |\pi(q^2-1)| = 4, 5 \). But since the divisor \( 41^2 - 1 \) of \( 41^2 - 1 \) has 4 prime divisors, i.e., \( \{2, 3, 5, 7\} \), thus if \( |\pi(q^2-1)| = 4 \), then \( f = 1 \) by Zsigmondy theorem, and if \( |\pi(q^2-1)| = 5 \), then \( \frac{41^2-1}{41^2-1} \) has only one prime divisor, i.e., \( 41^2 - 1 \) has only one primitive prime divisor \( r_{2f} \), since \( 13 = r_{2f} > 2f + 1 \), we have \( f \leq 6 \). Let \( \frac{41^2-1}{41^2-1} = 13^n \), it is easy to check this equation has no solution. If \( \frac{q^4+1}{2q^2-1} = 41 \), then \( q = 3^4 \). But \( |\pi((3^4)^2-1)| = 3 \), a contradiction. Thus \( S \) is \( L_2(41) \). But the prime graph of \( \text{Aut}(L_2(41)) \) is connected, then \( G/O_r(G) \simeq L_2(41) \), so \( O_r(G) \) is normal Sylow 13-subgroup. But \( 9 \in \omega(B_4(3)) \) and one is not in \( \omega(L_2(41)) \), so \( 3 \in \pi(O_{13}(G)) \), a contradiction.

If \( S \) is one of (2), (3) of Lemma 5 and (2)–(5) of Lemma 6, then \( \frac{q^4+1}{(q^2-1)(q^2+1)} = 41 \), these equations have no solution. If \( S \) is \( O_9(3) \), then \( \frac{q^4+1}{(q^2-1)(q^2+1)} = 41 \), so \( q = 9 \), but \( |\pi(9^4-3)| = 3 \), it is impossible. If \( S \) is \( G_2(q) \), then \( q^2 + q + 1 = 41 \), it has no solution. If \( S \) is \( S_3(2^{2n+1}) \), then \( 2^{2n+1} - 1 = 41 \) or \( 2^{2n+1} + 2n + 1 = 41 \), these equations have no solution. If \( S = R(3^{2n+1}) \), then \( 3^{2n+1} + 3n + 1 = 41 \), it also has no solution. If \( S \) is one of the last item of Lemma 5 and 6, it is easy to check that the possible groups are \( O_9(3) \), \( S_3(3) \), \( O_9(3) \). But \( 84 \in \omega(S_3(3)) \) and one is not \( \omega(B_4(3)) \), it is impossible. For the case \( S = O_9(3) \), if \( S \leq G \leq \text{Aut}(S) \), then the prime graph of \( \overline{G} \) is connected by \([7]\), so \( G/O_r(G) \simeq O_9^- (3) \), but \( \rho(3, O_9^- (3)) = \{3, 7, 13, 41\} \) and \( \rho(3, B_4(3)) = \{3, 41\} \), thus \( \{7, 13\} \subseteq \pi(O_r(G)) \), a contradiction. Therefore, \( S = O_9(3) \). If \( r = 3 \), we can assume \( O_r(G) \) is elementary abelian 3-group, since \( B_4(3) \) is unisingular \([4]\), then \( G \) has order \( 3 \cdot 41 \), a contradiction. If \( r \neq 3 \), since \( O_9(3) \) has a subgroup \( U : L_4(3) \), where \( |U| = 3^6 \), we have it has a Frobenius group.

3 Proof of Case \( m \geq 3 \)

By Lemma 4, there is non-abelian simple group \( S \) such that \( S \leq G/N \leq \text{Aut}(S) \), where \( S \) is a simple group in table 1 and \( N = O_r(G) \). In the following, we use three steps to complete the proof.

