Сибирский математический журнал
Сентябрь—октябрь, 2011. Том 52, № 5

УДК 519.542

РАСПОЗНАВАНИЕ ГРУПП $^2D_{2^m+1}(3)$ ПО ГРАФУ ПРОСТЫХ ЧИСЕЛ

А. Бабаи, Б. Хосрави

Аннотация. В [1] показано, что простая группа $^2D_{2^m+1}(3)$ распознаваема по спектру. В настоящей работе получено обобщение этого результата, а именно доказано, что простая группа $^2D_{2^m+1}(3)$ распознаваема по графу простых чисел. Другими словами, доказано, что если G — конечная группа такая, что $\Gamma(G) = \Gamma(^2D_{2^m+1}(3))$, то $G \cong ^2 D_{2^m+1}(3)$.

Ключевые слова: распознавание, граф простых чисел, простая группа, спектр, порядок элемента.

1. Введение

Для целого числа n обозначим через $\pi(n)$ множество всех простых делителей числа n. Если G — конечная группа, то $\pi(G)$ означает $\pi(|G|)$. Множество порядков элементов группы G называется ее *спектром* и обозначается через $\omega(G)$. *Граф простых чисел* группы G, который будем обозначать через $\Gamma(G)$, строится следующим образом: его множеством вершин служит $\pi(G)$ и два различных простых числа p и q соединены ребром (записывается как $p \sim q$) тогда и только тогда, когда в G есть элемент порядка pq. Пусть $s(G)$ — число компонент связности графа $\Gamma(G)$ и $\pi_i(G)$, $i = 1, \dots, s(G)$, — компоненты связности графа $\Gamma(G)$. Если $2 \in \pi(G)$, то всегда считается, что $2 \in \pi_1(G)$. В теории графов множество вершин графа называется *независимым*, если его вершины попарно не смежны. Обозначим через $t(G)$ максимальное число простых чисел из $\pi(G)$, попарно не смежных в $\Gamma(G)$. Другими словами, если $\rho(G)$ — некоторое независимое множество с максимальным числом вершин в $\Gamma(G)$, то $t(G) = |\rho(G)|$. Аналогично некоторое независимое множество, содержащее вершину p, с максимальным числом вершин в $\Gamma(G)$ обозначается через $\rho(p, G)$ и $t(p, G) = |\rho(p, G)|$.

Конечная группа G называется *распознаваемой по графу простых чисел*, если из равенства $\Gamma(H) = \Gamma(G)$ следует, что $H \cong G$. Неабелева простая группа P называется *квазираспознаваемой по графу простых чисел*, если любая конечная группа, граф простых чисел которой совпадает с $\Gamma(P)$, имеет единственный неабелев композиционный фактор, изоморфный P (см. [2]). Очевидно, что из распознаваемости (квазираспознаваемости) по графу простых чисел следует распознаваемость (квазираспознаваемость) по спектру, но обратное в общем случае неверно. Кроме того, не все методы, применяемые для доказательства распознаваемости по спектру, подходят для доказательства распознаваемости по графу простых чисел.

The second author was supported in part by a grant from IPM (N 89200113).

В [3] доказано, что все конечные простые группы с не менее чем тремя компонентами связности (кроме A_6) квазираспознаваемы по спектру. Также в [1] доказано, что ${}^2D_{2^m+1}(3)$ квазираспознаваема по спектру.

Хаги [4] описал все конечные группы G, удовлетворяющие условию $\Gamma(G) = \Gamma(S)$, где S — спорадическая простая группа. В [5] описаны конечные группы, имеющие такой же граф простых чисел, как у простой CIT-группы. Доказано, что для $q = 3^{2n+1}$ $(n > 0)$ простая группа ${}^2G_2(q)$ однозначно определяется своим графом простых чисел [2, 6]. В [7] показано, что группа $PSL(2, p)$, где $p > 11$ — простое число, распознаваема по графу простых чисел при $p \not\equiv 1 \pmod{12}$ и квазираспознаваема по графу простых чисел при $p \equiv 1 \pmod{12}$. В [8, 9] найдены конечные группы с графом простых чисел, как у $PSL(2, q)$. Доказано, что простые группы $F_4(q)$ с $q = 2^n > 2$ [10] и ${}^2F_4(q)$ [11] квазираспознаваемы по графу простых чисел (см. также [12–15]). В [16] авторы доказали, что группа ${}^2D_p(3)$, где $p = 2^n + 1 \geq 5$ — простое число, квазираспознаваема по графу простых чисел.

Основной результат настоящей работы состоит в следующем: если G — конечная группа такая, что $\Gamma(G) = \Gamma({}^2D_{2^m+1}(3))$, то $G \cong {}^2 D_{2^m+1}(3)$. В качестве следствия мы получаем основной результат работы [1].

Все группы, рассматриваемые в статье, конечны, и под простыми группами подразумеваются неабелевы простые группы. Все не определенные явно обозначения стандартны и взяты из [17]. При доказательстве используем классификацию конечных простых групп. Компоненты связности графов простых чисел неабелевых простых групп перечислены в [18], и на протяжении всей статьи пользуемся этим источником. В [19, табл. 2–9] указаны независимые множества и неплотности для всех простых групп, и мы используем эти результаты при доказательстве основной теоремы. Для натурального числа n и простого числа p через n_p обозначается p-часть числа n, т. е. $n_p = p^\alpha$, где $p^\alpha \mid n$ и $p^{\alpha+1} \nmid n$.

2. Предварительные результаты

Определение 2.1 [20]. Конечная группа G называется *двойной группой Фробениуса*, если она обладает нормальным рядом $1 \trianglelefteq H \trianglelefteq K \trianglelefteq G$, где K и G/H — группы Фробениуса с ядрами H и K/H соответственно.

Используя основные структурные свойства групп Фробениуса из [20–22], получаем следующие результаты.

