Сибирский математический журнал
Июль—август, 2005. Том 46, № 4

УДК 512.542

О РАСПОЗНАВАНИИ ПО СПЕКТРУ КОНЕЧНЫХ ПРОСТЫХ ЛИНЕЙНЫХ ГРУПП НАД ПОЛЯМИ ХАРАКТЕРИСТИКИ 2

А. В. Васильев, М. А. Гречкосеева

Аннотация: Конечная группа G называется распознаваемой по спектру, т. е. множеству порядков элементов, если любая конечная группа H, имеющая такой же спектр, что и G, изоморфна G. Показано, что простые линейные группы $L_n(2^k)$ распознаваемы по спектру при $n = 2^m \geq 32$.

Ключевые слова: конечная группа, конечная простая группа, линейная группа, спектр группы, распознавание по спектру, граф простых чисел.

Введение

Для конечной группы G обозначим через $\omega(G)$ ее *спектр*, т. е. множество порядков ее элементов. Группа G называется *распознаваемой по спектру* (короче, *распознаваемой*), если любая конечная группа H, удовлетворяющая условию $\omega(H) = \omega(G)$, изоморфна G. Поскольку любая конечная группа, обладающая нетривиальной нормальной разрешимой подгруппой, нераспознаваема, то в первую очередь интерес представляет вопрос о распознаваемости простых и почти простых групп.

К настоящему времени существует обширный список конечных простых и почти простых групп, для которых проблема распознаваемости решена. Наиболее современный вариант этого списка представлен в [1, табл. 1]; ссылки на некоторые новые результаты можно найти в [2].

Подавляющее большинство распознаваемых групп из этого списка имеет несвязный граф простых чисел, и доказательство их распознаваемости существенно использует это условие. Это вызвано тем, что несвязность графа конечной простой группы позволяет применить теорему Грюнберга — Кегеля при установлении некоторого свойства этой группы, названного в [3] квазираспознаваемостью. Конечная неабелева простая группа S называется *квазираспознаваемой*, если любая конечная группа H с таким же спектром, что и S, содержит единственный неабелев композиционный фактор и этот фактор изоморфен S.

К сожалению, несвязность графа простых чисел является среди конечных простых групп скорее исключением, чем правилом. Однако в недавно опубликованной работе [2] была установлена структурная теорема, позволяющая

Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований (код проекта 05–01–00797), Совета по грантам президента РФ и государственной поддержке ведущих научных школ (код проекта НШ–2069.2003.1), программы Рособразования «Развитие научного потенциала высшей школы» (код проекта 8294), программы «Университеты России» (код проекта УР.04.01.202), а также гранта Президиума СО РАН (№ 86–197).

приступать к доказательству квазираспознаваемости при гораздо более слабых условиях на рассматриваемую группу. В частности, она применима к почти всем простым группам лиева типа. В настоящей работе на основе этого результата мы доказываем распознаваемость бесконечной серии конечных простых линейных групп над полями характеристики 2.

Теорема. *Пусть* $L = L_n(q)$, *где* $n = 2^m \geq 32$, $q = 2^k \geq 2$. *Тогда* L *распознаваема по спектру.*

§ 1. Предварительные обозначения и результаты

Пусть G — конечная группа, $\omega(G)$ — ее спектр. Множество $\omega(G)$ упорядочено отношением делимости, и через $\mu(G)$ обозначается подмножество его максимальных по делимости элементов. Если p — простое число, то *p-периодом* группы G называется максимальная степень p, лежащая в $\omega(G)$.

Пусть $\pi(G)$ — множество простых делителей порядка G. На множестве $\pi(G)$ задается граф со следующим отношением смежности: вершины p и r из $\pi(G)$ соединены ребром тогда и только тогда, когда $pr \in \omega(G)$. Этот граф называется *графом Грюнберга — Кегеля* или *графом простых чисел* группы G и обозначается через $GK(G)$. Опираясь на указанное графовое представление, будем говорить, что простые делители p и r порядка группы G *смежны*, если вершины p и r соединены ребром в $GK(G)$. В противном случае будем говорить, что числа p и r *несмежны*.

Множество вершин графа называется *независимым*, если вершины этого множества попарно несмежны. Мощность произвольного независимого множества с наибольшим числом вершин принято называть *числом вершинной независимости* или *неплотностью* графа. Обозначим через $t(G)$ неплотность графа $GK(G)$ группы G. По аналогии обозначим через $t(2,G)$ наибольшее число вершин в независимых множествах графа $GK(G)$, содержащих вершину 2, и назовем это число *2-неплотностью*.

В [2] доказана следующая теорема, связывающая строение конечной группы со свойствами ее графа простых чисел.

Лемма 1. *Пусть G — конечная группа, удовлетворяющая двум условиям:*

(а) *существует три простых числа из $\pi(G)$, попарно несмежных в $GK(G)$, т. е. $t(G) \geq 3$;*

(б) *существует нечетное простое число из $\pi(G)$, несмежное в $GK(G)$, с числом 2, т. е. $t(2,G) \geq 2$.*

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 выполняется одно из следующих утверждений:

(1) *$S \simeq \mathrm{Alt}_7$ или $L_2(q)$ для некоторого нечетного числа q и $t(S) = t(2,S) = 3$;*

(2) *для каждого простого числа $p \in \pi(G)$, несмежного с 2 в $GK(G)$, силовская p-подгруппа группы G изоморфна силовской p-подгруппе группы S, в частности, $t(2,S) \geq t(2,G)$.*

Доказательство. См. [2].