**Step 1.** \( S \cong B_{2m'}(3), C_{2m'}(3), \) or \( ^2D_{2m'}(3) \) where \( m = m' \geq 3 \).

1. \( S \cong \text{Alt}_n \) \( (n \geq 5) \). If \( n \geq 7 \), then \( \text{Aut}(\text{Alt}_n) \cong S_n \). Since \( s(G) = s(D_{p'}) = 2 \), we have \( s(\text{Alt}_n) \geq 2 \). If \( s(\text{Alt}_n) = 2 \), then \( n = p, p + 1, p + 2 \) and \( n, n - 2 \) are not both prime by \([11]\). If \( s(\text{Alt}_n) = 3 \), then \( n = p, n - 2 \) are both prime. Since \( \frac{3^{2n-1}}{2} \geq 3281 \), we have \( n > 7 \). Since \( r_3 = 13 \) is not adjacent to \( r_{2m} \) and \( r_{2(2m-1)} \) in \( B_{2m}(3) \), then \( r_3 \) is also not adjacent to \( r_{2m} \) and \( r_{2(2m-1)} \) in \( G/N \). But \( 13 + r_{2m} \leq n \) and \( 13 + r_{2(2m-1)} \leq n \) in \( \text{Alt}_n \). In fact, since \( r_{2m} \) (or \( r_{2(2m-1)} \)) \( \leq \frac{3^{2m-1} + 1}{2} \), we have \( 13 + r_{2m} \leq \frac{3^{2m-1} + 1}{2} < \frac{3^{2m-1} + 1}{2} = p \leq n \), so \( 13 \) is adjacent to \( r_{2m} \) and \( r_{2(2m-1)} \) in \( \text{Alt}_n \).
then we have \(|\pi(N)| \geq 2\), contradicts.

(2) \(S\) is simple group of Lie type in characteristic \(r\).

(a) If \(S = A'_n(q)\) or \(A'_{p+1}(q)\), then \(t(S) = \frac{p+1}{q} - 1\) by Table 1 and (1)-2 of Lemma 4, so \(\frac{p+1}{q} = 3 \cdot 2^{m-2}, 3 \cdot 2^{m-2} + 1\) or \(3 \cdot 2^{m-2} + 2\), so \(p = 6 \cdot 2^{m-2} + 1\) or \(6 \cdot 2^{m-2} + 3\). Also equations \(\frac{p+1}{q} = \frac{2}{q} + 1\) and \(\frac{p+1}{q} = \frac{2}{q} + 1\) if \(q \geq 4\); or \(q \geq 3\) and \(m \geq 4\), we have \(\frac{p+1}{q} \geq \frac{2}{q} + 1 \geq \frac{2}{q} + 1 \geq \frac{2}{q} + 1 = \frac{2}{q} + 1 \geq \frac{2}{q} + 1 = \frac{2}{q} + 1\), thus the two equations above have no solution. If \(q = 3\) and \(m = 3\), it is easy to check the equations have no solution. If \(q = 2\), then \(\frac{2}{q} + 1 = \frac{2}{q} - 1\) or \(\frac{2}{q} + 1\), but these equations have no solution.

(b) If \(S = B_n(q), C_n(q), 2D_n(q)\), where \(n = 2^m\) and \(q = 2^f\), then the equations are \(2^m = 2^f + 1\) or \(2^f\), that is \(2^f + 1 = 3(2^{m-1} + 1)\) or \(2^f = 3(2^{m} + 1)\), obviously, these equations have no solution.

(c) If \(S = C_n(q), 2D_n(q)\), where \(n = 2^m\) and \(q = 2^f\), then the equations are \(2^m = q^n + 1\), that is \(2^f + 1 = 3(2^{m-1} + 1)\), it has no solution by Zsigmondy Theorem [13].

(d) If \(S = D_p(r)\), where \(r = 2, 3, 5\), then the equation is \(\frac{p+1}{r-1} = \frac{3}{2} + 1\), it is easy to see these equations have no solution.

(e) If \(S = 2D_n(3), 2D_n(3)\), where \(n = 2^m + 1\), then the equations are \(3^{m+1} + 1 = \frac{3}{2} + 1\), \(\frac{3}{2} + 1 = \frac{3}{2} + 1\), \(\frac{3}{2} + 1 = \frac{3}{2} + 1\), these equations have no solutions.

