

О распознаваемости линейных и унитарных групп по спектру

Исследование выполнено за счет гранта Российского научного фонда № 23-41-10003,
<https://rscf.ru/project/23-41-10003/>.

А. М. Старолетов

Старолетов Алексей Михайлович (ORCID 0000-0002-3914-6758),
Институт математики им. С.Л. Соболева, Новосибирск, Россия

staroletov@math.nsc.ru

Аннотация

Конечные группы называются изоспектральными, если они имеют одинаковые множества порядков элементов. В данной статье мы завершаем описание конечных групп, изоспектральных простым группам $PSL_n(q)$ или $PSU_n(q)$, где $n \geq 11$. Мы также получаем существенное ограничение на структуру конечных групп, изоспектральных ортогональным и симплектическим группам.

ключевые слова: порядок элемента, простая классическая группа, распознавание по спектру

1 Введение

В данной работе рассматриваются только конечные группы. Множество порядков элементов группы G обозначается через $\omega(G)$ и называется ее *спектром*. Группы называются *изоспектральными*, если они имеют одинаковые спектры. Обозначим через $h(G)$ наибольшее число попарно неизоморфных групп, изоспектральных группе G . Если $h(G) = 1$, то G однозначно (с точностью до изоморфизма) задается своим спектром в классе всех конечных групп, и поэтому G называется *распознаваемой* по спектру. Говорят, что G *почти распознаваема*, если $h(G)$ конечно, и *нераспознаваема*, если $h(G) = \infty$. Будем говорить, что *проблема распознаваемости (по спектру) решена* для G , если число $h(G)$ известно, и в случае $h(G) < \infty$ все группы, изоспектральные G , явно описаны.

В силу [1, лемма 1], если G имеет нетривиальную нормальную разрешимую подгруппу, то $h(G) = \infty$, поэтому проблема распознаваемости по спектру представляет интерес только для групп с тривиальным разрешимым радикалом. Большинство работ по данной проблеме посвящены простым неабелевым группам, однако есть различные примеры, когда проблема решена для групп с непрым цоклем. Подробный обзор результатов и список открытых вопросов можно найти в [2].

Мы обозначаем простые классические группы согласно [3]. В настоящее время проблема распознаваемости по спектру решена для всех простых неабелевых групп, кроме следующих классических групп, определенных над полем нечетного порядка q :

- (а) $L_n(q)$, где $8 \leq n \leq 26$, n не является простым числом;
- (б) $U_n(q)$, где $8 \leq n \leq 26$, n не является простым числом;
- (в) $S_{2n}(q)$ и $O_{2n+1}(q)$, где $5 \leq n \leq 15$, $n \neq 8$;
- (г) $O_{2n}^+(q)$, где $5 \leq n \leq 18$;

(д) $O_{2n}^-(q)$, где $5 \leq n \leq 17$, $n \neq 8, 16$.

Более точные формулировки и необходимые ссылки для групп, отличных от $U_6(q)$, $L_6(q)$ и $U_n(q)$, где n – простое число, могут быть найдены в [2, теорема 2.1]. Группы $U_5(q)$, $U_6(q)$ и $L_6(q)$ были рассмотрены в [4]. Решение проблемы распознаваемости для групп $U_n(q)$, где n – простое число, было недавно завершено в [5]. Эти два результата появились после публикации обзора [2].

Удобным инструментом для изучения проблемы распознаваемости является *граф простых чисел* (или *граф Грюнберга–Кегеля*). Граф простых чисел группы G определяется следующим образом: его вершины являются простыми делителями порядка группы G , и две различные вершины r и s смежны тогда и только тогда, когда $rs \in \omega(G)$. Напомним, что подмножество вершин графа называется *кликкой*, если любые две вершины этого подмножества не смежны. Обозначим через $t(G)$ наибольший размер клички в графе простых чисел группы G . Верхние границы размерностей групп в списке выше можно объяснить следующим образом. Основываясь на предыдущих результатах, А.В. Васильев и М.А. Гречкосеева доказали, что простая классическая группа L почти распознаваема, если $t(L) \geq 23$ [6, 7]. Позднее этот результат был распространен на классические группы L с $14 \leq t(L) < 23$ [8]. Переписывая условие $t(L) \leq 13$ в терминах размерности группы L , мы в точности получаем верхние границы на n из списка выше, за исключением того, что в пункте в) отсутствуют группы $S_{32}(q)$ и $O_{33}(q)$. Для этих групп проблема распознаваемости была ранее решена в [9–11].

Мы понижаем верхнюю границу размерностей для линейных и унитарных групп L , рассматривая случаи, когда $6 \leq t(L) \leq 13$.

Теорема 1. Предположим, что L – одна из простых групп $L_n(q)$ или $U_n(q)$, где $n \geq 11$. Тогда проблема распознаваемости по спектру для L решена. Более того, $L \leq G \leq \text{Aut } L$ для любой конечной группы G , изоспектральной L .

Как следствие получаем, что проблема распознаваемости для линейных и унитарных групп размерности n в настоящее время не решена только для $n = 8, 9, 10$.

На самом деле теорема 1 является следствием ряда предыдущих результатов и следующей теоремы, доказательство которой является основной целью данной статьи.

Теорема 2. Предположим, что L – одна из простых групп $L_n(q)$ или $U_n(q)$, где q нечетно и $12 \leq n \leq 26$. Если G – конечная группа, изоспектральная L , и S – неабелев композиционный фактор группы G , то S не изоморфна классической группе над полем характеристики, взаимно простой с q .

Ряд рассуждений из доказательства теоремы 2 не использует по существу то, что L является линейной или унитарной, и, как следствие, может быть проведен для классической группы L любого типа. Результат этих рассуждений выделен в отдельную теорему.

Теорема 3. Предположим, что L – простая классическая группа над полем нечетного порядка q такая, что $5 \leq t(L) \leq 13$. Предположим, что G – конечная группа, изоспектральная L , и G имеет неабелев композиционный фактор S такой, что S – классическая группа над полем характеристики, взаимно простой с q . Тогда справедливы следующие утверждения.

(а) Если L – линейная или унитарная группа с $t(L) \geq 6$, то $t(S) = t(L)$.

(б) Если L – линейная или унитарная группа с $t(L) = 5$ или ортогональная или симплектическая группа с $t(L) \geq 7$, то $0 \leq t(S) - t(L) \leq 1$.

(в) Если L – симплектическая или ортогональная группа с $5 \leq t(L) \leq 6$, то $0 \leq t(S) - t(L) \leq 2$.

Данная статья организована следующим образом. Раздел 2 посвящен определениям и вспомогательным арифметическим результатам, которые являются полезными при работе со спектром классических групп. В разделе 3 перечислены необходимые факты о спектрах и графах простых чисел классических групп. Теорема 3 доказывается в разделе 4, а разделы 5 и 6 посвящены доказательствам теорем 2 и 1 соответственно.

2 Предварительные данные: арифметические результаты

Наибольший общий делитель целых чисел a и b обозначается через (a, b) . Зафиксируем целое число a с $|a| > 1$ и простое число r .