Лемма 2.2. (а) *Пусть G — группа Фробениуса и H, K — фробениусово дополнение и фробениусово ядро группы G соответственно. Тогда $s(G) = 2$ и $\pi(H)$, $\pi(K)$ — компоненты связности графа простых чисел группы G. Кроме того, K нильпотентна, и, следовательно, $\Gamma(K)$ — полный граф. Если H разрешима, то $\Gamma(H)$ — полный граф, а если неразрешима, то $2, 3, 5 \in \pi(G)$ и $\Gamma(H)$ получается из полного графа на множестве $\pi(H)$ удалением ребра, соединяющего вершины 3 и 5.*

(б) *Если G — двойная группа Фробениуса, то $s(G) = 2$ и в обозначениях определения 2.1 выполнены равенства $\pi_1 = \pi(G/K) \cup \pi(H)$ и $\pi_2 = \pi(K/H)$. Кроме того, обе компоненты связности графа $\Gamma(G)$ являются полными графами.*

Лемма 2.3 (теорема Жигмонди) [23]. *Пусть p — простое число и n — положительное целое число. Тогда выполнено одно из следующих утверждений:*

(1) *для* $p^n - 1$ *найдется примитивный простой делитель, т. е. такое простое число* p', *что* $p' \mid (p^n - 1)$, *но* $p' \nmid (p^m - 1)$ *для любого* $1 \leq m < n$ *(как правило,* p' *обозначается через* r_n*);*

(2) $p = 2$, $n = 1$ *или 6;*

(3) p *— простое число Мерсенна и* $n = 2$.

Лемма 2.4 [24, лемма 5]. *Пусть* G *— конечная простая группа* $A_{n-1}(q)$.

(1) *Если существует примитивный простой делитель* r *числа* $q^n - 1$, *то* G *содержит подгруппу Фробениуса с ядром порядка* r *и циклическим дополнением порядка* n.

(2) G *содержит подгруппу Фробениуса с ядром порядка* q^{n-1} *и циклическим дополнением порядка* $(q^{n-1} - 1)/(n, q - 1)$.

Лемма 2.5 [25, лемма 2.8]. *Пусть* G *— конечная простая группа.*

(1) *Если* $G = C_n(q)$, *то* G *содержит подгруппу Фробениуса с ядром порядка* q^n *и циклическим дополнением порядка* $(q^n - 1)/(2, q - 1)$.

(2) *Если* $G = {}^2D_n(q)$ *и существует примитивный простой делитель* r *числа* $q^{2n-2} - 1$, *то* G *содержит подгруппу Фробениуса с ядром порядка* q^{2n-2} *и циклическим дополнением порядка* r.

(3) *Если* $G = D_n(q)$ *или* $B_n(q)$ *и существует примитивный простой делитель* r_m *числа* $q^m - 1$, *где* $m = n$ *или* $n - 1$ *и* m *нечетно, то* G *содержит подгруппу Фробениуса с ядром порядка* $q^{m(m-1)/2}$ *и циклическим дополнением порядка* r_m.

Лемма 2.6 [26]. *Пусть* G *— конечная группа такая, что* $t(G) \geq 3$ *и* $t(2, G) \geq 2$. *Тогда существует конечная неабелева простая группа* S *такая, что* $S \leq \overline{G} = G/K \leq \mathrm{Aut}(S)$ *для максимальной нормальной разрешимой подгруппы* K *группы* G. *Кроме того,* $t(S) \geq t(G) - 1$, *и выполнено одно из следующих утверждений:*

(1) $S \cong A_7$ *или* $L_2(q)$ *для некоторого нечетного* q *и* $t(S) = t(2, S) = 3$;

(2) *для любого простого числа* $p \in \pi(G)$, *не смежного с 2 в* $\Gamma(G)$, *силовская* p*-подгруппа группы* G *изоморфна силовской* p*-подгруппе группы* S. *В частности,* $t(2, S) \geq t(2, G)$.

Следующая лемма является следствием теоремы Грюнберга — Кегеля (см. [27]).

Лемма 2.7. *Если* G *— конечная группа с несвязным графом* $\Gamma(G)$, *то выполнено одно из следующих утверждений:*

(1) $s(G) = 2$ *и* G *— группа Фробениуса;*

(2) $s(G) = 2$ *и* G *— двойная группа Фробениуса;*

(3) *существует неабелева простая группа* S *такая, что* $S \leq \overline{G} = G/N \leq \mathrm{Aut}(S)$, *где* N *— нильпотентная нормальная подгруппа в* G*; кроме того,* N *и* $\overline{G}/S$ *тривиальны или являются* $\pi_1(G)$*-группами, граф* $\Gamma(S)$ *несвязен,* $s(S) \geq s(G)$ *и для каждого* i, *где* $2 \leq i \leq s(G)$, *существует* j *такое, что* $2 \leq j \leq s(S)$ *и* $\pi_i(G) = \pi_j(S)$.

Лемма 2.8 [28, лемма 2.2]. *Если* G *— конечная группа, в графе простых чисел которой больше одной компоненты связности, и* $1 \trianglelefteq N \trianglelefteq M \trianglelefteq G$ *— нормальный ряд такой, что* N *и* G/M *— тривиальные группы или* π_1*-группы, а группа* M/N *проста, то* N *нильпотентна.*

Лемма 2.9. *Пусть G — конечная группа с несвязным графом простых чисел. Пусть K — нормальная π_1-подгруппа в G, и пусть существует неабелева простая группа S такая, что $S \leq \overline{G} = G/K \leq \mathrm{Aut}(S)$ и $\overline{G}/S$ — π_1-группа. Если $K \neq 1$ и S содержит подгруппу Фробениуса с ядром F и циклическим дополнением C, причем $(|F|, |K|) = 1$, то $r \sim \pi(C)$ в $\Gamma(G)$ для некоторого простого делителя r числа $|K|$.*

Доказательство. Очевидно, $KC_G(K)/K \trianglelefteq G/K$, и поскольку S проста, получаем, что $S \cap KC_G(K)/K = 1$ или S. Если $S \cap KC_G(K)/K \neq 1$, то $S \leq KC_G(K)/K \cong C_G(K)/(K \cap C_G(K))$, что невозможно, так как у G несвязный граф простых чисел и $\pi_2(G) \subseteq \pi(S)$. Значит, $F \nleq KC_G(K)/K$ и $(|F|, |K|) = 1$. Теперь из [29, лемма 1] следует, что $r|C| \in \omega(G)$.

Лемма 2.10 [30, 31]. *За исключением соотношений $(239)^2 - 2(13)^4 = -1$ и $(3)^5 - 2(11)^2 = 1$, любое решение уравнения*

$$p^m - 2q^n = \pm 1, \quad p, q \text{ простые}, \ m, n > 1,$$

имеет показатели $m = n = 2$, т. е. получается из единицы $p - q2^{1/2}$ квадратичного расширения $Q(2^{1/2})$ с простыми коэффициентами p, q.