В [4] вычислены значения неплотности и 2-неплотности для всех конечных простых групп. Заметим, что из этих результатов и предыдущей леммы вытекает

Следствие. *Пусть L — конечная неабелева простая группа, отличная от групп $L_3(3)$, $U_3(3)$, $S_4(3)$, Alt_{10} и Alt_n, где n таково, что $\{r \mid n-3 \le r \le n,\ r$ простое$\} = \varnothing$. Пусть G — конечная группа, удовлетворяющая условию $\omega(G) = \omega(L)$. Тогда для группы G имеет место заключение леммы 1.*

Доказательство. См. [4, следствие 7.2].

В работе используются следующие теоретико-числовые обозначения. Если n — натуральное число, то $\pi(n)$ — это множество простых делителей числа n. Если $p \in \pi(n)$, то n_p — это максимальная степень числа p, являющаяся делителем числа n. Через $[x]$ обозначается целая часть числа x. Если q — натуральное число, r — нечетное простое число и $(q, r) = 1$, то через $e(r, q)$ обозначается наименьшее натуральное число m такое, что $q^m \equiv 1 \pmod r$. Для нечетного q положим $e(2, q) = 1$, если $q \equiv 1 \pmod 4$, и $e(2, q) = 2$, если $q \equiv -1 \pmod 4$.

При исследовании строения графа простых чисел конечных простых групп лиева типа фундаментальное значение имеет следующий теоретико-числовой результат.

Лемма 2 (Жигмонди). *Пусть q — натуральное число, большее 1. Тогда для каждого натурального числа m существует простое число r такое, что $e(r, q) = m$, за исключением следующих случаев:*

(1) *$m = 6$ и $q = 2$;*

(2) *$m = 2$ и $q = 2^l - 1$ для некоторого натурального числа l.*

Доказательство. См. [5].

Простое число r, удовлетворяющее условию $e(r, q) = m$, называется *примитивным простым делителем* числа $q^m - 1$. При фиксированном q мы будем обозначать через r_m любой примитивный делитель числа $q^m - 1$ (очевидно, что число $q^m - 1$ может иметь более одного примитивного простого делителя).

Лемма 3. *Пусть G — конечная группа, $K \lhd G$, G/K — группа Фробениуса с ядром F и циклическим дополнением C. Если $(|F|, |K|) = 1$ и F не содержится в $KC_G(K)/K$, то $r \cdot |C| \in \omega(G)$ для некоторого простого делителя r числа $|K|$.*

Доказательство. См. [6, лемма 1].

Лемма 4. *Пусть L — простая группа $L_n(q)$, q — степень простого числа p, $d = (q-1, n)$. Тогда*

(1) *$\frac{q^{n-1}-1}{d}$ принадлежит $\mu(L)$;*

(2) *p-период группы L равен p^m, где m — это наименьшее натуральное число такое, что $n \le p^m$;*

(3) *для любого $r \in \pi(L)$ найдется $s \in \pi(L)$, несмежное с r; кроме того, если $n \ge 4$ и $(n, q) \ne (6, 2), (7, 2)$, то в качестве числа s можно взять либо примитивный простой делитель r_n числа $q^n - 1$, либо примитивный простой делитель r_{n-1} числа $q^{n-1} - 1$.*

Доказательство. (1) См. [7, предложение 7].

(2) См. [8, предложение 0.5].

(3) Если $n = 2, 3$, то утверждение верно, так как в этом случае граф $GK(L)$ несвязен. Для групп $L_6(2)$, $L_7(2)$ утверждение доказывается прямой проверкой. Пусть $n \ge 4$ и $(n, q) \ne (6, 2), (7, 2)$. По лемме 2 существуют примитивные простые делители r_n и r_{n-1} чисел $q^n - 1$ и $q^{n-1} - 1$ соответственно. В силу [4, предложения 2.1, 3.1 и 4.1] простое число r несмежно либо с r_n, либо с r_{n-1}.

Лемма 5. *Пусть L — простая группа $L_n(q)$, $d = (q-1, n)$. Тогда*

(1) *если существует примитивный простой делитель r числа $q^n - 1$, то в L есть подгруппа Фробениуса с ядром порядка r и циклическим дополнением порядка n;*

(2) *в L есть подгруппа Фробениуса с ядром порядка q^{n-1} и циклическим дополнением порядка $\frac{q^{n-1}-1}{d}$.*

Доказательство. (1) Мы будем использовать построение максимальных торов конечной группы лиева типа на основе максимальных торов соответствующей алгебраической группы, описанное в [9, гл. 3]. Если X — группа и α — некоторый ее автоморфизм, то централизатор α в X обозначим через X_α.

Пусть $\overline{\mathbb{F}}_q$ — алгебраическое замыкание поля порядка q и $\overline{G} = SL_n(\overline{\mathbb{F}}_q)$. Пусть σ — автоморфизм Фробениуса группы $\overline{G}$ такой, что $G = \overline{G}_\sigma$ изоморфна $SL_n(q)$. Пусть $\overline{D}$ — группа диагональных матриц в $\overline{G}$, π — естественный гомоморфизм $N_{\overline{G}}(\overline{D})$ на Sym_n и w — элемент из $N_{\overline{G}}(\overline{D})$ такой, что $w^\sigma = w$ и $\pi(w)$ — цикл длины n. Положим $\sigma_w = \sigma \circ c_w^{-1}$, где c_w — сопряжение с помощью w. Тогда $\overline{T} = \overline{D}_{\sigma_w}$ — циклическая группа порядка $\frac{q^n-1}{q-1}$.