Через $\pi(a)$ обозначается множество всех простых делителей числа a . Через $a_{\{r\}}$ обозначается r -часть числа a , т.е. наибольшая степень числа r , делящая a . Если π – множество простых чисел, то определим $a_\pi = \prod_{r \in \pi} a_{\{r\}}$ и $a_{\pi'} = a/a_\pi$. В этом случае числа a_π и $a_{\pi'}$ называются π -частью и π' -частью числа a соответственно.

Если r нечетно и $(a, r) = 1$, то $e(r, a)$ обозначает мультипликативный порядок a по модулю r . Положим $e(2, a) = 1$, если 4 делит $a - 1$, и $e(2, a) = 2$, если 4 делит $a + 1$. Простое число r называется *примитивным простым делителем* числа $a^i - 1$, если $e(r, a) = i$. Обозначим через $r_i(a)$ некоторый примитивный простой делитель числа $a^i - 1$, если хотя бы один такой делитель существует, через $R_i(a)$ – множество всех таких делителей. Существование примитивных простых делителей для почти всех пар (a, i) было доказано Бэнгом [12] и Жигмонди [13].

Лемма 2.1 (Бэнг–Жигмонди). Пусть a – целое число и $|a| > 1$. Если i – натуральное число и $(a, i) \notin \{(2, 1), (2, 6), (-2, 2), (-2, 3), (3, 1), (-3, 2)\}$, то множество $R_i(a)$ непусто.

Для числа $i \neq 2$ произведение всех примитивных простых делителей числа $a^i - 1$, взятых с учетом кратности, обозначается через $k_i(a)$. Положим $k_2(a) = k_1(-a)$. Число $k_i(a)$ называется *наибольшим примитивным делителем* числа $a^i - 1$. Из определения следует, что $(k_i(a), k_j(a)) = 1$, если $i \neq j$. Легко проверить, что $k_1(a) = |a - 1|$, если $a \not\equiv 3 \pmod{4}$, и $k_1(a) = |a - 1|/2$, если $a \equiv 3 \pmod{4}$, а также $k_2(a) = |a + 1|$, если $a \not\equiv 1 \pmod{4}$, и $k_2(a) = |a + 1|/2$, если $a \equiv 1 \pmod{4}$. Из [14] следует, что при $i > 2$

$$k_i(a) = \frac{|\Phi_i(a)|}{(r, \Phi_{i_{\{r\}'}}(a))}, \quad (1)$$

где $\Phi_i(x)$ – i -й круговой многочлен, а r – наибольшее простое число, делящее i ; более того, если $i_{\{r\}'}$ не делит $r - 1$, то $(r, \Phi_{i_{\{r\}'}}(a)) = 1$. Для любого целого числа n , отличного от нуля, через $\varphi(n)$ обозначается значение функции Эйлера на n . Напомним, что $\deg \Phi_n(x) = \varphi(n)$. Из определения наибольших примитивных делителей и равенства (1) вытекает следующее полезное утверждение.

Лемма 2.2. Пусть a и i – целые числа такие, что $|a| > 1$ и $i \geq 1$. Если i нечетно, то $k_i(-a) = k_{2i}(a)$, и если i кратно 4, то $k_i(-a) = k_i(a)$.

Лемма 2.3. ([6, лемма 1.5]). Пусть a и i – целые числа, $\varepsilon \in \{+, -\}$. Если $a \geq 2$, $i \geq 3$ и $(a, i) \notin \{(2, 3), (2, 6)\}$, то $k_i(\varepsilon a) > a^{\varphi(i)/2}$.

Лемма 2.4. Справедливы следующие утверждения.

- (а) Если p – простое число, то $\Phi_{pm}(x) = \begin{cases} \Phi_n(x^p), & \text{если } (n, p) = p; \\ \Phi_n(x^p)/\Phi_n(x), & \text{если } (n, p) = 1. \end{cases}$

(б) Если $n < 105$, то все коэффициенты многочлена $\Phi_n(x)$ принадлежат множеству $\{-1, 0, 1\}$.

(в) Если $3 \leq n < 105$, то $\Phi_n(a) > 0$ для всех действительных чисел a с $|a| \geq 2$.

(г) Предположим, что унитарный многочлен $f(x) \in \mathbb{Z}[x]$ имеет степень $n \geq 1$ и все его коэффициенты принадлежат множеству $\{-1, 0, 1\}$. Если $a \geq k > 1$, где k – действительное число, то $\frac{k-2}{k-1}a^n < f(a) < \frac{k}{k-1}a^n$.

Доказательство. Пункт (а) хорошо известен и упоминается, например, в [15]. Пункт (б) – это [16, теорема 13.5]. Чтобы доказать (в), заметим, что если $n \geq 3$, то $\varphi(n)$ чётно. Из (б) следует, что если $3 \leq n < 105$ и $|a| \geq 2$, то

$$\Phi_n(a) \geq |a|^{\varphi(n)} - |a|^{\varphi(n)-1} - \dots - |a| - 1 = |a|^{\varphi(n)} - \frac{|a|^{\varphi(n)} - 1}{|a| - 1} = \frac{|a|^{\varphi(n)+1} - 2|a|^{\varphi(n)} + 1}{|a| - 1} > 0.$$

Теперь докажем (г). По предположению получаем, что $f(a) \leq 1 + a + \dots + a^n = \frac{a^{n+1}-1}{a-1}$, поэтому для доказательства верхней оценки достаточно проверить, что $\frac{a^{n+1}-1}{a-1} < \frac{k}{k-1}a^n$. Последнее неравенство эквивалентно неравенству $a^{n+1} + k - 1 > ka^n$, которое является верным, поскольку $a \geq k$. Аналогично получаем, что $f(a) \geq a^n - a^{n-1} - \dots - 1 = 2a^n - a^n - a^{n-1} - \dots - 1 = 2a^n - \frac{a^{n+1}-1}{a-1}$. Мы знаем, что $-\frac{a^{n+1}-1}{a-1} > -\frac{k}{k-1}a^n$. Поэтому $f(a) > 2a^n - \frac{k}{k-1}a^n = \frac{k-2}{k-1}a^n$, что и требовалось показать. \square

В качестве следствия из пункта (в) этой леммы получаем, что в равенстве (1) для $k_i(a)$ модуль в числителе можно убрать, если $3 \leq i < 105$.

Лемма 2.5. [6, лемма 1.7] Пусть q и m – целые числа, большие 1, и $\varepsilon \in \{+, -\}$.

(а) Если нечётное простое число r делит $\varepsilon q - 1$, то $((\varepsilon q)^m - 1)_{\{r\}} = m_{\{r\}}(\varepsilon q - 1)_{\{r\}}$.

(б) Если нечётное простое число r делит $(\varepsilon q)^m - 1$, то r делит $(\varepsilon q)^{m_{\{r\}'}} - 1$.

(в) Если $\varepsilon q - 1$ делится на 4, то $((\varepsilon q)^m - 1)_{\{2\}} = m_{\{2\}}(\varepsilon q - 1)_{\{2\}}$.