Замечание 2.11 [32]. Пусть p — простое число и $(q, p) = 1$. Пусть $k \geq 1$ — наименьшее положительное целое число такое, что $q^k \equiv 1 \pmod p$. Тогда k называется *порядком числа q по модулю p* и будем обозначать это число через $\mathrm{ord}_p(q)$. Из малой теоремы Ферма следует, что $\mathrm{ord}_p(q)|(p-1)$. Кроме того, если $q^n \equiv 1 \pmod p$, то $\mathrm{ord}_p(q)|n$. Если $a > 1$ — целое число и $(q, a) = 1$, то аналогичным образом определяется $\mathrm{ord}_a(q)$. Для нечетного числа a величина $\mathrm{ord}_a(q)$ также обозначается через $e(a, q)$.

Замечание 2.12 [32]. Пусть $(k, n) = 1$. Если существует целое число x такое, что $x^2 \equiv k \pmod n$, то k называется *квадратичным вычетом* $\pmod n$. В противном случае k называется *квадратичным невычетом* $\pmod n$. Пусть p — нечетное простое число. Значение символа (a/p) равно 1, если a — квадратичный вычет $\pmod p$, равно -1, если a — квадратичный невычет $\pmod p$, и равно нулю, если $p \mid a$. Символ (a/p) называется *символом Лежандра.*

Лемма 2.13 [32]. *Пусть p — нечетное простое число. Тогда $(-1/p) = (-1)^{(p-1)/2}$.*

3. Основные результаты

Лемма 3.1. *Пусть $G = A_{p-1}(q)$ или ${}^2A_{p-1}(q)$, где $q = 2^f$ и $p > 3$ — простое число. Тогда $t(3, G) = 2$.*

Доказательство. Предположим сначала, что $G = A_{p-1}(q)$. Известно, что $\pi_1(G) = \pi\left(2\prod_{i=1}^{p-1}(q^i - 1)\right)$ и $3 \mid (q^2 - 1)$, следовательно, $3 \in \pi_1(G)$. Покажем, что $3 \sim 2$ и 3 смежно с любым числом из $\pi(q^i - 1) \setminus \{3\}$ для $1 \leq i \leq p-1$. Если h — примитивный простой делитель числа $q^i - 1$, где $1 \leq i \leq p-2$, то $3 \sim h$, так как по [19] группа G содержит максимальный тор T такой, что $\frac{(q^i-1)(q^2-1)}{(p,q-1)(q-1)}$ делит $|T|$. Если $h \in \pi(q^{p-1} - 1)$, то 3 смежно с h, поскольку $3 \in \pi(q^{p-1} - 1)$ и $(q^{p-1} - 1) \mid |T|$ для некоторого максимального тора T группы G. С другой стороны, $3 \sim 2$ в силу [19, предложение 3.1]. Таким образом, $t(3, A_{p-1}(q)) = 2$.

Равенство $t(3, G) = 2$ для $G = {}^2A_{p-1}(q)$ доказывается аналогичным образом.

Замечание 3.2. Пусть $G = {}^2D_n(3)$, где $n = 2^m + 1$ не является простым числом. В [18, табл. 1a–1c] указано, что

$$s(G) = 2, \quad \pi_1(G) = \pi\left(3^{n(n-1)}(3^n+1)(3^{n-1}-1)\prod_{i=1}^{n-2}(3^{2i}-1)\right)$$

и нечетная компонента группы G совпадает с $\pi((3^{n-1}+1)/2)$. Также из [19] известно, что $t(2,\ {}^2D_n(3)) = 3$, $\rho(2,{}^2D_n(3)) = \{2, r_{2(n-1)}, r_{2n}\}$, $\rho(3,{}^2D_n(3)) = \{3, r_{2(n-1)}, r_{2n}\}$ и $t({}^2D_n(3)) = [(3n+4)/4]$. Отметим, что $t({}^2D_n(3)) \geq 7$, поскольку $n = 2^m + 1 \geq 9$.

Лемма 3.3. *Пусть $G = {}^2D_n(3)$, где $n = 2^m+1$ не является простым числом, и $A = \{5, r_{2(n-2)}, r_{2(n-1)}, r_{2n}\}$. Тогда A — независимое множество в $\Gamma(G)$.*

Доказательство. По определению $e(5,3) = 4$, $e(r_{2n},3) = 2n$ и $e(r_{2(n-2)},3) = 2(n-2)$. Значит, по [33, предложение 2.4] число 5 не смежно с r_{2n} и $r_{2(n-2)}$, а также r_{2n} не смежно с $r_{2(n-2)}$. С другой стороны, $5, r_{2n}, r_{2(n-2)} \in \pi_1({}^2D_n(3))$, и $r_{2(n-1)}$ лежит в нечетной компоненте. Таким образом, доказательство завершено.

Теорема 3.4. *Если G — конечная группа такая, что $\Gamma(G) = \Gamma({}^2D_{2^m+1}(3))$, то $G \cong {}^2D_{2^m+1}(3)$. Другими словами, ${}^2D_{2^m+1}(3)$ распознаваема по графу простых чисел.*

Доказательство. По условию граф простых чисел группы G несвязен. Если $n = 2^m+1$ — простое число, то $s(G) = 3$, и если $n = 2^m+1$ не простое число, то $s(G) = 2$. Используя [19], получаем, что $t(G) = t({}^2D_n(3)) = [(3n+4)/4] \geq 7$, так как $n \geq 9$. Теперь из леммы 2.2 следует, что G не является ни группой Фробениуса, ни двойной группой Фробениуса. Значит, по леммам 2.7 и 2.8 в G есть нормальный ряд $1 \trianglelefteq N \trianglelefteq M \trianglelefteq G$ такой, что N и G/M тривиальны или являются π_1-группами, а N нильпотентна. Кроме того, M/N — неабелева простая группа с не менее чем $s(G)$ связными компонентами и $G/M \leq \mathrm{Out}(M/N)$. Более того, существует $i \geq 2$ такое, что $\pi_i(M/N) = \pi_2({}^2D_n(3))$. Отметим, что, как показано в доказательстве леммы 2.7, $N = S_{\pi_1}(G)$, т. е. N — максимальная π_1-отделимая нормальная подгруппа группы G. С другой стороны, $t(2,G) \geq 2$ и $t(G) \geq 3$, поэтому по лемме 2.6 существует неабелева простая группа S такая, что $S \leq \overline{G} = G/K \leq \mathrm{Aut}(S)$, где K — максимальная нормальная разрешимая подгруппа группы G. Очевидно, K является π_1-отделимой, следовательно, $K \subseteq N$. Кроме того, N — нильпотентная нормальная подгруппа в G, и, значит, $N \subseteq K$. Таким образом, $N = K$, $S = M/N$ и $\overline{G}/S \leq \mathrm{Out}(S)$.