Пусть t — элемент группы $\overline{T}$ порядка r. Так как $t^w = t^\sigma = t^q$, то w действует на группе $\langle t\rangle$ сопряжением. Предположим, что $t = t^{w^l}$ для некоторого l. Тогда $t = t^{q^l}$, значит, $t^{q^l-1} = 1$, следовательно, r делит $q^l - 1$. В силу примитивности r число l делится на n, т. е. $w^l = 1$. Таким образом, группа $F = \langle t, w\rangle$ является группой Фробениуса с ядром порядка r и дополнением порядка n. Заметим, что $F \cap Z(G) = \langle t\rangle \cap Z(G) = 1$.

По теореме Ленга — Стейнберга [10] в группе $\overline{G}$ есть элемент g такой, что $\pi(g^{-1}g^\sigma) = \pi(w)$. В силу равенств

$$({}^g t)^\sigma = g^\sigma t^\sigma (g^{-1})^\sigma = gwt^\sigma w^{-1}g^{-1} = gt^{\sigma_w}g^{-1} = {}^g t,$$

$$({}^g w)^\sigma = g^\sigma w (g^{-1})^\sigma = gwww^{-1}g^{-1} = {}^g w$$

группа ${}^g F$ лежит в G и ее образ в $G/Z(G)$ является искомой группой Фробениуса.

(2) Рассмотрим в $SL_n(q)$ параболическую подгруппу P, состоящую из всех матриц вида

$$M(a,b) = \left(\begin{array}{c|c} a & 0 \\ \hline b & \det a^{-1} \end{array}\right), \quad \text{где} \quad a \in GL_{n-1}(q), \quad b \in \mathbb{F}_q^{n-1}.$$

Обозначим через A подгруппу группы P, состоящую из всех матриц вида $M(a, \mathbf{0})$, где $\mathbf{0}$ — нулевая строка в $\mathbb{F}_q^{n-1}$. Обозначим через B подгруппу, состоящую из всех матриц вида $M(\mathbf{1}, b)$, где $\mathbf{1}$ — единичная матрица в $GL_{n-1}(q)$. Группа P является полупрямым произведением B на A, причем $M(\mathbf{1}, b)^{M(a,\mathbf{0})} = M(\mathbf{1}, ba\det a)$.

Снова рассмотрим алгебраическое замыкание $\overline{\mathbb{F}}_q$ поля порядка q, алгебраическую группу $\overline{G} = SL_n(\overline{\mathbb{F}}_q)$ и подгруппу $\overline{A}$ группы $\overline{G}$, состоящую из матриц

$$M(a,b) = \left(\begin{array}{c|c} \bar{a} & 0 \\ \hline \mathbf{0} & \det \bar{a}^{-1} \end{array}\right), \quad \text{где} \quad \bar{a} \in GL_{n-1}(\overline{\mathbb{F}}_q).$$

Пусть $\overline{D}$ — группа диагональных матриц в $\overline{A}$, π — естественный гомоморфизм $N_{\overline{A}}(\overline{D})$ на Sym_{n-1} и w — элемент из $N_{\overline{A}}(\overline{D})$ такой, что $\pi(w)$ — цикл длины $n-1$. Положим $\sigma_w = \sigma \circ c_w^{-1}$, где c_w — сопряжение с помощью w. Тогда $\overline{T} =$

$\overline{D}_{\sigma_w}$ является циклической группой порядка $q^{n-1}-1$ и порождается матрицей $t = \mathrm{diag}(\lambda, \lambda^q, \dots, \lambda^{q^{n-2}}, \lambda^{(1-q^{n-1})/(q-1)})$, где λ — примитивный корень степени $q^{n-1}-1$ из единицы. Так же, как в предыдущем пункте, выберем $g \in \overline{A}$ такой, что ${}^g t \in A$, и обозначим группу, порожденную ${}^g t$, через C.

Предположим, что некоторый элемент $M(c, \mathbf{0})$ группы C централизует нетривиальный элемент из B. Тогда $bc \det c = b$, где $b \neq \mathbf{0}$, следовательно, матрица $c \det c$ имеет собственное число, равное 1. Поскольку матрица c сопряжена с матрицей $\mathrm{diag}(\lambda, \lambda^q, \dots, \lambda^{q^{n-2}})$, где $\lambda^{q^{n-1}-1} = 1$, то собственные числа матрицы $c \det c$ равны $\lambda^{q^i} \cdot \lambda^{(1-q^{n-1})/(q-1)}$, $0 \leq i \leq n-2$. Если $\lambda^{q^i} \cdot \lambda^{(1-q^{n-1})/(q-1)} = 1$, то $\lambda^{q^i(q-1)} = 1$, следовательно, $\lambda^{q-1} = 1$. Значит, $M(c, \mathbf{0}) \in Z(SL_n(q))$. Таким образом, ядро действия C на B совпадает с $Z(SL_n(q))$, а все остальные элементы из C действуют на B без неподвижных точек. Следовательно, образ группы BC в $L_n(q)$ является искомой группой Фробениуса. Лемма доказана.