Лемма 2.6. Пусть q – степень нечётного простого числа. Если $\varepsilon \in \{+, -\}$ и $r \geq 7$ – простое число, то $k_r(\varepsilon q) > \frac{5}{3}q^{r-2}$.

Доказательство. Используя равенство (1), находим, что $k_r(\varepsilon q) = \frac{q^r - \varepsilon 1}{(q - \varepsilon 1, r)(q - \varepsilon 1)} \geq \frac{q^r + 1}{(q - \varepsilon 1, r)(q + 1)}$. Если $(q - \varepsilon 1, r) = 1$, то $k_r(\varepsilon q) \geq \frac{q^r + 1}{q + 1} > \frac{5}{3}q^{r-2}$, так как $q \geq 3$. Предположим, что $(q - \varepsilon 1, r) = r$. Тогда $q - \varepsilon 1$ делится на r , поэтому $q + 1 \geq 2r$. Теперь $\frac{q^r + 1}{(q + 1)r} > \frac{5}{3}q^{r-2}$ тогда и только тогда, когда $3q^r + 3 > 5rq^{r-1} + 5rq^{r-2}$. Поскольку $q \geq 2r - 1$ и $r \geq 7$, получаем, что $3q^r + 3 \geq (6r - 3)q^{r-1} + 3 \geq (5r + 4)q^{r-1} + 3$. Далее $(5r + 4)q^{r-1} + 3 = 5rq^{r-1} + 4q^{r-1} + 3 \geq 5rq^{r-1} + (8r - 4)q^{r-2} + 3$. Наконец, находим, что $5rq^{r-1} + (8r - 4)q^{r-2} + 3 > 5rq^{r-1} + 5rq^{r-2}$ и, следовательно, $3q^r + 3 > 5rq^{r-1} + 5rq^{r-2}$, что и требовалось показать. \square

Лемма 2.7. Пусть q – степень нечётного простого числа и $\varepsilon \in \{+, -\}$. Тогда $k_9(\varepsilon q) > q^{5.5}$ или $k_7(\varepsilon q) > q^{5.5}$.

Доказательство. Предположим, что $q \geq 13$. Тогда $q^{0.5} > 3.5$. Используя равенство (1), находим, что

$$k_9(\varepsilon q) \geq (q^6 - q^3 + 1)/3 > (3.5q^{5.5} - q^3)/3 > q^{5.5} + (0.5q^{5.5} - q^3) > q^{5.5}.$$

Предположим, что $q < 13$. Тогда $(q - \varepsilon 1, 7) = 1$, поэтому

$$k_7(\varepsilon q) = \Phi_7(\varepsilon q) \geq q^6 - q^5 + q^4 - q^3 + q^2 - q + 1 > q^6 - q^5.$$

Легко видеть, что $q^6 - q^5 > q^{5.5}$, если $q \geq 3$ и, значит, $k_7(\varepsilon q) > q^{5.5}$ в этом случае. \square

Лемма 2.8. Пусть q и w – степени простых чисел, при этом $q \neq w$ и q нечетно. Если $k_7(\varepsilon q)$ делит $k_7(\tau w)$, где $\varepsilon, \tau \in \{+, -\}$ и $(q - \varepsilon 1, 7) = 1$, то $5q^6 < w^6$.

Доказательство. Предположим, что $k_7(\varepsilon q) = k_7(\tau w)$. Если $(w - \tau 1, 7) = 1$, то $\Phi_7(\varepsilon q) = \Phi_7(\tau w)$ в силу равенства (1). Легко видеть, что если $a > 0$, то $\Phi_7(\varepsilon(a + 1)) - \Phi_7(\varepsilon a) > 0$ и $\Phi_7(\tau(a + 1)) - \Phi_7(\tau a) > 0$. Поскольку $w \neq q$, верно, что $w \geq q + 1$ или $q \geq w + 1$. В первом случае получаем, что $\Phi_7(\tau w) \geq \Phi_7(\tau(q + 1)) > q^6 + q^5 + q^4 + q^3 + q^2 + q + 1 \geq \Phi_7(\varepsilon q)$, а во втором случае получаем, что $\Phi_7(\varepsilon q) \geq \Phi_7(\varepsilon(w + 1)) > w^6 + w^5 + w^4 + w^3 + w^2 + w + 1 \geq \Phi_7(\tau w)$; противоречие с $\Phi_7(\varepsilon q) = \Phi_7(\tau w)$. Поэтому можно считать, что $(w - \tau 1, 7) = 7$ и, следовательно, $w \geq 8$. Заметим, что $k_7(\varepsilon q) \leq \frac{3}{2}q^6$ по лемме 2.4(г), и $k_7(\tau w) \geq \frac{1}{7}(w^6 - w^5 + w^4 - w^3 + w^2 - w + 1) > \frac{1}{8}w^6$, поскольку $w \geq 8$. Значит, $q^6 \geq \frac{12}{12}w^6$ и поэтому $q \geq 7$. Теперь $\frac{6}{7}q^6 < 1 - q + q^2 - q^3 + q^4 - q^5 + q^6 \leq k_7(\varepsilon q) = k_7(\tau w)$, в то время как $k_7(\tau w) < \frac{8}{49}w^6$ по лемме 2.4(г). Следовательно, $5q^6 < w^6$, что и требовалось доказать.

Предположим, что $k_7(\varepsilon q)$ – собственный делитель $k_7(\tau w)$. Поскольку любое число из $R_7(\tau w)$ не меньше 29, заключаем, что $29k_7(\varepsilon q) \leq k_7(\tau w)$. Следовательно, по лемме 2.4(г) получаем, что $29\frac{1}{2}q^6 < 2w^6$. Это влечет требуемое неравенство $5q^6 < w^6$. \square

Лемма 2.9. Предположим, что u – степень простого числа v и q – степень нечетного простого числа p . Пусть j – целое число такое, что $\varphi(j) \geq 4$. Тогда выполнены следующие утверждения.

(а) Если $k_j(u)$ делит $(q^2 - 1)$ и $(j, u) \neq (10, 4)$, то $k_j(u) > u^3$.

(б) Если $k_j(u)$ делит $(q^2 - 1) \log_v u$, и $(k_j(u), \log_v u) > 1$, то $k_j(u) > u^3 \log_v u$.

(в) Если $k_j(u)$ делит $p(q^2 - 1)$, где $p < 31$, $p \in R_j(u)$, и $(j, u) \neq (10, 4)$, то $k_j(u) > \frac{p}{12}u^3$.

(г) Если $k_j(u)$ делит $p(q^2 - 1) \log_v u$, и p делит $(k_j(u), \log_v u)$, то $k_j(u) > pu^3 \log_v u$.

(д) Если $k_j(u)$ делит $p(q^2 - 1) \log_v u$, $p < 31$, и $(k_j(u), \log_v u) > 1$, то $k_j(u) > pu^3 \log_v u$.

Более того, во всех пунктах верно неравенство $2u^3 < q^2$, даже если $(j, u) = (10, 4)$.

