QUASIRECOGNITION BY PRIME GRAPH OF THE GROUPS $^2D_{2n}(q)$ WHERE $q < 10^5$

HOSSEIN MORADI$^{1,A}$ & MOHAMMAD REZA DARAFSHEH$^{2,B}$ & ALI IRANMANESH$^{1,C}$

Abstract. Let $G$ be a finite group. The prime graph $\Gamma(G)$ of $G$ is defined as follows: The set of vertices of $\Gamma(G)$ is the set of prime divisors of $|G|$ and two distinct vertices $p$ and $p'$ are connected in $\Gamma(G)$, whenever $G$ has an element of order $pp'$. A non-abelian simple group $P$ is called recognizable by prime graph if for any finite group $G$ with $\Gamma(G) = \Gamma(P)$, $G$ has a composition factor isomorphic to $P$. In [4] proved finite simple groups $^2D_n(q)$, where $n \neq 4k$ are quasirecognizable by prime graph. Now in this paper we discuss the quasirecognizability by prime graph of the simple groups $^2D_{2k}(q)$, where $k \geq 9$ and $q$ is a prime power less than $10^5$.

1. Introduction

Let $G$ be a finite group. By $\pi_e(G)$ we denote the set of elements orders of $G$. For an integer $n$ we define $\pi(n)$ as the set of prime divisors of $n$, and we set $\pi(G)$ for $\pi(|G|)$. The prime graph of the Gr"{u}enberg-Kegel graph of $G$ is denoted by $\Gamma(G)$ and is graph with vertices set $\pi(G)$ in which two distinct vertices $p$ and $q$ are joined by an edge if and only if $pq \in \pi(G)$, and in this case we will write $p \sim q$.

A subset of vertices of $\Gamma(G)$ is called an independent subset of $\Gamma(G)$ if its vertices are pairwise nonadjacent. Denote by $t(G)$ the maximal number of primes in $\pi(G)$ pairwise nonadjacent in $\Gamma(G)$. Also we denote by $t(2,G)$ the maximal number of vertices in the independent sets of $\Gamma(G)$ containing 2. A finite nonabelian simple group $P$ is called quasirecognizable by prime graph, if every finite group $G$ with $\Gamma(G) = \Gamma(P)$ has a composition factor isomorphic to $P$. Also $P$ is called recognizable by prime graph if $\Gamma(G) = \Gamma(P)$ implies that $G \cong P$.

In [3] and [5], finite groups with the same prime graph as $\Gamma(PSL(2,q))$, where $q$ is a prime power, are determined. In [7, 8, 9] finite groups with the same prime graph as $\Gamma(L_n(2))$, $\Gamma(U_n(2))$, $\Gamma(D_n(2))$, $\Gamma(^2D_n(2))$ and $\Gamma(^2D_{2k}(3))$ are obtained. Also in [10] it is proved that if $p$ is a prime less than 1000 and for suitable $n$, the finite simple groups $L_n(p)$, $U_n(p)$ are quasirecognizable by prime graph. Now as the main result of this paper, we prove the following theorem:

Main Theorem. The finite simple group $^2D_{2k}(q)$, where $k \geq 9$ and $q < 10^5$ is quasirecognizable by prime graph.

Throughout this paper, all groups are finite and by a simple group we mean nonabelian simple groups. All further unexplained notations are standard and the reader is referred to [2].

2000 Mathematics Subject Classification. AMS Classification: 20D05, 20D60, 20D06.

Key words and phrases. prime graph; simple group; orthogonal groups; quasirecognition.
2. Preliminary Results

Lemma 2.1. [16, Theorem 1] Let $G$ be a finite group with $t(G) \geq 3$ and $t(2, G) \geq 2$. Then the following hold:

1. there exists a finite nonabelian simple group $S$ such that

$$S \leq \bar{G} = G/K \leq \text{Aut}(S)$$

for the maximal normal soluble subgroup $K$ of $G$.