Замечание. Доказательство второго утверждения леммы принадлежит А. В. Заварницину и опубликовано в [11, лемма 3]. Поскольку этот источник не является общедоступным, мы, с любезного позволения автора, приводим доказательство с небольшими уточнениями в настоящей статье.

§ 2. Доказательство теоремы

В этом параграфе мы будем рассматривать классические группы как группы лиева типа и обозначать их согласно [12]. Иногда мы будем использовать обозначения $A_n^\varepsilon(q)$ и $D_n^\varepsilon(q)$, где $\varepsilon \in \{+, -\}$ и $A_n^+(q) = A_n(q)$, $A_n^-(q) = {}^2A_n(q)$, $D_n^+(q) = D_n(q)$, $D_n^-(q) = {}^2D_n(q)$.

Пусть $L = L_n(q) = A_{n-1}(q)$, где $n = 2^m \geq 32$, $q = 2^k \geq 2$. Из [4, § 8] следует, что $t(L) \geq 16$ и $t(2, L) = 3$. Кроме того, из п. (2) леммы 4 вытекает, что 2-период группы L равен $n = 2^m$.

Пусть G — конечная группа, удовлетворяющая условию $\omega(G) = \omega(L)$ и K — ее максимальная нормальная разрешимая подгруппа. В силу леммы 1 найдется конечная неабелева простая группа S такая, что $S \leq \overline{G} = G/K \leq \mathrm{Aut}(S)$, причем $t(S) \geq t(G) - 1$ и либо $t(S) = t(2, S) = 3$, либо $t(2, S) \geq t(2, G)$. Так как $t(G) = t(L) \geq 16$ и $t(2, G) = t(2, L) = 3$, то для группы S должно быть выполнено $t(S) \geq 15$ и $t(2, S) \geq 3$. Пользуясь [4, § 8], мы составили таблицу всех конечных неабелевых простых групп, удовлетворяющих этим условиям. Для каждой группы S в таблице указаны значение 2-неплотности и некоторое независимое множество $\rho(2, S)$ в графе $GK(S)$ с наибольшим числом вершин, содержащее вершину 2. Кроме того, для каждой группы лиева типа в таблице приведено значение ее неплотности в зависимости от ее лиева ранга.

Пусть r_n, r_{n-1} и r_{n-2} — это, если не оговорено особо, некоторые фиксированные примитивные простые делители чисел $q^n - 1$, $q^{n-1} - 1$ и $q^{n-2} - 1$ соответственно. По определению примитивного простого делителя эти числа попарно различны. По [4, предложение 3.1] числа r_n и r_{n-1} несмежны с 2 в $GK(L)$, а значит, и в $GK(G)$, следовательно, по лемме 1 эти числа делят порядок группы S.

Пусть $S = \mathrm{Alt}_{n'}$. Тогда $n' \geq 137$ и среди чисел n', $n'-1$, $n'-2$, $n'-3$ есть два простых — это числа r_n и r_{n-1}. Из [7, предложение 7] следует, что $4 \cdot r_{n-2} \notin \omega(L)$, хотя и $2 \cdot r_{n-2} \in \omega(L)$. Предположим, что r_{n-2} делит порядок S. Так как в S не может быть элемента порядка $4 \cdot r_{n-2}$, то $n' \geq r_{n-2} \geq n' - 5$. Таким образом, среди шести последовательных чисел $n', \dots, n'-5$ есть три простых, но

Таблица 1. Простые группы S с $t(S) \geq 15$ и $t(2,S) \geq 3$

S	Дополнительные условия на S	$t(2,S)$	$\rho(2,S)\setminus\{2\}$	$t(S)$
Alt_n, $n \geq 137$	$n, n-2$ простые	3	$\{n, n-2\}$	
	$n-1, n-3$ простые	3	$\{n-1, n-3\}$	
$A_{n-1}(q)$, $n \geq 29$	$2 < (q-1)_2 = n_2$	3	$\{r_{n-1}, r_n\}$	$\left[\frac{n+1}{2}\right]$
	q четно	3	$\{r_{n-1}, r_n\}$	
${}^2A_{n-1}(q)$, $n \geq 29$	$2 < (q+1)_2 = n_2$	3	$\{r_{2n-2}, r_n\}$	$\left[\frac{n+1}{2}\right]$
	q четно, $n \equiv 0 \pmod 4$	3	$\{r_{2n-2}, r_n\}$	
	$n \equiv 1 \pmod 4$	3	$\{r_{n-1}, r_{2n}\}$	
	$n \equiv 2 \pmod 4$	3	$\{r_{2n-2}, r_{n/2}\}$	
	$n \equiv 3 \pmod 4$	3	$\{r_{(n-1)/2}, r_{2n}\}$	
$B_n(q), n \geq 19$	q четно	3	$\{r_n, r_{2n}\}$	$\left[\frac{3n+5}{4}\right]$
$D_n(q)$, $n \geq 20$	$q \equiv 5 \pmod 8$, $n \equiv 1 \pmod 2$	3	$\{r_n, r_{2n-2}\}$	$\left[\frac{3n+1}{4}\right]$
	q четно, $n \equiv 0 \pmod 2$	3	$\{r_{n-1}, r_{2n-2}\}$	
	$n \equiv 1 \pmod 2$	3	$\{r_n, r_{2n-2}\}$	
${}^2D_n(q)$, $n \geq 19$	$q \equiv 3 \pmod 8$, $n \equiv 1 \pmod 2$	3	$\{r_{2n-2}, r_{2n}\}$	$\left[\frac{3n+4}{4}\right]$
	q четно, $n \equiv 0 \pmod 2$	4	$\{r_{n-1}, r_{2n-2}, r_{2n}\}$	
	$n \equiv 1 \pmod 2$	3	$\{r_{2n-2}, r_{2n}\}$	