Доказательство. Сначала предположим, что $\varphi(j) \geq 6$. Покажем, что $k_j(u) > u^4$. Это верно, если $\varphi(j) \geq 8$ по лемме 2.3. Предположим, что $\varphi(j) = 6$. Тогда $j \in \{7, 14, 9, 18\}$. Если $j = 9$ или $j = 18$, то $k_j(u) \geq \frac{u^6 - u^3 + 1}{3}$ в силу равенства (1). Следовательно, в этом случае $k_j(u) > u^4$. Более того, видим, что $k_7(u) = \frac{u^7 - 1}{(u - 1, 7)(u - 1)} \geq \frac{u^7 - 1}{(u - 1)^2} > u^4$ и $k_{14}(2) = 43 > 2^4$, в то время как для $u > 2$ верно, что $k_{14}(u) > \frac{u^7 + 1}{(u + 1)^2} > u^4$. Поскольку $u > \log_v u$, получаем, что $k_j(u) > u^4 > u^3 \log_v u$. Предположим, что $p \in R_j(u)$ и $p < 31$. Заметим, что $u^4 > \frac{p}{12}u^3$, если $u \geq 3$ или $p \leq 23$. С другой стороны, если $u = 2$ и $23 < p < 31$, то $R_7(2) = \{127\}$, $R_{14}(2) = \{43\}$, $R_9(2) = \{19\}$, $R_{18}(2) = \{73\}$, так что этот случай невозможен. Осталось доказать пункты (г) и (д) в этом случае. Предположим, что r – простое число такое, что r делит $k_j(u)$ и $\log_v(u)$. Поскольку $\varphi(j) \geq 6$, по малой теореме Ферма получаем, что $r \geq 17$. Обозначим $k = \log_v u$. Поскольку $k \geq 17$, верно, что $2^k > k^2$ и $2^k > 31k$. Это означает, что $u = v^k > k^2$ и $u > 31k$. Следовательно, $k_j(u) > u^4 > u^3 \cdot (\log_v u)^2$ и $k_j(u) > u^4 > 31u^3 \log_v u$. Эти неравенства завершают доказательство для всех чисел j с $\varphi(j) \geq 6$.

Предположим, что $\varphi(j) = 4$. Тогда $j \in \{5, 8, 12, 10\}$. Сначала покажем, что $k_j(u) > u^3$, если $(j, u) \neq (10, 4)$. Используя равенство (1), видим, что $k_{12}(u) = \Phi_{12}(u) = u^4 - u^2 + 1$ и $k_8(u) = \frac{\Phi_8(u)}{(u - 1, 2)} = \frac{u^4 + 1}{(u - 1, 2)}$. Следовательно, если $j = 12$, то $k_j(u) \geq 2u^3 - u^2 + 1 > u^3$, а если $j = 8$, то $k_j(u) \geq (u^4 + 1)/2 > u^3$. Предположим, что $j = 5, 10$. Заметим, что $k_j(u) > u^3$ при $u = 2, 3$ и $k_5(4) = 341 > 4^3$. Таким образом, можно считать, что $u \geq 5$.

Используя равенство (1), получаем, что $k_j(u) \geq \frac{1}{d}(u^4 - u^3 + u^2 - u + 1)$, где либо $d = 1$, либо $d = 5$ и $u \geq 9$. Если $d = 1$, то $u^4 - u^3 + u^2 - u + 1 \geq 2u^3 - u^3 + u^2 - u + 1 > u^3$. Если $d = 5$, то $k_j(u) \geq \frac{1}{5}(9u^3 - u^3 + u^2 - u + 1) > u^3$. Следовательно, мы доказали требуемое неравенство $k_j(u) > u^3$ во всех случаях.

Предположим, что $p \in R_j(u)$, и $k_j(u)$ делит $p(q^2 - 1)$, где $p < 31$ и $(j, u) \neq (10, 4)$. Покажем, что $k_j(u) > \frac{p}{12}u^3$. Мы знаем, что $k_j(u) > u^3$, поэтому можно считать, что $p > 12$. Поскольку $p < 31$ и $p \in R_j(u)$ с $j \in \{5, 8, 10, 12\}$, получаем, что $p - 1$ делится на j , и, следовательно, $(p, j) \in \{(13, 12), (17, 8)\}$. Если $j = 12$, то $k_{12}(2) = 13 > \frac{13}{12}2^3$, а для $u > 2$ верно, что $k_{12}(u) = u^4 - u^2 + 1 > 3u^3 - u^2 > 2u^3 > \frac{13}{12}u^3$. Если $j = 8$, то $k_8(2) = 17 > \frac{17}{12}2^3$, а для $u > 2$ верно, что $k_8(u) \geq (u^4 + 1)/2 > \frac{3}{2}u^3 > \frac{17}{12}u^3$.

Предположим, что $(k_j(u), \log_v u) > 1$, и возьмем простое число r , которое делит оба числа $k_j(u)$ и $\log_v u$. По малой теореме Ферма получаем, что $r \geq 11$, и поэтому $u \geq 2^{11}$. Используя равенство (1), находим, что $k_j(u) \geq \frac{u^4 - u^3 + u^2 - u + 1}{5}$. По лемме 2.4(г) получаем, что $k_j(u) > \frac{u-2}{5(u-1)}u^4 > \frac{1}{6}u^4$. Обозначим $k = \log_v u$. Поскольку $k \geq 11$, верно, что $u \geq 2^k > 6k^2$ и $u \geq 2^k > 6 \cdot 31 \cdot k$. Это означает, что $k_j(u) > u^3(\log_v u)^2$ и $k_j(u) > 31u^3 \log_v u$.

Теперь покажем, что $2u^3 < q^2$ во всех случаях. Поскольку $\varphi(j) \geq 4$, получаем, что $(k_j(u), 6) = 1$. С другой стороны, ясно, что $q^2 - 1$ делится на 8, а $p(q^2 - 1)$ делится на 24. Если $(j, u) = (10, 4)$, то $k_j(u) = 41$ и $\log_v u = 2$. Таким образом, если $k_{10}(4)$ делит $p(q^2 - 1)$, то $q \geq 40$ и, очевидно, $2u^3 < q^2$. Если $(j, u) \neq (10, 4)$, то неравенство $2u^3 < q^2$ следует из доказанных неравенств для $k_j(u)$ и того, что 8 делит $q^2 - 1$, а 24 делит $p(q^2 - 1)$. \square

Лемма 2.10. Предположим, что u – степень простого числа v и q – степень нечетного простого числа p . Предположим, что j_1, \dots, j_k – различные натуральные числа такие, что $\varphi(j_i) \geq 4$ для всех $1 \leq i \leq k$. Если $\prod_{i=1}^k k_{j_i}(u)$ делит $p(q^2 - 1) \log_v u$, где либо каждый множитель $k_{j_i}(u)$ взаимно прост с p , либо p делит $\log_v u$, либо $p < 31$, то $u^{3k} < q^2$.

Доказательство. Сначала будем считать, что $(p, k_{j_i}(u)) = 1$ для всех $1 \leq i \leq k$. Заметим, что если $1 \leq i \leq k$, то $(k_{j_i}(u), 6) = 1$. С другой стороны, видно, что $q^2 - 1$ делится на 8. Поскольку $k_{10}(4) = 41 > 4^3/2$ и $8 \cdot \prod_{i=1}^k k_{j_i}(u)$ делит $(q^2 - 1) \log_v u$, получаем, что $u^{3k} < q^2 - 1$ по лемме 2.9(а),(б).