(f) If \(S = E_6(q), E_7(q), E_8(q)\) or \(E_8(q)\), then \(3 \cdot 2^m + 1 = u\) for \(5 \leq u \leq 12\), we have \(3 \cdot 2^m + 1 = u - 1\), so \(m = 3\). But since \(n_4(S) = 3281\), it is impossible.

(3) If \(S\) is a sporadic simple group, then \(n_4(S) \leq 71\) by [8] or [12], but \(\frac{32^m+1}{2} \geq 3281\), thus \(n_4(S) = \frac{32^m+1}{2}\) is impossible.

Step 2. \(S = B_{2m}(3)\).

If \(S = C_{2m}(3)\), then there is element order \(p(3^{2m-1} + 1)\) in \(C_{2m}(3)\), which is not in \(\omega(B_{2m}(3))\) by [14], so it is impossible. If \(S = 2D_{2m}(3)\), since \(S \leq \omega(S)\), then \(G/K(S)\) is a connected, thus \(S = B_{2m}(3)\). But \(\rho(3, 2D_{2m}(3)) = \{3, r_{2m-1}, r_{2m+1-2}, r_{2m+1}\}\), and \(\rho(3, B_{2m}(3)) = \{3, r_{2m+1}\}\), so \(|\pi(N)| \geq 2\), a contradiction.

Step 3. \(G \simeq B_{2m}(3)\).

If \(\alpha\) is a diagonal automorphism of \(D_p(5)\), then the prime graph of \(D_p(5)\) is connected. If \(\alpha\) is a graph automorphism, then \(o(\alpha) = 2\) and \(\pi([C_{D_p(5)}(\alpha)]) = \pi(B_{p-1}(5))\), so there is order \(2r_{2(p-1)}\), but by Table 6 of [10], there is not \(2r_{2(p-1)}\) in \(D_p(5)\), thus it is impossible, then \(G/N \simeq D_5(5)\). Now if \(N \neq 1\), since \(N\) is \(r\)-group, without loss of generality, assume that \(N\) is elementary \(r\)-group. Since \(C_G(N)\) is normal in \(G\), so \(C_G(N)/N\) is also normal in \(G/N \simeq D_p(5)\), if \(C_G(N)/N \neq 1\), but since \(D_p(5)\) is simple, we have \(D_p(5) \leq C_G(N)/N\), then \(r\cdot \omega(D_p(5)) \leq \omega(C_G(N)/N) \leq \omega(G)\), that is \(\omega(G) \neq \omega(D_p(5))\). If \(C_G(N)/N = 1\) and \(r \neq 5\), then \(D_p(5)\) has subgroup \(U : SL_2(5)\), where \(|U| = 5^{16n-15}\). In fact, since
$D_p(5) \simeq P\Omega^+_{2p}(5) \simeq \Omega^+_{2p}(5)/Z$, where $Z$ is the center subgroup with order 2, we consider the stabilizers of maximal ($p$-dimensional) totally isotropic subspaces in $\Omega^+_{2p}(5)$. The stabilizer of this is $U : SL_p(5).Z_2$, becoming $U : GL_p(5)$ in $SO^+_{2p}(5)$ (See [1] and [5]), of course $U$ has order $5^{p(p-1)/2}$. On the other hand, $r_p$ is not adjacent to 5 in $GK(D_p(5))$, so $D_p(5)$ has a Frobenius group with order $5^{p(p-1)/2} \cdot r_p$, then $G$ has element with order $r \cdot r_p$ by Lemma 1 of [9], contradicts. If $C_G(N)/N = 1$ and $r = 5$, since $D_p(5)$ is a unisingular group [4], then there is non-trivial fixed point for every element if $D_p(5)$ acts on $N$ by conjugacy, then $G$ has element with order $r \cdot r_p$, contradicts.

References