это невозможно, так как $n' \geq 137$. Значит, r_{n-2} принадлежит $\pi(K) \cup \pi(\mathrm{Out}(S))$. Так как $\pi(\mathrm{Out}(S)) = \{2\}$, то $r_{n-2} \in \pi(K)$.

Обозначим r_{n-2} через r. Пусть $\widetilde{G} = G/O_{r'}(K)$ и $\widetilde{K} = K/O_{r'}(K)$. Тогда $R = O_r(\widetilde{K}) \neq 1$. Предположим, что $\widetilde{K} = R$. Группа S действует на $\widetilde{K}$ точно, так как иначе она в силу своей простоты централизовала бы $\widetilde{K}$ и, следовательно, в G был бы элемент порядка $4 \cdot r$. В группе Alt_6, а значит, и в S есть подгруппа Фробениуса F с ядром порядка 9 и циклическим дополнением порядка 4. Применяя лемму 3 к прообразу F в $\widetilde{G}$, получаем, что $4 \cdot r \in \omega(G)$; противоречие. Пусть $\widetilde{K} \neq R$. Тогда найдется простое число t такое, что группа $T = O_t(\widetilde{K}/R)$ нетривиальна. Поскольку $O_{r'}(\widetilde{K}) = 1$, группа T действует на R точно. Тогда T действует точно и на $\widehat{R} = R/\Phi(R)$, где $\Phi(R)$ — подгруппа Фраттини группы R. Обозначим через $\widehat{G}$ фактор-группу $\widetilde{G}/\Phi(R)$. По лемме 4 хотя бы одно из чисел r_n и r_{n-1} несмежно с t в $\omega(G)$. Обозначим это число через s. Пусть x — элемент группы $\widehat{G}/\widehat{R}$ порядка s. Тогда $H = T\langle x \rangle$ — подгруппа Фробениуса в $\widehat{G}/\widehat{R}$. Прообраз H в $\widehat{G}$ удовлетворяет условиям леммы 3, поэтому в G существует элемент порядка $r \cdot s$, а это противоречит [4, предложение 2.1].

Пусть $S = A^{\varepsilon}_{n'-1}(q')$, где q' нечетно. Тогда $n'_2 = (q' - \varepsilon 1)_2 > 2$ и $t(S) = n'/2$. Поскольку $t(S) \geq t(G) - 1$ и $t(G) = n/2$, то $n'/2 \geq n/2 - 1$, откуда $n' \geq n - 2$. Так как $n \geq 32$, то $n - 2 \geq n/2 + 2 = 2^{m-1} + 2$, таким образом, $n' \geq 2^{m-1} + 2$. Следовательно, в S есть циклическая подгруппа порядка ${q'}^{2^{m-1}} - 1$. Поскольку

$$
{q'}^{2^{m-1}} - 1 = (q' - 1)(q' + 1)({q'}^2 + 1) \dots ({q'}^{2^{m-2}} + 1),
$$

имеем

$$({q'}^{2^{m-1}}-1)_2=(q'-1)_2(q'+1)_2({q'}^2+1)_2\dots({q'}^{2^{m-2}}+1)_2\geq 4\cdot 2^{m-1}=2^{m+1}.$$

Таким образом, $2^{m+1}\in\omega(S)$; противоречие.

Пусть $S=D^{\varepsilon}_{n'}(q')$, где q' нечетно. Тогда $q'-\varepsilon 1\equiv 4\pmod 8$, $n'\equiv 1\pmod 2$ и $t(S)\leq(3n'+3)/4$. Поскольку $t(S)\geq t(G)-1$ и $t(G)=n/2$, то $(3n'+3)/4\geq n/2-1$, откуда $n'\geq(2n-7)/3$. Так как $n\geq 32$, то $(2n-7)/3\geq n/2+3$, таким образом, $n'\geq n/2+3$. Поскольку $D^{\varepsilon}_{n'}(q')$ содержит универсальную накрывающую группы $A_{n'-2}(q')$, то, повторяя рассуждение предыдущего абзаца, получаем, что $2^{m+1}\in\omega(S)$; противоречие.

Пусть теперь S — группа лиева типа над полем порядка $2^{k'}$. Выберем примитивные простые делители r_n и r_{n-1} чисел q^n-1 и $q^{n-1}-1$ так, чтобы $e(r_n,2)=nk$ и $e(r_{n-1},2)=(n-1)k$. Как уже отмечалось, r_n и r_{n-1} делят порядок группы S. Положим $e_n=e(r_n,2^{k'})$ и $e_{n-1}=e(r_{n-1},2^{k'})$. Так как r_n делит $2^{e_nk'}-1$, то nk делит e_nk'. По тем же соображениям $(n-1)k$ делит $e_{n-1}k'$. Предположим, что $e_nk'>nk$. Тогда простое число r, удовлетворяющее условию $e(r,2)=e_nk'$, делит порядок S и не делит порядок L, следовательно, $r\in\omega(S)\setminus\omega(G)$, что невозможно. Таким образом, $e_nk'=nk$. Предположим, что $e_{n-1}k'>(n-1)k$. Тогда $e_{n-1}k'\geq 2(n-1)k>nk$ и рассуждение, аналогичное предыдущему, приводит к противоречию. Таким образом, $e_{n-1}k'=(n-1)k$. Заметим, что $e_n>e_{n-1}$.