Предположим, что существует число $j \in \{j_1, \dots, j_k\}$ такое, что p делит $k_j(u)$ и $p < 31$. Можно считать, что $j = j_1$. Поскольку $k_{10}(4) = 41$ и $p < 31$, получаем, что $(j, u) \neq (10, 4)$. По лемме 2.9(в) верно неравенство $k_j(u) > \frac{p}{12}u^3$. Заметим, что $p(q^2 - 1)$ делится на 24.

Поэтому достаточно доказать, что $\prod_{i=2}^k k_{j_i}(u) > \frac{1}{2}u^{3k-3}$, если каждое число $k_{j_i}(u)$ взаимно просто с $\log_v(u)$ или $\prod_{i=2}^k k_{j_i}(u) > \frac{1}{2}u^{3k-3} \log_v u$, если хотя бы одно $k_{j_i}(u)$ не взаимно просто с $\log_v(u)$. Это верно в силу леммы 2.9(а),(б) и неравенства $k_{10}(4) = 41 > 4^3/2$.

Предположим, что существует число $j \in \{j_1, \dots, j_k\}$ такое, что p делит $(\log_v u, k_j(u))$. Лемма 2.9(г) влечет, что $k_j(u) > pu^3 \log_v u$, и произведение оставшихся чисел $k_{j_i}(u)$ не меньше $u^{3k-3}/2$. Теперь утверждение следует из того, что 8 делит $q^2 - 1$. \square

Лемма 2.11.[17, 18] Предположим, что x, y и k – ненулевые целые числа. Если $x^2 + x + 1 = y^k$, то либо $k = 1$, либо $k = 3$ и $(x, y) \in \{(18, 7), (-19, 7)\}$. Если $x^2 + x + 1 = 3y^k$, то $k \leq 2$.

Лемма 2.12. Предположим, что q – степень нечетного простого числа и $\varepsilon \in \{+, -\}$. Если $k_6(\varepsilon q) = r^m$, где $r \in \{7, 31\}$ и m – натуральное число, то

$$(r, m, \varepsilon q) \in \{(7, 1, 5), (7, 1, 3), (7, 3, 19), (31, 1, -5)\}.$$

Доказательство. Используя равенство (1), находим, что $k_6(\varepsilon q) = \frac{q^2 - \varepsilon q + 1}{(q + \varepsilon 1, 3)}$. Пусть $k_6(\varepsilon q) = r^m$, где $r \in \{7, 31\}$. Если $(q + \varepsilon 1, 3) = 3$, то имеем равенство $3r^m = q^2 - \varepsilon q + 1 = (\varepsilon q - 1)^2 + (\varepsilon q - 1) + 1$. По лемме 2.11 находим, что $m = 1$ или $m = 2$. Поскольку $r = 7$ или $r = 31$, заключаем, что $(r, m, \varepsilon q - 1) \in \{(7, 1, 4), (7, 1, -5)\}$. По предположению q нечетно, поэтому возможен только случай $r = 7$ и $\varepsilon q = 5$.

Пусть теперь $(q + \varepsilon 1, 3) = 1$. Тогда имеем равенство $r^m = q^2 - \varepsilon q + 1 = (\varepsilon q - 1)^2 + (\varepsilon q - 1) + 1$. По лемме 2.11 верно, что либо $m = 3$ и $\varepsilon q - 1 \in \{18, -19\}$, либо $m = 1$. Если $m = 3$ и $\varepsilon q - 1 \in \{18, -19\}$, то $r = 7$, $\varepsilon q = 19$. Наконец, если $m = 1$, то $(r, \varepsilon q - 1) \in \{(7, 2), (7, -3), (31, 5), (31, -6)\}$. Поскольку q нечетно, получаем, что $(r, \varepsilon q) \in \{(7, 3), (31, -5)\}$. \square

Далее для линейных и унитарных групп над полем порядка q мы часто используем стандартное обозначение $L_n^\varepsilon(q)$, где $\varepsilon \in \{+, -\}$, т. е. $L_n^+(q) = L_n(q)$ и $L_n^-(q) = U_n(q)$. Следуя [6], через $\text{prk } L$ будем обозначать размерность группы L , если L – линейная или унитарная группа, и левый ранг группы L в случае симплектических или ортогональных групп.

Наименьшее общее кратное элементов спектра $\omega(G)$ равно периоду группы G и обозначается через $\text{exp}(G)$. Для простого числа $r \in \pi(G)$ период силовой r -подгруппы группы G обозначается через $\text{exp}_r(G)$, а наименьшее общее кратное элементов $\omega(G)$, взаимно простых с r , обозначается через $\text{exp}_{r'}(G)$.

Лемма 2.13.[19, следствие 0.5] Предположим, что L – простая классическая группа над полем характеристики p . Пусть $p^\gamma > \text{prk } L - 1$, если L линейная или унитарная, и $p^\gamma > 2 \text{prk } L - 1$ в противном случае. Тогда $\text{exp}_p(L) \leq p^\gamma$.

Лемма 2.14.[20, лемма 3.5] Пусть u – степень простого числа v . Тогда справедливы следующие утверждения.

(а) Если $S = L_n^\tau(u)$, где $\tau \in \{+, -\}$ и $n \geq 3$, то

$$\text{exp}_{v'}(S) = \frac{1}{c} \cdot \prod_{i=1}^n \Phi_i(\tau u),$$

где $c = r \in \pi(u - \tau 1)$, если $n = r^s$, и $c = 1$ иначе.

(б) Если $S = S_{2n}(u)$ или $S = O_{2n+1}(u)$ при $n \geq 2$, то

$$\text{exp}_{v'}(S) = \frac{1}{c} \cdot \prod_{i=1}^n \Phi_i(u^2),$$

где $c = (2, u - 1)^2$, если $n = 2^s$, и $c = (2, u - 1)$ иначе.

(в) Если $S = O_{2n}^\varepsilon(u)$, где $\varepsilon \in \{+, -\}$ и $n \geq 4$ четно, то $\text{exp}_{v'}(S) = \text{exp}_{v'}(O_{2n-\varepsilon 1}(q))$.

(г) Если $S = O_{2n}^\varepsilon(u)$, где $\varepsilon \in \{+, -\}$ и $n \geq 4$ нечетно, то

$$\text{exp}_{v'}(S) = \frac{\Phi_n(\varepsilon u)}{(2, u - 1)} \prod_{i=1}^{n-1} \Phi_i(u^2).$$

Предложение 2.15. Предположим, что S – простая классическая группа над полем характеристики v и порядка u такая, что $5 \leq t(S) \leq 14$. Тогда

$$\frac{1}{\alpha(S)} \cdot v \cdot u^{\gamma(S)} \leq \exp(S) \leq \beta(S) \cdot v \cdot u^{\gamma(S)},$$

где числа $\alpha(S), \beta(S)$ и $\gamma(S)$ указаны в таблице 1.