2. for every independent subset $\rho$ of $\pi(G)$ with $|\rho| \geq 3$ at most one prime in $\rho$ divides the product $|K| \cdot |\bar{G}/S|$. In particular, $t(S) \geq t(G) - 1$.

3. one of the following holds:

(a) every prime $r \in \pi(G)$ nonadjacent to 2 in $\Gamma(G)$ does not divide the product $|K| \cdot |\bar{G}/S|$; in particular, $t(2, S) \geq t(2, G)$;

(b) there exists a prime $r \in \pi(K)$ nonadjacent to 2 in $\Gamma(G)$; in which case $t(G) = 3$, $t(2, G) = 2$, and $S \cong A_7$ or $L_2(q)$ for some odd $q$.

Remark 2.2. In Lemma 2.1, for every odd prime $p \in \pi(S)$, we have $t(p, S) \geq t(p, G) - 1$.

If $q$ is a natural number, $r$ is an odd prime and $(q, r) = 1$, then by $e(r, q)$ we denote the smallest natural number $m$ such that $q^m \equiv 1 \pmod{r}$. Given an odd $q$, put $e(2, q) = 1$ if $q \equiv 1 \pmod{4}$ and put $e(2, q) = 2$ if $q \equiv -1 \pmod{4}$. Using Fermat’s little theorem we can see that if $r$ is an odd prime such that $r \mid (q^n - 1)$, then $e(r, q) \mid n$.

Lemma 2.3. [20, Proposition 2.5] Let $G = D_6^\ast(q)$, where $q$ is power of prime $p$. Define

$$\eta(m) = \begin{cases} 
  m, & \text{if } m \text{ is odd}; \\
  m/2, & \text{otherwise}.
\end{cases}$$

Suppose $r, s$ are odd primes and $r, s \in \pi(D_6^\ast(q)) \setminus \{p\}$. Put $k = e(r, q)$, $l = e(s, q)$, and $1 \leq \eta(k) \leq \eta(l)$. Then $r$ and $s$ are non-adjacent if and only if $2\eta(k) + 2\eta(l) > 2n - (1 - \varepsilon(-1)^{k+l})$ and $k$ and $l$ satisfy the following condition:

$$\frac{l}{k}$$

is not an odd integer,

and, if $\varepsilon = +$, then the chain of equalities:

$$n = l = 2\eta(l) = 2\eta(k) = 2k$$

is not true.

Lemma 2.4. [20, Proposition 2.3] Let $G$ be one of simple groups of Lie type, $B_n(q)$ or $C_n(q)$, over a field of characteristic $p$. Define

$$\eta(m) = \begin{cases} 
  m, & \text{if } m \text{ is odd}; \\
  m/2, & \text{otherwise}.
\end{cases}$$

Let $r, s$ be odd primes with $r, s \in \pi(G) \setminus \{p\}$. Put $k = e(r, q)$ and $l = e(s, q)$, and suppose that $1 \leq \eta(k) \leq \eta(l)$. Then $r$ and $s$ are non-adjacent if and only if $\eta(k) + \eta(l) > n$, and $k, l$ satisfy to:

$$\frac{l}{k}$$

is not an odd natural number.
Lemma 2.5. [19, Proposition 2.1] Let $G = L_n(q)$, where $q$ is a power of prime $p$. Let $r$ and $s$ be odd primes and $r, s \in \pi(G) \setminus \{p\}$. Put $k = e(r, q)$ and $l = e(s, q)$ and assume that $2 \leq k \leq l$. Then $r$ and $s$ are nonadjacent if and only if $k + l > n$ and $k$ does not divide $l$.