Покажем, что ${}^2D_{2^m+1}(3)$ квазираспознаваема по графу простых чисел. Если $n = 2^m + 1$ — простое число, то у $\Gamma(G)$ три компоненты связности. Тогда согласно [16] группа ${}^2D_{2^m+1}(3)$ квазираспознаваема по графу простых чисел, т. е. $S \cong {}^2D_{2^m+1}(3)$. Следовательно, можно считать, что $n = 2^m + 1$ — не простое число. В этом случае $s(G) = s({}^2D_n(3)) = 2$ и $t({}^2D_n(3)) \geq 7$. По лемме 2.6 выполнены неравенства $t(S) \geq t(G) - 1$ и $t(2,S) \geq t(2,G)$. Кроме того, по лемме 2.7 справедливо неравенство $s(S) \geq s(G) = 2$ и найдется $i \geq 2$ такое, что $\pi_2({}^2D_n(3)) = \pi_i(S)$. Далее в тексте r_i обозначает примитивный простой делитель числа $3^i - 1$. В силу замечания 3.2 и леммы 2.6 имеем $r_{2n} \in \rho(2,G)$ и, значит, $r_{2n} \in \pi(S)$. Рассмотрим все возможности для группы S, следуя [18, табл. 1a–1c].

Случай 1. Пусть $S \cong G_2(q)$, где $q = 3^f$. Известно, что $t(G_2(q)) = 3$ и $t({}^2D_n(3)) \geq 7$. Следовательно, $t(S) < t(G) - 1$; противоречие.

Аналогичным образом доказывается, что S не изоморфна ни одной из групп $F_4(q)$, $E_6(q)$, ${}^2E_6(q)$, ${}^3D_4(q)$, ${}^2B_2(q)$, где $q = 2^{2n+1}$; ${}^2G_2(q)$, где $q = 3^{2n+1}$; ${}^2F_4(q)$, где $q = 2^{2n+1}$; ${}^2F_4(2')$, $A_1(q)$, $A_2(2)$, $A_2(4)$, ${}^2A_5(2)$ и ни одной из спорадических групп, исключая, возможно, J_4.

Случай 2. Пусть $S \cong A_{p-1}(q)$, где $(p,q) \neq (3,2),(3,4)$, $q = r^f$ и p — нечетное простое число. Если $p = 3$, то $t(A_2(q)) \leq 4$ по [19]. Тогда $t(S) < t(G)-1$, что неверно. Следовательно, $p \geq 5$. Если q нечетно, то $t(2, A_{p-1}(q)) = 2$ по [19], и получаем противоречие с леммой 2.6, так как $t(2,G) = 3$. Значит, $q = 2^f$. Из замечания 3.2 и леммы 2.6 следует, что $r_{2n} \in \pi(S)$. Поскольку $r_{2n} \in \pi_1(G)$ и $s(S) = 2$, получаем, что $r_{2n} \in \pi_1(S)$. Тогда 3 смежно с r_{2n} по лемме 3.1, что противоречит замечанию 3.2.

Аналогичным образом доказывается, что S не изоморфна ${}^2A_{p-1}(q)$.

Случай 3. Пусть $S \cong A_p(q)$, где $(q-1) \mid (p+1)$, или $S \cong {}^2A_p(q)$, где $(q+1) \mid (p+1)$, $(p,q) \neq (3,3),(5,2)$, причем $q = r^f$ и $p \geq 3$ — простое число. Определим $A_p^\varepsilon(q)$, где $\varepsilon \in \{+,-\}$, следующим образом: $A_p^+(q) = A_p(q)$ и $A_p^-(q) = {}^2A_p(q)$.

Поскольку $t(A_p^\varepsilon(q)) \leq 4$ при $p \leq 7$ по [19], заключаем, что $p > 7$.

(a) Пусть q нечетно. Если $(p+1)_2 \neq (q-\varepsilon 1)_2$ или $(p+1)_2 = (q-\varepsilon 1)_2 = 2$, то по [19] выполнено $t(2, A_p^\varepsilon(q)) = 2$; противоречие. Следовательно, $2 < (p+1)_2 = (q-\varepsilon 1)_2$.

(a.1) Если $q = 3^f$, то

$$\pi((3^{n-1}+1)/2) = \pi((3^{pf}-\varepsilon 1)/(3^f-\varepsilon 1)).$$

Пусть x — примитивный простой делитель числа $(3^{pf}-\varepsilon 1)/(3^f-\varepsilon 1)$. Тогда, используя соображения о порядке элемента x, получаем, что $pf \mid 2(n-1) = 2^{m+1}$ и, значит, $p = 2$, что неверно.

(a.2) Пусть $q = r^f$ и $r \neq 3$. По [19, предложение 3.1] число r смежно с 2 в $\Gamma(S)$. Кроме того, для любого $2 \leq i \leq p-1$ число $q^i - (\varepsilon 1)^i$ делит порядок некоторого максимального тора T группы S и $2 \mid |T|$. Поскольку $r_{2n} \in \pi_1(S)$ и $2 \nsim r_{2n}$ в $\Gamma(G)$, получаем, что $e(r_{2n}, q) = p+1$. Дальнейшие рассуждения проводится параллельно для $A_p(q)$ и ${}^2A_p(q)$.

• Если $S \cong A_p(q)$ и $e(3,q) = 2$, то по [19, предложение 2.1] имеем $3 \sim r_{2n}$, что невозможно. Значит, $e(3,q) = 1$.