Доказательство. Будем использовать, что $\exp(S) = \exp_v(S) \cdot \exp_{v'}(S)$, и оценим каждый из этих множителей.

Предположим, что $S = L_m^\tau(u)$, где $\tau \in \{+, -\}$. Тогда получаем, что $9 \leq m \leq 28$ (см. таблицу 2). По лемме 2.13 число $\exp_v(S)$ не превосходит минимальной степени v , большей $m - 1$, и, следовательно, $v \leq \exp_v(S) \leq (m - 1)v$. По лемме 2.14 мы знаем, что

$$\exp_{v'}(S) = \frac{1}{c} \cdot \prod_{i=1}^m \Phi_i(\tau u),$$

где $c = r \in \pi(u - \tau 1)$, если $m = r^s$, и $c = 1$ в противном случае. Тогда $1 \leq c$ и $c \leq 3, 11, 13, 2, 17, 19, 23, 5, 3$, если $m = 9, 11, 13, 16, 17, 19, 23, 25, 27$ соответственно. Будем использовать следующие оценки для произведений круговых многочленов. Если $s \geq 1$, то $\prod_{k=0}^s \Phi_{2^k}(x) = x^{2^s} - 1$ и, следовательно, $\frac{3}{4}u^{2^s} \leq \prod_{k=0}^s \Phi_{2^k}(\tau u) < u^{2^s}$. Если t – нечетное простое число, а s – натуральное число, то из леммы 2.4(а) следует, что $\Phi_{t^s}(x) = \Phi_{2t^s}(-x) = 1 + x^{t^{s-1}} + x^{2t^{s-1}} + \dots + x^{(t-1)t^{s-1}} = \frac{x^{t^s} - 1}{x^{t^{s-1}} - 1}$. Если $u \geq 3$, то из леммы 2.4 следует, что

$$\frac{1}{2}u^{t^s - t^{s-1}} \leq \Phi_{t^s}(\tau u), \quad \Phi_{2t^s}(\tau u) \leq 2u^{t^s - t^{s-1}}.$$

Эти неравенства верны для $u = 2$, поскольку $\Phi_{t^s}(\pm 2) \geq \frac{2^{t^s} + 1}{2^{t^{s-1}} + 1} > 2^{t^s - t^{s-1} - 1}$. Более того, из леммы 2.4(а) следует, что $\Phi_{t^s}(\tau u)\Phi_{2t^s}(\tau u) = \Phi_{t^s}(u^2) = 1 + u^{2t^{s-1}} + \dots + u^{2(t-1)t^{s-1}}$. Поскольку $u^2 \geq 4$, лемма 2.4(г) влечет, что $u^{2t^{s-1}(t-1)} < \Phi_{t^s}(\tau u)\Phi_{2t^s}(\tau u) < \frac{4}{3}u^{2t^{s-1}(t-1)}$. Для оставшихся многочленов используем следующие неравенства:

$$\frac{3}{4}u^4 < \Phi_{12}(\tau u) = u^4 - u^2 + 1 < u^4,$$

$$\frac{u^8}{2} < \Phi_{15}(\tau u) = u^8 - (\tau u)^7 + (\tau u)^5 - u^4 + (\tau u)^3 - (\tau u) + 1 < 2u^8,$$

$$\frac{3}{4}u^8 < \Phi_{20}(\tau u) = u^8 - u^6 + u^4 - u^2 + 1 < u^8, \quad \frac{3}{4}u^8 < \Phi_{24}(\tau u) = u^8 - u^4 + 1 < u^8,$$

$$\frac{3}{4}u^{12} < \Phi_{28}(\tau u) = u^{12} - u^{10} + u^8 - u^6 + u^4 - u^2 + 1 < u^{12}.$$

Например, если $m = 12$, то $\exp_{v'}(S) = \prod_{i=1}^{12} \Phi_i(\tau u)$. Находим, что

$$\frac{3}{4}u^8 < \Phi_1(\tau u)\Phi_2(\tau u)\Phi_4(\tau u)\Phi_8(\tau u) < u^8, \quad u^4 < \Phi_3(\tau u)\Phi_6(\tau u) < \frac{4}{3}u^4,$$

$$u^8 < \Phi_5(\tau u)\Phi_{10}(\tau u) < \frac{4}{3}u^8, \quad \frac{1}{2}u^6 < \Phi_7(\tau u), \Phi_9(\tau u) < 2u^6,$$

$$\frac{1}{2}u^{10} < |\Phi_{11}(\tau u)| < 2u^{10}, \quad \frac{3}{4}u^4 < \Phi_{12}(\tau u) < u^4.$$

Поскольку $v \leq \exp_v(S) \leq 11v$, получаем, что $\exp(S) > v \cdot (\frac{1}{2})^3 \cdot (\frac{3}{4})^2 u^{46} = \frac{9}{128}vu^{46} > \frac{1}{15}vu^{46}$ и $\exp(S) < 11v \cdot (\frac{4}{3})^2 2^3 u^{46} < 157vu^{46}$.

Предположим, что $S \in \{S_{2m}(u), O_{2m+1}(u), O_{2m+2}^+(u)\}$, где m нечетно и $5 \leq m \leq 17$. По лемме 2.13 получаем, что $v \leq \exp_v(S) \leq (2m+1)v$. По лемме 2.14(б),(в) мы знаем, что $\exp_v(S) = \frac{1}{c} \cdot \prod_{i=1}^m \Phi_i(u^2)$, где $c \leq 4$, если $n = 2^s$, и $c \leq 2$ в противном случае. Оценим $\Phi_i(u^2)$

следующим образом. Во-первых, воспользуемся тем, что $\prod_{k=0}^s \Phi_{2^k}(u^2) = u^{2^s} - 1$, поэтому это произведение меньше u^{2^s} и не меньше $\frac{15}{16}u^{2^s}$ для всех $s \geq 2$. Поскольку $u^2 \geq 4$, из леммы 2.4 следует, что $\frac{2}{3}u^{2\varphi(i)} < \Phi_i(u^2) < \frac{4}{3}u^{2\varphi(i)}$. Мы используем эти неравенства, если $i = t^s$, где t – нечетное простое число и $2i > m$. Если $i = t^s$ и $2i \leq m$, то $\Phi_i(u^2)\Phi_{2i}(u^2) = \Phi_i(u^4) = 1 + u^4 + \dots + u^{4\varphi(i)} > u^{4\varphi(i)}$ и, поскольку $u^4 \geq 16$, получаем, что $\Phi_i(u^2)\Phi_{2i}(u^2) < \frac{16}{15}u^{4\varphi(i)}$. Оставшиеся две оценки для этого случая:

$$\frac{15}{16}u^8 < \Phi_{12}(u^2) = u^8 - u^4 + 1 < u^8,$$

$$\frac{3}{4}u^{16} < \Phi_{15}(u^2) = u^{16} - u^{14} + u^{10} - u^8 + u^6 - u^2 + 1 < u^{16}.$$

Предположим, что $S \in \{S_{2m}(u), O_{2m+1}(u), O_{2m}^-(u)\}$, где m четно и $6 \leq m \leq 18$. По лемме 2.13 получаем, что $v \leq \exp_v(S) \leq (2m-1)v$. По лемме 2.14(б),(в) мы знаем, что $\exp_v(S) = \frac{1}{c} \cdot \prod_{i=1}^m \Phi_i(u^2)$, где $c \leq 4$, если $n = 2^s$, и $c \leq 2$ в противном случае. Для многочленов $\Phi_i(u^2)$ используем неравенства из предыдущего случая.