Lemma 2.6. [19, Proposition 2.2] Let $G = U_n(q)$, where $q$ is a power of prime $p$. Define

$$\nu(m) = \begin{cases} m, & m \equiv 0 \pmod{4}; \\ m/2, & m \equiv 2 \pmod{4}; \\ 2m, & m \equiv 1 \pmod{2}. \end{cases}$$

Let $r$ and $s$ be odd primes and $r$, $s \in \pi(G) \setminus \{p\}$. Put $k = e(r, q)$ and $l = e(s, q)$ and suppose that $2 \leq \nu(k) \leq \nu(l)$. Then $r$ and $s$ are nonadjacent if and only if $\nu(k) + \nu(l) > n$ and $\nu(k)$ does not divide $\nu(l)$.

For every Lemmas 2.3 and 2.6, simultaneously we define the following function:

$$\nu'(m) = \begin{cases} m, & \epsilon = +; \\ \nu(m), & \epsilon = -. \end{cases}$$

which we will use in the proofs. We note that a prime $r$ with $e(r, q) = m$ is called a primitive prime divisor of $q^m - 1$ (obviously, $q^m - 1$ can have more than one primitive prime divisor).

Lemma 2.7. (Zsigmondy’s theorem) [22] Let $p$ be a prime and let $n$ be a positive integer. Then one of the following holds:

1. there is a primitive prime $p'$ for $p^n - 1$, that is, $p' \mid (p^n - 1)$ but $p' \nmid (p^m - 1)$, for every $1 \leq m < n$,
2. $p = 2$, $n = 1$ or 6,
3. $p$ is a Mersenne prime and $n = 2$.

3. Proof of the Main Theorem

Throughout this section, we suppose that $D := {^2D}_{2k}(p^n)$ where $k \geq 9$, $2 < p^n < 10^5$ and $G$ is a finite group such that $\Gamma(G) = \Gamma(D)$. We denote a primitive prime divisors of $q^r - 1$ by $r_i$ and a primitive prime divisors of $q^n - 1$ by $r_i'$, where $q' \neq q$.

By [19, Tables 4, 6, 8], we deduce that $t(D) \geq 14$ and $t(2, D) \geq 2$. Therefore $t(G) \geq 14$ and $t(2, G) \geq 2$. Now by Lemma 2.1, it follows that there exists a finite nonabelian simple group $S$ such that

$$S \leq G := G/K \leq \text{Aut}(S)$$

where $K$ is the maximal normal solvable subgroup of $G$. Also, $t(S) \geq t(G) - 1$ and $t(2, S) \geq t(2, G)$ by Lemma 2.1. Therefore $t(S) \geq 13$ and $t(2, S) \geq 2$. On the other hand, by [19, Tables 2, 9], if $S$ is isomorphic to a sporadic or an exceptional simple group of Lie type, then $t(S) \leq 12$. This implies that $S$ is not isomorphic to any sporadic and any exceptional simple group of Lie type.

In the sequel, we consider each possibility for $S$.

Lemma 3.1. $S$ is not isomorphic to any alternating group.
**Proof.** Suppose that $S \cong A_m$, where $m \geq 5$. Since $t(S) \geq 13$, Lemma 2.1, we get that $m \geq 61$ and so $\{47, 59\} \subseteq \pi(S)$.

**Case 1.** Let $\{47, 59\} \not\subseteq \pi(q^2 - 1)$, where $q = p^a < 10^5$. Therefore we get that $e(47, q) \geq 23$ or $e(59, q) \geq 29$. \{47, 59\} $\subseteq \pi(S)$. Hence $G$ contains an element $a \in A_m$, such that $e(a, q) \geq 23$, which implies that $n \geq 24$. Now we have $\min\{t(47, G), t(59, G)\} \geq 19$. Hence, according to Remark 2.2, $\min\{t(47, S), t(59, S)\} \geq 18$ in $S$. On the other hand, 47 is not connected to the prime numbers in the interval $[m - 46, m]$ in the prime graph of $A_m$ and similarly, 59 is not connected to the prime numbers in the interval $[m - 58, m]$, in the prime graph of $A_m$. But these intervals contains at most 16 prime numbers, and this implies that $t(S) < t(G) - 1$, a contradiction.