Поскольку r_n и r_{n-1} несмежны с 2 в $GK(S)$, то [4, предложение 3.1] накладывает на e_n и e_{n-1} ограничения, которые и будут использоваться в дальнейшем рассмотрении.

Если $S=A_{n'-1}(2^{k'})$, то $e_n,e_{n-1}\in\{n',n'-1\}$. Поэтому $n'k'=nk$ и $(n'-1)k'=(n-1)k$, откуда $k'=k$, $n'=n$ и $S\simeq L$.

Пусть $S={}^2A_{n'-1}(2^{k'})$. Если $n'\equiv 0\pmod 4$, то $e_n,e_{n-1}\in\{2n'-2,n'\}$. Значит, $2(n'-1)k'=nk$ и $n'k'=(n-1)k$, откуда $2k'=(n-2)k$ и $n'-1=n/(n-2)$. Поскольку $n\geq 32$, то $n/(n-2)$ не может быть целым числом; противоречие. Если $n'\equiv 2\pmod 4$, то $e_n,e_{n-1}\in\{2n'-2,n'/2\}$, следовательно, $2(n'-1)k'=nk$ и $n'k'=2(n-1)k$, откуда $2k'=(3n-4)k$ и $n'-1=n/(3n-4)$. Но $n'=n/(3n-4)+1$ не может быть целым числом. Если $n'\equiv 1\pmod 4$, то $e_n,e_{n-1}\in\{2n',n'-1\}$. Значит, $2n'k'=nk$ и $(n'-1)k'=(n-1)k$, откуда $2k'=(2-n)k$. Поскольку $2-n<0$, то $k'<0$, что невозможно. Если $n'\equiv 3\pmod 4$, то $e_n,e_{n-1}\in\{2n',(n'-1)/2\}$, следовательно, $2n'k'=nk$ и $(n'-1)k'=2(n-1)k$, откуда $2k'=(4-3n)k$ и $k'<0$; противоречие.

Если $S=B_{n'}(2^{k'})$, то $e_n,e_{n-1}\in\{2n',n'\}$. Значит, $2n'k'=nk$ и $n'k'=(n-1)k$, откуда $n=2$; противоречие.

Если $S=D_{n'}(2^{k'})$ и n' четно, то $e_n,e_{n-1}\in\{2n'-2,n'-1\}$. Так же, как в предыдущем случае, получается, что $n=2$. Если же n' нечетно, то $e_n,e_{n-1}\in\{2n'-2,n'\}$, а невозможность такого варианта уже доказана.

Если $S={}^2D_{n'}(2^{k'})$, то $e_n,e_{n-1}\in\{2n',2n'-2,n'\}$. В предыдущих случаях разобраны все варианты, кроме $2n'k'=nk$ и $2(n'-1)k'=(n-1)k$. Из этих равенств следует, что $n'=n$, $k'=k/2$ и $S={}^2D_n(2^{k/2})$. Из [8, предложение 0.5] вытекает, что 2-период группы S равен 2^{m+1} и тем самым превосходит 2-период группы G; противоречие.

Таким образом, $S\simeq L$, и квазираспознаваемость доказана.

Оставшаяся часть доказательства может быть проведена при более слабых условиях на n и q, поэтому она оформлена в виде двух предложений.

Предложение 1. *Пусть $L = A_{n-1}(q)$, где $n = 2^m \geq 4$, $q = 2^k \geq 2$. Пусть G — конечная группа и K — ее нетривиальная нормальная разрешимая подгруппа, удовлетворяющие условию $L \leq G/K \leq \mathrm{Aut}(L)$. Тогда $\omega(G) \not\subseteq \omega(L)$.*

Доказательство. Существует такое простое число r, что $O^r(K) \neq K$. Обозначим через $\widetilde{G}$ и $\widetilde{K}$ фактор-группы $G/O^r(K)$ и $K/O^r(K)$ соответственно. Группа $\widetilde{K}$ является нетривиальной r-группой. Пусть $\Phi(\widetilde{K})$ — ее подгруппа Фраттини. Обозначим через $\widehat{G}$ и $\widehat{K}$ фактор-группы $\widetilde{G}/\Phi(\widetilde{K})$ и $\widetilde{K}/\Phi(\widetilde{K})$ соответственно. Поскольку $G/K \simeq \widehat{G}/\widehat{K}$, достаточно показать, что $\omega(\widehat{G}) \not\subseteq \omega(L)$. Поэтому можно считать, что $G = \widehat{G}$ и $K = \widehat{K}$ — нетривиальная элементарная абелева r-группа.

Предположим, что $C = C_G(K) \neq K$. Поскольку C нормальна в G, а L проста, то C/K содержит L. Следовательно, $r \cdot \omega(L) \subseteq \omega(C) \subseteq \omega(G)$, что противоречит п. (3) леммы 4. Таким образом, $C = K$, и L действует на K точно.