Предположим, что $S \simeq O_{2m}^\epsilon(u)$, где $\epsilon \in \{+, -\}$, m нечетно и $5 \leq m \leq 19$. По лемме 2.13 получаем, что $v \leq \exp_v(S) \leq (2m-1)v$. По лемме 2.14(б),(в) мы знаем, что $\exp_v(S) = \frac{\Phi_n(\epsilon u)}{(2, u-1)} \prod_{i=1}^{n-1} \Phi_i(u^2)$. Очевидно, что $(2, u-1) \leq 2$. Для многочленов $\Phi_i(u^2)$ мы используем неравенства из предыдущего случая. Наконец, оцениваем $\Phi_n(\epsilon u)$ так же, как в случае линейных и унитарных групп. \square

3 Предварительные сведения: графы простых чисел и спектры групп лиева типа

Обозначим через $\pi(G)$ множество всех простых делителей порядка группы G . Граф простых чисел группы G обозначается через $GK(G)$. Коклику в $GK(G)$, содержащую r , будем называть $\{r\}$ -коккликой. Если $r \in \pi(G)$, то $t(r, G)$ обозначает наибольший размер $\{r\}$ -кокклики в $GK(G)$. Через $\rho(r, G)$ обозначается множество вершин в некоторой $\{r\}$ -кокклике в $GK(G)$ размера $t(r, G)$.

Простое число $r \in \pi(G)$ называется *большим* (относительно G), если r лежит в некоторой кокклике наибольшего размера в $GK(G)$, и *малым* (относительно G) в противном случае.

Таблица 1: Оценки для $\exp(S)$, когда $5 \leq t(S) \leq 14$

S	$(\alpha(S), \beta(S), \gamma(S))$	S	$(\alpha(S), \beta(S), \gamma(S))$
L_9^\pm	(32, 86, 28)	L_{19}^\pm	(1081, 1821, 120)
L_{10}^\pm	(6, 64, 32)	L_{20}^\pm	(76, 1922, 128)
L_{11}^\pm	(118, 143, 42)	L_{21}^\pm	(152, 4046, 140)
L_{12}^\pm	(15, 157, 46)	L_{22}^\pm	(76, 2832, 150)
L_{13}^\pm	(370, 342, 58)	L_{23}^\pm	(3490, 5934, 172)
L_{14}^\pm	(15, 247, 64)	L_{24}^\pm	(203, 6203, 180)
L_{15}^\pm	(29, 531, 72)	L_{25}^\pm	(2023, 12946, 200)
L_{16}^\pm	(57, 569, 80)	L_{26}^\pm	(203, 8990, 212)
L_{17}^\pm	(968, 1214, 96)	L_{27}^\pm	(1214, 18699, 230)
L_{18}^\pm	(29, 860, 102)	L_{28}^\pm	(540, 19419, 242)
S_{10}, O_{11}, O_{12}^+	(5, 20, 20)	S_{32}, O_{33}, O_{32}^-	(21, 90, 160)
S_{12}, O_{13}, O_{12}^-	(4, 16, 24)	S_{34}, O_{35}, O_{36}^+	(16, 135, 192)
S_{14}, O_{15}, O_{16}^+	(5, 29, 36)	S_{36}, O_{37}, O_{36}^-	(11, 108, 204)
S_{16}, O_{17}, O_{16}^-	(10, 29, 44)	O_{10}^\pm	(7, 24, 16)
S_{18}, O_{19}, O_{20}^+	(8, 49, 56)	O_{14}^\pm	(7, 37, 30)
S_{20}, O_{21}, O_{20}^-	(5, 39, 64)	O_{18}^\pm	(10, 65, 50)
S_{22}, O_{23}, O_{24}^+	(8, 63, 84)	O_{22}^\pm	(10, 85, 74)
S_{24}, O_{25}, O_{24}^-	(8, 63, 92)	O_{26}^\pm	(16, 135, 104)
S_{26}, O_{27}, O_{28}^+	(12, 98, 116)	O_{30}^\pm	(16, 167, 136)
S_{28}, O_{29}, O_{28}^-	(8, 78, 128)	O_{34}^\pm	(21, 190, 176)
S_{30}, O_{31}, O_{32}^+	(11, 90, 144)	O_{38}^\pm	(21, 228, 222)

Лемма 3.1. Предположим, что L – неабелева простая группа с $t(L) \geq 5$ и $t(2, L) \geq 2$. Если G – группа с $\omega(G) = \omega(L)$, то справедливы следующие утверждения.

(а) Существует неабелева простая группа S такая, что $S \leq \overline{G} = G/K \leq \text{Aut } S$ для максимальной нормальной разрешимой подгруппы K группы G .

(б) Для любой коклики ρ из $GK(G)$ с $|\rho| \geq 3$, не более одного простого числа из ρ делит произведение $|K| \cdot |\overline{G}/S|$. В частности, $t(S) \geq t(G) - 1$.

(в) Каждое простое число $r \in \pi(G)$, не смежное с 2 в $GK(G)$, не делит произведение $|K| \cdot |\overline{G}/S|$. В частности, $t(2, S) \geq t(2, G)$.

(г) Группа K нильпотентна.

Доказательство. Первые три утверждения следуют из основной теоремы из [21]. Четвертое утверждение – это [22, теорема 1]. \square

Предположим, что L – простая классическая группа над полем порядка q и характеристики p . Положим

$$\delta(L) = \begin{cases} \pi(q - \varepsilon 1), & \text{если } L = L_n^\varepsilon(q), \\ \pi((2, q - 1)), & \text{если } L \text{ – симплектическая или ортогональная группа.} \end{cases}$$

Из основных результатов работы [23] (см. также [6, лемма 2.2]) следует, что для двух различных простых чисел $r, s \in \pi(L) \setminus \delta(L)$, где $r \neq p$, ответ на вопрос, являются ли они смежными в $GK(L)$, зависит только от $e(r, q)$, если $s = p$, и $e(r, q)$, $e(s, q)$, если $s \neq p$.