**Case 2.** Let $\{47, 59\} \subseteq \pi(q^2 - 1)$, where $q = p^a < 10^5$. Using GAP, we get that:

First let $q \in A \setminus \{21713\}$. Then we have $e(23, q) \geq 11$ and so similarly to Case 1, we get that $t(23, G) - 1 > t(23, S)$, a contradiction.

Let $q = 21713$. Since $e(19, q) = 18$, again similarly to Case 1, we get that a contradiction. 

\[ \square \]

**Lemma 3.2.** If $S$ is isomorphic to a classical simple group of Lie type over a field of characteristic $p$, then $S \cong D$.

**Proof.** Let $S$ be a nonabelian simple group of Lie type over $GF(q')$, $q' = p^\beta$. By the hypothesis,

$$S \leq \bar{G} := G/N \leq \text{Aut}(S),$$

where $N$ is the maximal normal solvable subgroup of $G$. In the sequel, we denote by $r_i$, a primitive prime divisor of $q^i - 1$ and denote by $r'_i$, a primitive prime divisor of $q^i - 1$. We remark that $\{p, r_2\} \subseteq \pi(S)$ and $|\rho(p, G) \cap \pi(S)| \geq 3$ by Lemma 2.1.

Now we consider the following cases:

**Case 1.** Let $r_{2n-2} \in \pi(S)$. Also let $p_1$ and $p_2$ be two primitive prime divisors of $p^{(2n-2)\alpha} - 1$ and $p^{2n\alpha} - 1$, respectively. So we may assume that $p_1$ and $p_2$ are $r_{2n-2}$ and $r_{2n}$, respectively. This implies that $\{r_{2n-2}, r_{2n}\} \subseteq \pi(S)$. Thus $r_{2-2}$ is a primitive prime divisor of $q^{\alpha} - 1$ and $r_{2n}$ is a primitive prime divisor of $q^{\beta} - 1$, where $s = e(r_{2n-2}, p^\beta)$ and $t = e(r_{2n}, p^\beta)$. It follows that $(2n - 2)\alpha \mid s\beta$ and $2n\alpha \mid t\beta$. On the other hand, using Zsigmondy’s theorem, we conclude that $t\beta \leq 2n\alpha$ and so $t\beta = 2n\alpha$. Also since $2n < 2(2n - 2)$, we have $s\beta = (2n - 2)\alpha$ and $s < t$.

Now we consider each possibility for $S$, separately. If $\rho(p, S) = \{r'_i \mid i \in I\} \cup \{p\}$, then using the results in [19], each $r'_i \in \pi(S)$, where $j \notin I$, is adjacent to $p$ in $\Gamma(S)$.

**Subcase 1.1.** Let $S \cong L_m(q')$. By [19, Proposition 2.6], we see that each prime divisor of $|L_m(q')|$ is adjacent to $p$, except $r'_m$ and $r'_{m-1}$. Hence $\rho(p, S) = \{p, r'_m, r'_{m-1}\}$. Therefore $p_1$ and $p_2$ are two primitive prime divisors of $q^{m-1} - 1$ and $q^{m-1} - 1$. Since $s < t$, we conclude that $m = t$ and $m - 1 = s$. Hence $2n\alpha = m\beta$ and $(2n - 2)\alpha = (m - 1)\beta$. Consequently, we get that $\beta = 2\alpha$ and $m = n$, that is $S \cong L_n(p^{2\alpha})$. Then $S$ has a maximal torus of order $(p^{2\alpha} - 1)/((p^{2\alpha} - 1)(n, p^{2\alpha} - 1))$, say $T$. Obviously, $r_n, r_{2n} \in \pi(T)$. 

\[ \square \]
Therefore $r_n \sim r_{2n}$ in $\Gamma(L_n(p^{2n}))$, whereas $r_n \sim r_{2n}$ in $\Gamma(G)$, by Lemma 2.3, which is a contradiction.