◦ Если $S \cong {}^2A_p(q)$ и $e(3,q) = 1$, то по [19, предложение 2.2] имеем $3 \sim r_{2n}$, что невозможно. Следовательно, $e(3,q) = 2$.

Возможны два случая.

(1) Пусть $r \neq 5$. Отметим, что $e(5,q) \mid 4$.

• Если $S \cong A_p(q)$ и $e(5,q) = 4$ или $e(5,q) = 2$, то по [19, предложение 2.1] из условия $(p+1)_2 > 2$ следует, что $5 \sim r_{2n}$, а это противоречит лемме 3.3. Значит, $e(5,q) = 1$ и $5 \mid (q-1)$.

◦ Если $S \cong {}^2A_p(q)$ и $e(5,q) = 4$ или $e(5,q) = 1$, то по [19, предложение 2.2] получаем, что $5 \sim r_{2n}$; противоречие с леммой 3.3. Значит, $e(5,q) = 2$ и $5 \mid (q+1)$.

Покажем, что $r_{2(n-2)} \in \pi_1(S)$. В противном случае $r_{2(n-2)} \in \pi(K) \cup \pi(\overline{G}/S)$, поскольку $\pi_2(G) = \pi_2(S)$.

► Если $r_{2(n-2)} \in \pi(\overline{G}/S)$, то

$$r_{2(n-2)} \in \pi(\mathrm{Out}(S)) \subseteq \{2\} \cup \pi(f(p+1, q-\varepsilon 1)).$$

Число $r_{2(n-2)}$ нечетно, поэтому $r_{2(n-2)} \neq 2$. Если $r_{2(n-2)} \mid (q-\varepsilon 1)$, то 5 смежно с $r_{2(n-2)}$, так как $5 \mid (q-\varepsilon 1)$ и $(q-\varepsilon 1) \mid |T|$ для некоторого максимального тора T

группы S; противоречие с леммой 3.3. Если $r_{2(n-2)} \mid f$, то $r_{2(n-2)}$ — порядок полевого автоморфизма группы S. Полевой автоморфизм централизует элементы группы $A_p^\varepsilon(r)$ и $5 \in \pi\big(A_p^\varepsilon(r)\big)$. Следовательно, 5 смежно с $r_{2(n-2)}$; противоречие.

Таким образом, $r_{2(n-2)} \in \pi(K)$.

• Если $S \cong A_p(q)$, то $5 \mid (q-1)$. По лемме 2.4 в $A_p(q)$ есть подгруппа Фробениуса с ядром порядка r', где r' — примитивный делитель числа $q^{p+1}-1$, и циклическим дополнением порядка $p+1$. Поскольку $r' \in \pi(S)$ и $r_{2(n-2)} \notin \pi(S)$, применяя лемму 2.9, получаем, что $r_{2(n-2)} \sim \pi(p+1)$. Отсюда в силу включения $5 \in \pi(q-1) \subseteq \pi(p+1)$ следует, что $5 \sim r_{2(n-2)}$; противоречие.

◦ Если $S \cong {}^2A_p(q)$, то воспользуемся тем, что $C_{(p+1)/2}(q) \leq {}^2A_p(q)$ по [34]. По лемме 2.5 группа $C_{(p+1)/2}(q)$ содержит подгруппу Фробениуса с ядром порядка $q^{(p+1)/2}$ и циклическим дополнением порядка $(q^{(p+1)/2}-1)/2$. По лемме 2.9 получаем, что $r_{2(n-2)} \sim \pi((q^{(p+1)/2}-1)/2)$. Поскольку $(p+1)_2 > 2$ и $e(5,q)=2$, это, в частности, означает, что $5 \sim r_{2(n-2)}$; противоречие.

Таким образом, $r_{2(n-2)} \in \pi_1(S)$. По доказанному $5 \mid (q-\varepsilon 1)$, и $5 \nsim r_{2(n-2)}$ по лемме 3.3. Используя порядки максимальных торов группы S, выводим, что $e(r_{2(n-2)},q) = p+1$. Следовательно, $e(r_{2(n-2)},q) = e(r_{2n},q) = p+1$, и по [19, предложения 2.1, 2.2] число $r_{2(n-2)}$ смежно с r_{2n}, что противоречит лемме 3.3.

(2) Пусть $r=5$ и, значит, $q=5^f$.

• Пусть $S \cong A_p(q)$. По [19] имеем $t(5, A_p(q)) = 3$, и по лемме 3.3 выполнено неравенство $t(5, {}^2D_n(3)) \geq 4$. Поскольку $\{5, r_{2(n-1)}, r_{2n}\} \subseteq \pi(S)$, получаем, что $r_{2(n-2)} \notin \pi(S)$ и, значит, $r_{2(n-2)} \in \pi(K)$ или $r_{2(n-2)} \in \pi(\overline{G}/S)$. Предположим, что $r_{2(n-2)} \in \pi(K)$. По лемме 2.4 в $A_p(q)$ есть подгруппа Фробениуса с ядром порядка $q^p = 5^{fp}$ и циклическим дополнением порядка $(q^p-1)/(q-1)$. Тогда $r_{2(n-2)} \sim \pi((q^p-1)/(q-1))$ по лемме 2.9. Это противоречит тому, что $r_{2(n-2)}$ лежит в $\pi_1(G)$. Следовательно, $r_{2(n-2)} \in \pi(\overline{G}/S) \subseteq \pi(\mathrm{Out}(S)) \subseteq \{2\} \cup \pi(f(p+1,q-1))$. Число $r_{2(n-2)}$ нечетно, и $\pi(q-1) \subseteq \pi(S)$, поэтому $r_{2(n-2)} \mid f$. Повторяя рассуждения из п. (1), приходим к противоречию.

◦ Если $S \cong {}^2A_p(q)$, то $3 \mid (q+1)$ и, значит, f нечетно. Отметим, что $\mathrm{ord}_5(16) = 4$ и $4 \nmid (p-1)$, так как $(p+1)_2 > 2$. Следовательно, $16 \nmid (q^{p-1}-1)$. С другой стороны, $\pi((3^{n-1}+1)/2) = \pi((q^p+1)/(q+1))$. Если $x \in \pi((q^p+1)/(q+1))$, то $x \mid (3^{n-1}+1)$. Кроме того, x — примитивный делитель числа $3^{2(n-1)}-1$, иначе x лежал бы в $\pi_1(G)$. Значит, $2(n-1) \mid (x-1)$, откуда $x = 2(n-1)k+1 = 16k'+1$ для некоторых $k,k'>0$. Таким образом, $(q^p+1)/(q+1) = 16k''+1$ для некоторого $k''>0$. Следовательно, $16 \mid (q^{p-1}-1)$, что неверно.