Пусть $r = 2$. По п. (1) леммы 5 в группе L есть подгруппа Фробениуса с ядром нечетного порядка и циклическим дополнением порядка n. Применяя лемму 3, получаем, что $2 \cdot n = 2^{m+1} \in \omega(G)$. Из п. (2) леммы 4 имеем, что 2-период группы L равен 2^m, т. е. $2^{m+1} \notin \omega(L)$.

Пусть $r \neq 2$. По п. (2) леммы 5 в группе L есть подгруппа Фробениуса с ядром порядка q^n и циклическим дополнением порядка $(q^{n-1}-1)/d$. Применяя лемму 3, получаем, что $r \cdot (q^{n-1}-1)/d \in \omega(G)$. С другой стороны, по п. (1) леммы 4 выполнено $r \cdot (q^{n-1}-1)/d \notin \omega(L)$. Предложение доказано.

Предложение 2. *Пусть $L = A_{n-1}(q)$, где $n \geq 10$, $q = 2^k \geq 2$ и $(q-1, n) = 1$. Пусть $L < G \leq \mathrm{Aut}(L)$. Тогда $\omega(G) \not\subseteq \omega(L)$.*

Доказательство. Группа G содержит подгруппу $G_1 = L\langle\alpha\rangle$, где порядок образа α в $\mathrm{Out}(L)$ равен некоторому простому числу r. Достаточно показать, что $\omega(G_1) \not\subseteq \omega(L)$, поэтому можно считать, что $G = G_1$.

Группа $\mathrm{Aut}(L)$ обладает нормальным рядом $L \leq \widetilde{L} \leq \mathrm{Aut}(L)$, где фактор $\widetilde{L}/L$ изоморфен группе полевых автоморфизмов — циклической группе порядка k — и фактор $\mathrm{Aut}(L)/\widetilde{L}$ изоморфен группе графовых изоморфизмов — циклической группе порядка 2.

Пусть $r = 2$. Если $\alpha \notin \widetilde{L}$, то α — это либо графовый автоморфизм, либо произведение графового и инволютивного полевого автоморфизмов. В первом случае $C_L(\alpha) \simeq C_{n/2}(q)$, если n четно, и $C_L(\alpha) \simeq B_{(n-1)/2}(q)$, если n нечетно, и следовательно, $2 \cdot r_n \in \omega(G)$ или $2 \cdot r_{n-1} \in \omega(G)$. Во втором случае $q = q_0^2$, $C_L(\alpha)$ содержит подгруппу, изоморфную ${}^2A_{n-1}(q_0)$, и опять в зависимости от четности n либо $2 \cdot r_{n-1} \in \omega(G)$, либо $2 \cdot r_n \in \omega(G)$. Так как r_n и r_{n-1} несмежны с 2 в $\omega(L)$, то при $\alpha \notin \widetilde{L}$ утверждение справедливо.

Пусть теперь α — инволютивный полевой автоморфизм, индуцированный автоморфизмом φ поля $\mathbb{F}_q$, и пусть u — элемент поля $\mathbb{F}_q$ такой, что $u + u^\varphi \neq 0$. Рассмотрим произведение α и унипотентного элемента x группы L вида $x_1(u)x_2(u)\dots x_{n-1}(u)$, где $x_1, x_2, \dots, x_{n-1}$ — корневые элементы, соответствующие простым корням системы корней A_{n-1}. Элемент

$$(x\alpha)^2 = x_1(u)x_2(u)\dots x_{n-1}(u)x_1(u^\varphi)x_2(u^\varphi)\dots x_{n-1}(u^\varphi)$$

лежит в группе L и в силу коммутаторной формулы Шевалле [12, теорема 5.2.2] может быть преобразован к виду $x_1(u + u^\varphi)\dots x_{n-1}(u + u^\varphi)y$, где y — произведение корневых элементов, соответствующих непростым положительным корням. Так как $u + u^{\varphi} \neq 0$, то по [9, предложение 5.1.3] элемент $(x\alpha)^2$ является регулярным и, следовательно, имеет порядок, равный 2-периоду группы L (см. доказательство следствия 0.5 из [8]). Таким образом, порядок $x\alpha$ в два раза больше 2-периода группы L, и, значит, $\omega(G) \nsubseteq \omega(L)$.

Пусть $r \neq 2$. Тогда α — полевой автоморфизм и $C_L(\alpha) \simeq A_{n-1}(q_0)$, где $q_0 = 2^{k/r}$. Положим $s = e(r, q)$. Напомним, что s — это наименьшее число такое, что $q^s - 1$ делится на r. Если $s > n$, то $r \in \omega(G) \setminus \omega(L)$; если $s = n, n-1$, то $2r \in \omega(G) \setminus \omega(L)$, поэтому можно считать, что $1 \leq s \leq n-2$. Прежде чем приступить к дальнейшему разбору случаев в зависимости от s, заметим, что если $e(p, q_0)$ равно t и $(t, r) = 1$, то $e\big(p, q_0^r\big)$ также равно t. Другими словами, если $t \neq 6$ и $(t, r) = 1$, то найдется примитивный простой делитель числа $q^t - 1$, который будет делить число $q_0^t - 1$.