**Subcase 1.2.** Let $S \cong U_m(q')$. If $m = 3$, then $\rho(p, S) = \{p, r'_1 \neq 2, r'_6\}$ and so $s = 1$ and $t = 6$, hence $(2n - 2)\alpha = \beta$ and $2n\alpha = 6\beta$. Therefore $n = 6/5$, a contradiction.

If $m \equiv 0 \pmod{4}$, then $\rho(p, S) = \{p, r'_{m-2}, r'_m\}$ and so $s = m$ and $t = 2m - 2$, hence $(2n - 2)\alpha = m\beta$ and $2n\alpha = (2m - 2)\beta$. Then $n = (2m - 2)/(m - 2)$ and so $n = 3$, a contradiction.

If $m \equiv 3 \pmod{4}$, then $\rho(p, S) = \{p, r'_{(m-1)/2}, r'_m\}$. Therefore $s = (m - 1)/2$ and $t = 2m$.

Hence $(2n - 2)\alpha = (m - 1)\beta/2$ and $2n\alpha = 2m\beta$. Now easy computation shows that it is impossible.

If $m \equiv 1, 2 \pmod{4}$, then similarly to the above discussion, we get a contradiction.

**Subcase 1.3.** Let $S \cong B_m(q')$ or $C_m(q')$. Since $t(p, S) \geq 3$, using [19, Tables 4], we get that $m$ is odd. In this case $\rho(p, S) = \{p, r'_m, r'_{2m}\}$. Hence $s = m$ and $t = m$ and so $(2n - 2)\alpha = m\beta$ and $2n\alpha = m\beta$, which implies that $n = 2$, a contradiction.

Let $S \cong 2D_m(q')$, where $m$ is odd. Since $\rho(p, S) = \{p, r'_{2m-2}, r'_{2m}\}$, we conclude that $(2n - 2)\alpha = (2m - 2)\beta$ and $2n\alpha = 2m\beta$ and so $m = n$, which is impossible, since $n$ is even.

Similarly, we can prove that $S \not\cong 2D_m(q')$, where $m$ is even and $S \not\cong D_m(q')$.

**Case 2.** Let $r_{2n-2} \not\in \pi(S)$. Hence $r_{n-1} \in \pi(S)$. Let $p_1$ and $p_2$ be as $r_{n-1}$ and $r_{2n}$, respectively. Therefore $r_{n-1}$ and $r_{2n}$ are primitive prime divisors of $q^s - 1$ and $q^t - 1$, respectively, where $s = e(r_{n-1}, p^\beta)$ and $t = e(r_{2n}, p^\beta)$. Now we conclude that $(n - 1)\alpha | s\beta$ and $2n\alpha | t\beta$. On the other hand, using Zsigmondy’s theorem, we conclude that $t\beta \leq 2n\alpha$ and so $t\beta = 2n\alpha$. If $s\beta > (n - 1)\alpha$, then using Zsigmondy’s theorem we conclude that $s\beta = (2n - 2)\alpha$, which implies that $r_{2n-2} \in \pi(S)$, which is a contradiction. Hence we suppose that $s\beta = (n - 1)\alpha$.

**Subcase 2.1.** Let $S \cong L_m(q')$, where $q' = p^\beta$. We know that $\rho(p, S) = \{p, r'_{m-1}, r'_m\}$. Hence $t = m$ and $s = m - 1$ and $2n\alpha = m\beta$ and $(n - 1)\alpha = (m - 1)\beta$. These equations imply that $m = 2 - 2/\beta(n + 1)$, which is impossible.

**Subcase 2.2.** Let $S \cong 2D_m(q')$, where $m$ is odd. We note that $\rho(p, S) = \{p, r'_{2m-2}, r'_{2m}\}$ and so $(n - 1)\alpha = (2m - 2)\beta$ and $2n\alpha = 2m\beta$ and so $m = 2 - 2/(n + 1)$, which is impossible.