(b) Пусть $q=2^f$. Тогда $r_{2n} \in \pi_1(S)$, так как $s(S)=2$. Значит, либо $r_{2n}=2$, что невозможно, либо $r_{2n} \mid (q^i-(\varepsilon 1)^i)$ для некоторого $2 \leq i \leq p-1$, либо $r_{2n} \mid (q^{p+1}-1)$. Предположим, что r_{2n} — примитивный простой делитель числа $q^i-(\varepsilon 1)^i$ для $2 \leq i \leq p-2$. Существует максимальный тор порядка $\frac{(q^i-(\varepsilon 1)^i)(q^2-1)(q^k-(\varepsilon 1)^k)}{(q-\varepsilon 1)^2}$, где $k = p+1-i-2$. Поскольку $3 \mid (q^2-1)$, числа 3 и r_{2n} смежны; противоречие. Если r_{2n} — примитивный простой делитель числа $q^{p-1}-1$, то $3 \sim r_{2n}$, так как $q^{p-1}-1$ делит порядок некоторого максимального тора группы S. Таким образом, $e(r_{2n},q) = p+1$.

• Если $S \cong A_p(q)$ и $e(3,q)=2$, то по [19, предложение 2.1] числа 3 и r_{2n} смежны; противоречие. Следовательно, $e(3,q)=1$. Поскольку $q=2^f$, получаем, что f четно. Если $e(5,q)=2$, то по [19, предложение 2.1] числа 5 и r_{2n} смежны; противоречие. Значит, $5 \mid (q-1)$. Рассуждая, как выше, можно показать, что $r_{2(n-2)} \in \pi(S)$ и $e(r_{2(n-2)},q) = p+1$. Тогда по [19, предложение 2.1] числа $r_{2(n-2)}$ и r_{2n} смежны; противоречие.

$\circ$ Если $S \cong {}^2A_p(q)$ и $e(3,q) = 1$, то по [19, предложение 2.2] числа 3 и r_{2n} смежны, что неверно. Следовательно, $e(3,q) = 2$, и, значит, f нечетно. Тогда $e(5,q) = 4$. По [19, предложение 2.1] получаем, что $5 \sim r_{2n}$; противоречие.

Случай 4. Пусть $S \cong B_{n'}(q)$, где $n' = 2^{m'} \geq 4$ и q нечетно. Тогда $t(2, B_{n'}(q)) = 2$ по [19], и, используя лемму 2.6, приходим к противоречию.

По тем же причинам S не изоморфна $C_{n'}(q)$, где $n' = 2^{m'} \geq 2$.

Случай 5. Пусть $S \cong B_p(3)$, где $p \geq 3$ — простое число. Тогда $\pi((3^p - 1)/2) = \pi((3^{n-1}+1)/2)$. Следовательно, $p \mid 2(n-1)$, откуда $p = 2$, что неверно.

Аналогичным образом доказывается, что S не изоморфна ни одной из групп $D_p(3)$, $C_p(3)$, $D_{p+1}(3)$ и не изоморфна ${}^2D_p(3)$, где p — простое число и $p \neq 2^{n'} + 1 \geq 5$.

Случай 6. Пусть $S \cong D_{p+1}(2)$, где $p \geq 3$ — простое число. Тогда $\pi(2^p - 1) = \pi((3^{n-1}+1)/2)$. Если $x \in \pi(2^p - 1)$, то $x \mid (3^{n-1}+1)/2$. Следовательно, $3^{n-1} \equiv -1 \pmod{x}$, и, значит, $(-1/x) = 1$. Тогда $x \equiv 1 \pmod{4}$ по лемме 2.13. Таким образом, $2^p - 1 = 4k + 1$, что неверно.

По аналогичным соображениям S не изоморфна $D_p(2)$ и $C_p(2)$.

Случай 7. Пусть $S \cong {}^2D_{n'}(2)$, где $n' = 2^{m'} + 1 \geq 5$. По лемме 2.6 число r_{2n} лежит в $\pi(S)$, поэтому $\rho(3, {}^2D_n(3)) \subseteq \rho(3, {}^2D_{n'}(2))$. С другой стороны, из [33, предложение 2.4] несложно вывести, что $t(3, {}^2D_{n'}(2)) = 2$.

Аналогичным образом доказывается, что S не изоморфна $D_p(5)$.

Случай 8. Пусть $S \cong {}^2D_{n'}(q)$, где $n' = 2^{m'} \geq 4$ и $q = r^f$. По лемме 2.6 число r_{2n} лежит в $\pi(S)$, поэтому $\rho(3, {}^2D_n(3)) \subseteq \rho(3, {}^2D_{n'}(q))$. Теперь, используя [33, предложение 2.4], получаем, что $r = 3$. Тогда по [19] выполнено равенство $t(2, {}^2D_{n'}(q)) = 2$, а это противоречит лемме 2.6.

Случай 9. Пусть $S \cong {}^2D_p(3)$, где $p = 2^{n'} + 1 \geq 5$ простое. Поскольку $s({}^2D_p(3)) = 3$ и $s({}^2D_n(3)) = 2$, нужно рассмотреть два случая. Если $\pi((3^{n-1} + 1)/2) = \pi((3^p+1)/4)$, то $r_{2p} \mid (3^{2(n-1)} - 1)$ и, значит, $2p \mid 2(n-1)$, откуда следует, что $p = 2$; противоречие. Если $\pi((3^{n-1}+1)/2) = \pi((3^{p-1}+1)/2)$, то $r_{2(p-1)} \in \pi((3^{n-1}+1)/2)$, и приходим к противоречию тем же путем.