Пусть $s = 1$, т. е. $r \mid q - 1$. По условию предложения $(n, r) = 1$, следовательно, существует примитивный простой делитель r_n числа $q^n - 1$, являющийся делителем $q_0^n - 1$. Из [4, предложение 4.1] следует, что $r \cdot r_n \notin \omega(L)$. С другой стороны, $r \cdot r_n \in r \cdot \omega(A_{n-1}(q_0)) \subseteq \omega(G)$.

Пусть $2 \leq s \leq n - 2$. Среди чисел $n, n-1, \dots, n-s+1$ есть только одно число, делящееся на s. Среди оставшихся $s - 1$ чисел можно выбрать число t, которое взаимно просто с r и не равно 6, за исключением случая, когда $s = 2$ и $r \mid n - 1$. Мы рассмотрим этот случай позже, а пока будем считать, что такое t выбрано. Поскольку $(t, r) = 1$, существует примитивный простой делитель r_t числа $q^t - 1$, делящий $q_0^t - 1$. Так как $t + s > n$ и $s \nmid t$, то по [4, предложение 2.1] выполнено $r \cdot r_t \notin \omega(L)$. С другой стороны, $r \cdot r_t \in r \cdot \omega(A_{n-1}(q_0)) \subseteq \omega(G)$.

Пусть $s = 2$ и $r \mid n - 1$. Из [13, предложение 4.3] следует, что если C — централизатор инволюции в L, то $\omega(C) \subseteq \omega(SL_{n-2}(q))$. Пусть n четно. Тогда так как $(n - 3, r) = 1$ и $2 \nmid n - 3$, то, повторяя рассуждения предыдущего абзаца, можно найти простой делитель r_{n-3} числа $q_0^{n-3} - 1$ такой, что $r_{n-3} \cdot r \notin \omega(A_{n-3}(q))$. Поскольку порядок центра группы $SL_{n-2}(q)$ взаимно прост и с r_{n-3}, и с r, выполняется $r_{n-3} \cdot r \notin \omega(SL_{n-2}(q))$. Таким образом, $2 \cdot r_{n-3} \cdot r \notin \omega(L)$. С другой стороны, $2 \cdot r_{n-3} \in \omega(A_1(q_0) \times A_{n-3}(q_0)) \subseteq \omega(A_{n-1}(q_0))$, следовательно, $2 \cdot r_{n-3} \cdot r \in \omega(G)$. Пусть n нечетно. Тогда аналогичным образом можно найти простой делитель r_{n-2} числа $q_0^{n-2} - 1$ такой, что $2 \cdot r_{n-2} \cdot r \notin \omega(L)$ и $2 \cdot r_{n-2} \cdot r \in \omega(G)$. Предложение доказано.

Вернемся к доказательству теоремы. В силу предложения 1 разрешимый радикал K группы G тривиален. Если G не изоморфна L, то по предложению 2 имеем $\omega(G) \nsubseteq \omega(L)$. Полученное противоречие завершает доказательство теоремы.

ЛИТЕРАТУРА

1. *Mazurov V. D.* Characterizations of groups by arithmetic properties // Algebra Colloq. 2004. V. 11, N 1. P. 129–140.
2. *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.
3. *Алексеева О. А., Кондратьев А. С.* О распознаваемости групп $E_8(q)$ по множеству порядков элементов // Укр. мат. журн. 2002. Т. 54, № 7. С. 998–1003.
4. *Васильев А. В., Вдовин Е. П.* Критерий смежности двух вершин в графе простых чисел конечной простой группы. Новосибирск, 2005. (Препринт/РАН. Сиб. отд-ние. Ин-т математики; № 152).
5. *Zsigmondy K.* Zur Theorie der Potenzreste // Monatsh. Math. Phys. 1892. Bd 3. S. 265–284.
6. *Мазуров В. Д.* Характеризация конечных групп множествами порядков их элементов // Алгебра и логика. 1997. Т. 36, № 1. С. 37–53.

7. *Carter R. W.* Centralizers of semisimple elements in the finite classical group // Proc. London Math. Soc. (3). 1981. V. 42, N 1. P. 1–41.
8. *Testerman D. M.* A_1-type overgroups of elements of order p in semisimple algebraic groups and the associated finite groups // J. Algebra. 1995. V. 177. P. 34–76.
9. *Carter R. W.* Finite groups of Lie type: Conjugacy classes and complex characters. New York: John Wiley & Sons, 1985.
10. *Steinberg R.* Endomorphisms of algebraic groups. Providence RI: Amer. Math. Soc., 1986. (Mem. Amer. Math. Soc.; 80)
11. *Заварницин А. В.* Порядки элементов в накрытиях групп $L_n(q)$ и распознаваемость знакопеременной группы A_{16}. Новосибирск, 2000. (Препринт/НИИДМИ; № 48).
12. *Carter R. W.* Simple groups of Lie type. London: John Wiley & Sons, 1972.
13. *Aschbacher M., Seitz G. M.* Involutions in Chevalley groups over fields of even order // Nagoya Math. J. 1976. V. 63. P. 1–91.

Статья поступила 20 марта 2005 г.

Васильев Андрей Викторович
Институт математики им. С. Л. Соболева СО РАН,
пр. Академика Коптюга, 4, Новосибирск 630090
vdr@gorodok.net

Гречкосеева Мария Александровна
Новосибирский гос. университет, механико-математический факультет,
ул. Пирогова, 2, Новосибирск 630090
grechkoseeva@gorodok.net