**Subcase 2.3.** Let $S \cong D_m(q')$, where $m$ is even. Since $\rho(p, S) = \{p, r'_{m-1}, r'_{2m-2}, r'_{2m}\}$, we get that $2n\alpha = 2m\beta$ and $(n - 1)\alpha = (2m - 2)\beta$ or $(n - 1)\alpha = (m - 1)\beta$. If $(n - 1)\alpha = (m - 1)\beta$, then we get that $m = 2 - 2/(n + 1)$, which is impossible. Hence $(n - 1)\alpha = (m - 1)\beta$, which implies that $m = n$ and $\alpha = \beta$, and so $S \cong D$, which is a contradiction, since $r_{2n-2} \not\in \pi(S)$.

We can use a similar proof for groups $U_m(q')$, $B_m(q')$, $C_m(q')$ and $D_m(q')$ and get a contradiction. We omit the proof for convenience.

**Lemma 3.3.** If $S$ is isomorphic to a classical simple group of Lie type over a field of characteristic $p' \neq p$, then $S \not\cong D$.

**Proof.** Let $S$ be isomorphic to a classical simple group of Lie type over a field with $q'$ elements, where $q' = p^\beta$. Using [19, Table 4], $t(p', S) \leq 4$ and so Lemma 2.1 implies that $t(p', G) \leq 5$. On the other hand, by Lemma 2.3, we deduce that if $r \in \pi(G) \setminus \{r_1, r_2, r_3, r_4, r_6\}$, then $t(r, G) > 5$. Hence $p' \in \{r_1, r_2, r_3, r_4, r_6\}$ and so $p' | (q^2 + 1)(q^3 - 1)$.
Consider $r'_3 \in \pi(S) \subseteq \pi(G)$ and $3 = e(r'_3, q') \leq e(r'_3, p')$. By Lemmas 2.3, 2.4, 2.5 and 2.6 we get that for each classical simple group of Lie type $S$, we have $t(r'_3, S) \leq 6$. On the other hand using Remark 2.2, we have $t(r'_3, G) \leq t(r'_3, S) + 1$ and so $t(r'_3, G) \leq 7$. We note that $r'_3 \in \pi(S) \subseteq \pi(G) = \pi(D_{2k}(q))$. Hence, by Lemma 2.3, it follows that $e(r'_3, q) \leq 10$. Since $t(S) \geq 13$, we conclude that $r'_3 \in \pi(S)$, where $2 \leq i \leq 10$ and we have similar argument for $r'_i$, $2 \leq i \leq 10$ and we have $e(r'_i, q) \leq 2i + 4$.

Hence according above discussion, if $p' \in \pi((q^2 + 1)(q^6 - 1))$, then the following condition holds:

If $r'_i \in \pi(p'^6 - 1)$, then $e(r'_i, q) \leq 2i + 4$, where $2 \leq i \leq 10$.

Using GAP, we get that the above condition holds only for $q = 54251$, where $p' = 2$. Since $t(S) \geq 13$, we conclude that $r'_{13} \in \pi(S)$. If $p' = 2$ and $q = 54251$, then $r'_{13} = 8191$ and so $e(8191, q) = 1365$, which contradicts to Remark 2.2. Therefore by the above argument, we get that $S$ is not isomorphic to any classical simple group of Lie type over a field of characteristic $p' \neq p$.

Using the Classification Theorem of finite simple groups and Lemmas 3.1, 3.2 and 3.3, we get that the finite simple group $2D_{2k}(q)$, where $k \geq 9$ and $q < 10^5$ is quasirecognizable by prime graph.

**References**


QUASIRECOGNITION BY PRIME GRAPH OF THE GROUPS $2D_{2n}(q)$ WHERE $q < 10^5$


1) Department of Mathematics, Tarbiat Modares University, Tehran, Iran, 2) School of mathematics, statistics and computer, College of science, University of Tehran, Tehran, Iran

E-mail address: A) moradi61hh@yahoo.com, B) darafsheh@ut.ac.ir, C) Iranmana@yahoo.com