Случай 10. Пусть $S \cong A_k$, где $k > 6$. Тогда нечетная компонента группы S состоит из одного простого числа r, лежащего в множестве $\{k, k-1, k-2\}$. Если $\pi((3^{n-1}+1)/2) = \{r\}$, то $r = r_{2(n-1)}$, и по лемме 2.10 получаем, что $(3^{n-1}+1)/2 = r$. Пусть $s = r_{2n}$. Тогда s делит $(3^n+1)/4$. Если $s \neq (3^n+1)/4$, то $s \leq (3^n+1)/12 < k - 3$ и, значит, числа 3 и s смежны в $\Gamma(G)$; противоречие. Таким образом, $s = (3^n+1)/4$. Несложно видеть, что $s > k$. Следовательно, $s \nmid |A_k|$, а это противоречит тому, что $r_{2n} = s \in \pi(S)$ по замечанию 3.2.

Случай 11. Пусть $S \cong E_8(q)$. Тогда множество $\pi((3^{n-1}+1)/2)$ должно равняться нечетной компоненте группы $E_8(q)$.

(11.1) Предположим, что $q \equiv 2, 3 \pmod{5}$. Если

$$\pi((3^{n-1}+1)/2) = \pi(q^8 - q^4 + 1) \subseteq \pi(q^{24} - 1),$$

то любой x из $\pi((3^{n-1}+1)/2)$ лежит в $\pi(q^{24}-1)$. Покажем, что x — примитивный простой делитель числа $(q^{24}-1)$. В противном случае найдется натуральное число l такое, что $l|24$ и $x|(q^l - 1)$. Тогда $l \in \{1, 2, 3, 4, 6, 8, 12\}$ и из [18, табл. 1a–1c] следует, что $x \in \pi_1(E_8(q))$; противоречие. Значит, $24 \mid (x-1)$, откуда $x = 24k'+1$ для некоторого $k' > 0$. Следовательно, $(3^{n-1}+1)/2 = 24k+1$ для некоторого $k > 0$, откуда $3^{n-1} - 24k'' = 1$ для некоторого $k'' > 0$, что неверно. Если

$$\pi((3^{n-1}+1)/2) = \pi(q^8 - q^7 + q^5 - q^4 + q^3 - q + 1) \subseteq \pi(q^{15}-1)$$

или

$$\pi((3^{n-1}+1)/2) = \pi(q^8 + q^7 - q^5 - q^4 - q^3 + q + 1) \subseteq \pi(q^{30}-1),$$

то противоречие достигается аналогичным образом.

(11.2) Если $q' \equiv 0, 1, 4 \pmod 5$, то противоречие достигается так же, как в (11.1).

Случай 12. Пусть $S \cong E_7(2)$. Поскольку $s(E_7(2)) = 3$, рассмотрим два случая. Если $\pi((3^{n-1}+1)/2) = \pi(73)$, то по лемме 2.10 выполнено равенство $(3^{n-1}+1)/2 = 73$, которое невозможно. Если $\pi((3^{n-1}+1)/2) = \pi(127)$, то аналогичным образом приходим к противоречию.

Таким же образом показывается, что S не изоморфна ни $E_7(3)$, ни J_4.

Случай 13. Пусть $S \cong {}^2D_{n'}(3)$, где $n' = 2^{m'}+1$ не простое. Тогда

$$\pi((3^{n-1}+1)/2) = \pi((3^{n'-1}+1)/2),$$

откуда $r_{2(n-1)} \in \pi((3^{n'-1}+1)/2)$. Следовательно, $(n-1) \mid (n'-1)$. По тем же соображениям $(n'-1) \mid (n-1)$. Значит, $n = n'$ и $S \cong {}^2D_n(3)$. Таким образом, ${}^2D_n(3)$ квазираспознаваема по графу простых чисел.

Теперь покажем, что $K = 1$. В противном случае можно без потери общности считать, что K — элементарная абелева p-группа. По лемме 2.5 в ${}^2D_n(3)$ есть подгруппа Фробениуса с ядром порядка 3^{2n-2} и циклическим дополнением порядка r_{2n-2}, где r_{2n-2} — примитивный простой делитель числа $3^{2n-2}-1$. Если $p \neq 3$, то $p \sim r_{2n-2}$ по лемме 2.9. Это противоречит тому, что $p \in \pi_1(G)$ и $r_{2n-2} \in \pi_2(G)$. Значит, $r = 3$. По [35, теорема 1.3] любой элемент группы S имеет неподвижную точку в K, что приводит к противоречию.

Таким образом, $S \trianglelefteq G \leq \mathrm{Aut}(S)$. Предположим, что n — не простое число. Если $G \neq S$, то граф $\Gamma(G)$ связен в силу [36, теорема 5]. Следовательно, в этом случае $G \cong {}^2D_n(3)$. Пусть теперь n — простое число. Если $G \ncong {}^2D_n(3)$, то по [36, теорема 5] группа G изоморфна группе $S : \langle\gamma\rangle$, где γ — полевой автоморфизм группы S порядка 2. Как указано в [34], централизатор $C_S(\gamma)$ содержит подгруппу, изоморфную $B_{n-1}(3)$. Значит, $r_{2(n-1)} \in \pi(C_S(\gamma))$, откуда следует, что $2 \sim r_{2n-2}$; противоречие с замечанием 3.2. Следовательно, $G \cong S$. Таким образом, ${}^2D_n(3)$ распознаваема по графу простых чисел, и доказательство теоремы завершено.

Благодарности. Авторы выражают благодарность рецензенту за ценные замечания. Второй автор благодарит Исследовательский институт фундаментальных наук (IPM) за финансовую поддержку.

ЛИТЕРАТУРА

1. *Kondrat'ev A. S.* Recognition by spectrum of the groups ${}^2D_{2^m+1}(3)$ // Sci. China Ser. A. 2009. V. 52, N 2. P. 293–300.
2. *Хосрави А., Хосрави Б.* Квазираспознавание простой группы ${}^2G_2(q)$ по графу простых чисел // Сиб. мат. журн. 2007. Т. 48, № 3. С. 707–716.

3. *Алексеева О. А., Кондратьев А. С.* Квазираспознаваемость одного класса конечных простых групп по множеству порядков элементов // Сиб. мат. журн. 2003. Т. 44, № 2. С. 241–255.

4. *Hagie M.* The prime graph of a sporadic simple group // Comm. Algebra. 2003. V. 31, N 9. P. 4405–4424.

5. *Khosravi B., Khosravi B., Khosravi B.* Groups with the same prime graph as a CIT simple group // Houston J. Math. 2007. V. 33, N 4. P. 967–977.

6. *Заварницын А. В.* О распознавании конечных групп по графу простых чисел // Алгебра и логика. 2006. Т. 45, № 4. С. 390–408.

7. *Khosravi B., Khosravi B., Khosravi B.* On the prime graph of $PSL(2,p)$ where $p>3$ is a prime number // Acta Math. Hungar. 2007. V. 116, N 4. P. 295–307.

8. *Хосрави А., Хосрави Б.* 2-Распознаваемость $PSL(2,p^2)$ по графу простых чисел // Сиб. мат. журн. 2008. Т. 49, № 4. С. 934–944.

9. *Khosravi B.* n-Recognition by prime graph of the simple group $PSL(2,q)$ // J. Algebra Appl. 2008. V. 7, N 6. P. 735–748.

10. *Khosravi B., Babai A.* Quasirecognition by prime graph of $F_4(q)$ where $q=2^n>2$ // Monatsh. Math. (to appear) (DOI: 10.1007//s00605-009-0155-6)

11. *Akhlaghi Z., Khatami M., Khosravi B.*, Quasirecognition by prime graph of the simple group ${}^2F_4(q)$ // Acta Math. Hungar. 2009. V. 122, N 4. P. 387–397.

12. *Akhlaghi Z., Khosravi B., Khatami M.* Characterization by prime graph of $PGL(2,p^k)$ where p and $k>1$ are odd // Int. J. Algebra Comput. 2010. V. 20, N 7. P. 847–873.

13. *Khosravi B., Akhlaghi Z., Khatami M.* Quasirecognition by prime graph of simple group $D_n(3)$ // Publ. Math. Debrecen, Doklady Math. Deb. (to appear)

14. *Khosravi B., Moradi H.* Quasirecognition by prime graph of finite simple groups $L_n(2)$ and $U_n(2)$ // Acta. Math. Hungar. (to appear)

15. *Khosravi B.* Some characterizations of $L_9(2)$ related to its prime graph // Publ. Math. Debrecen, Doklady Math. Deb. 2009. V. 75, N 3–4. P. 375–385.

16. *Babai A., Khosravi B., Hasani N. Quasirecognition by prime graph of ${}^2D_p(3)$ where $p=2^n+1\geq 5$ is a prime* // Bull. Malays. Math. Sci. Soc. (2). 2009. V. 32, N 3. P. 343–350.

17. *Conway J. H., Curtis R. T., Norton S. P., Parker R. A., Wilson R. A.* Atlas of finite groups. Oxford: Oxford Univ. Press, 1985.

18. *Васильев А. В., Гречкосеева М. А.* О распознаваемости конечных простых ортогональных групп размерности 2^m, 2^m+1 и 2^m+2 над полем характеристики 2 // Сиб. мат. журн. 2004. Т. 45, № 3. С. 510–526.

19. *Васильев А. В., Вдовин Е. П.* Критерий смежности в графе простых чисел конечной простой группы // Алгебра и логика. 2005. Т. 44, № 6. С. 682–725.

20. *Gruenberg K. W., Roggenkamp K. W.* Decomposition of the augmentation ideal and of the relation modules of a finite group // Proc. London Math. Soc. (3). 1975. V. 31, N 2. P. 149–166.

21. *Gorenstein D.* Finite Groups. New York: Harper and Row, 1968.

22. *Huppert B.* Endliche Gruppen. I. Berlin: Springer-Verl., 1967.

23. *Zsigmondy K.* Zur theorie der potenzreste // Monatsh. Math. Phys. 1892. V. 3. P. 265–284.

24. *Васильев А. В., Гречкосеева М. А.* О распознавании по спектру конечных простых линейных групп над полями характеристики 2 // Сиб. мат. журн. 2005. Т. 46, № 4. С. 749–758.

25. *He H., Shi W. Recognition of some finite simple groups of type $D_n(q)$ by spectrum* // Int. J. Algebra Comput. 2009. V. 19, N 5. P. 681–698.

26. *Васильев А. В.* О связи между строением конечной группы и свойствами ее графа простых чисел // Сиб. мат. журн. 2005. Т. 46, № 3. С. 511–522.

27. *Williams J. S.* Prime graph components of finite groups // J. Algebra. 1981. V. 69, N 2. P. 487–513.

28. *Khosravi A., Khosravi B.* r-Recognizability of $B_n(q)$ and $C_n(q)$ where $n=2^m\geq 4$ // J. Pure Appl. Algebra. 2005. V. 199, N 1–3. P. 149–165.

29. *Мазуров В. Д. Характеризации конечных групп множествами порядков их элементов* // Алгебра и логика. 1997. Т. 36, № 1. С. 37–53.

30. *Crescenzo P.* A diophantine equation which arises in the theory of finite groups // Adv. Math. 1975. V. 17, N 1. P. 25–29.

31. *Khosravi A., Khosravi B.* A new characterization of some alternating and symmetric groups // Houston J. Math. 2004. V. 30, N 4. P. 953–967.

32. *Sierpiński W.* Elementary theory of numbers, Panstwowe. Warsaw: Wydawnictwo Nauk., 1964. (Monogr. Mat.; V. 42).

33. *Vasil'ev A. V., Vdovin E. P.* Cocliques of maximal size in the prime graph of a finite simple group // http://arxiv.org/abs/0905.1164v1.

34. *Stensholt E.* Certain embeddings among finite groups of Lie type // J. Algebra. 1978. V. 53. P. 136–187.

35. *Guralnick R. M., Tiep P. H.* Finite simple unisingular groups of Lie type // J. Group Theory. 2003. V. 6, N 3. P. 271–310.

36. *Lucido M. S.* Prime graph components in finite almost simple groups // Rend. Sem. Mat. Univ. Padova. 2002. V. 107. P. 189–190.

Статья поступила 18 февраля 2010 г.

Azam Babai
Dept. of Pure Math., Faculty of Math. and Computer Sci.,
Amirkabir University of Technology (Tehran Polytechnic)
424, Hafez Ave., Tehran 15914, Iran

Behrooz Khosravi
School of Mathematics, Institute for Research in Fundamental Sciences (IPM);
Dept. of Pure Math., Faculty of Math. and Computer Sci.,
Amirkabir University of Technology (Tehran Polytechnic)
424, Hafez Ave., Tehran 15914, Iran
khosravibbb@yahoo.com