Для формулировки критерия смежности в [23] используется несколько функций целочисленного аргумента. В частности, для симплектических и ортогональных групп используется функция $\eta(k)$, где

$$\eta(k) = \begin{cases} k, & \text{если } k \text{ нечетно,} \\ k/2, & \text{если } k \text{ четно.} \end{cases}$$

Для линейных и унитарных групп будем использовать переформулировку критерия смежности из [24, леммы 2.1–2.3], который сформулирован в несколько иных терминах. Следуя [6], определим функцию φ для унификации дальнейших рассуждений.

$$\varphi(r, L) = \begin{cases} e(r, \varepsilon q), & \text{если } L = L_n^\varepsilon(q), \\ \eta(e(r, q)), & \text{если } L \text{ симплектическая или ортогональная.} \end{cases}$$

Из определения и свойств функции $e(r, q)$ следует, что

$$e(r, q) = \begin{cases} 2\varphi(r, L), & \text{если либо } e(r, q) \text{ четно и } L \text{ симплектическая} \\ & \text{или ортогональная,} \\ & \text{либо } e(r, q) \equiv 2 \pmod{4} \text{ и } L \text{ унитарная;} \\ \varphi(r, L)/2, & \text{если } e(r, q) \equiv 1 \pmod{2} \text{ и } L \text{ унитарная;} \\ \varphi(r, L) & \text{иначе.} \end{cases}$$

В следующей лемме перечислены критерии смежности в графах простых чисел классических групп из [23]–[25] для всех типов классических групп.

Лемма 3.2. Пусть L – простая классическая группа над полем порядка q и характеристики p , где $\text{rk } L = n \geq 4$. Возьмем нечетные простые числа r, s такие, что $r, s \in \pi(G) \setminus \{p\}$. Положим $k = e(r, q)$ и $l = e(s, q)$. Предположим, что $2 \leq \varphi(r, L) \leq \varphi(s, L)$. Тогда справедливы следующие утверждения.

(а) Если $L = L_n^\varepsilon(q)$, то r и s не смежны в $GK(L)$ тогда и только тогда, когда $\varphi(r, L) + \varphi(s, L) > n$, и $\frac{\varphi(s, L)}{\varphi(r, L)}$ не является целым числом.

(б) Если $L \in \{O_{2n+1}(q), S_{2n}(q)\}$, то r и s не смежны в $GK(L)$ тогда и только тогда, когда $\varphi(r, L) + \varphi(s, L) > n$, и $\frac{l}{k}$ не является нечетным целым числом.

(в) Если $L = O_{2n}^\varepsilon(q)$, то r и s не смежны в $GK(L)$ тогда и только тогда, когда $2\varphi(r, L) + 2\varphi(s, L) > 2n - (1 - \varepsilon)(-1)^{k+l}$, $\frac{l}{k}$ не является нечетным целым числом, и, если $\varepsilon = +$, то цепочка равенств $n = l = 2\varphi(s, L) = 2\varphi(r, S) = 2k$ неверна.

В некоторых случаях удобнее использовать следующее следствие критерия смежности.

Лемма 3.3. [6, лемма 2.4] Пусть L – простая классическая группа над полем порядка q и характеристики p , и пусть $\text{rk } L = n \geq 4$.

(а) Если $r \in \pi(L) \setminus \{p\}$, то $\varphi(r, L) \leq n$.

(б) Если r и s – различные простые числа из $\pi(L) \setminus \{p\}$, причем $\varphi(r, L) \leq n/2$ и $\varphi(s, L) \leq n/2$, то r и s смежны в $GK(L)$.

(в) Если r и s – различные простые числа из $\pi(L) \setminus \{p\}$, причем $n/2 < \varphi(r, L) \leq n$ и $n/2 < \varphi(s, L) \leq n$, то r и s смежны в $GK(L)$ тогда и только тогда, когда $e(r, q) = e(s, q)$.

(г) Если r и s – различные простые числа из $\pi(L) \setminus \{p\}$ и $e(r, q) = e(s, q)$, то r и s смежны в $GK(L)$.

Следующая лемма является аналогом [6, лемма 2.7], сформулированным при новых ограничениях на L .

Лемма 3.4. Пусть L – простая классическая группа над полем порядка q и характеристики p , и пусть $t(L) \geq 5$.

- (а) Если $\varphi(r, L) \geq n/2$, то r является большим относительно L .
- (б) Если r большое относительно L , то $\varphi(r, L) \geq n/2 - 1$.
- (в) Если r большое относительно L , то

$$\varphi(r, L) \geq \begin{cases} t(L), & \text{если } L \text{ линейная или унитарная;} \\ (2t(L) - 4)/3, & \text{если } L \text{ симплектическая или ортогональная.} \end{cases}$$

(г) Если ρ – коклика в $GK(L)$ и $n/2 < \varphi(r, L)$ для каждого $r \in \rho$, то $GK(L)$ имеет коклику σ размера $t(L)$ с $\rho \subseteq \sigma$.

Доказательство. Все пункты могут быть проверены с помощью [25, таблицы 2 и 3]. \square

Лемма 3.5. Пусть L – простая классическая группа над полем порядка q и характеристики p . Тогда $t(p, L) \leq 4$. Более того, предположим, что $\text{rk } L \geq 8$, если L – линейная или унитарная группа, и $\text{rk } L \geq 5$ в противном случае. Тогда справедливы следующие утверждения.

- (а) Если r не смежно с p в $GK(L)$, то r является большим относительно L .
- (б) Если L – линейная или унитарная группа, то $t(p, L) = 3$.
- (в) Если $t(p, L) = 2$, то $L \in \{O_{2n+1}(q), S_{2n}(q)\}$, где n – четное целое число.

Доказательство. Обозначим $n = \text{rk } L$. Значения $t(p, L)$ можно найти в [23, таблица 4]. Предположим, что $r \in \pi(L)$ не смежно с p в $GK(L)$. По [23, предложение 3.1] находим, что $\varphi(r, L) > n - 2$, если $L = L_n^\varepsilon(q)$ или $L = O_{2n}^\pm(q)$, и $\varphi(r, L) > n - 1$, если $L = O_{2n+1}(q)$ или $L = S_{2n}(q)$. По лемме 3.4 получаем, что r является большим по отношению к L . \square

Лемма 3.6.[6, лемма 2.3] Пусть L – простая классическая группа над полем порядка q и характеристики p . Если r – нечетное простое число из $\pi(L) \setminus \{p\}$, то $\varphi(r, L)$ делит $r - 1$, а если L – симплектическая или ортогональная группа, то $2\varphi(r, L)$ делит $r - 1$.

Лемма 3.7.[26, лемма 1.3] Предположим, что S – простая классическая группа лиева ранга m над полем порядка u . Тогда порядки элементов группы S не превосходят $\frac{u}{u-1}u^m$.

Пусть L – простая классическая группа над полем порядка q и характеристики p . Для $\sigma \subseteq \pi(L) \setminus \{p\}$, положим $E(\sigma, L) = \{e(r, -q) \mid r \in \sigma\}$, если L – унитарная группа, и $E(\sigma, L) = \{e(r, q) \mid r \in \sigma\}$ в противном случае. По лемме 3.5 верно, что $t(p, L) \leq 4$, поэтому если $t(L) \geq 5$, то любая коклика ρ наибольшего размера в $GK(L)$ не содержит p , и, следовательно, множество $E(\rho, L)$ корректно определено. Определим $J(L)$ как объединение множеств $E(\rho, L)$, а $E(L)$ – как пересечение этих множеств, где ρ пробегает все коклики наибольшего размера из $GK(L)$. Следующая лемма является аналогом [6, леммы 2.5] при новых ограничениях на L .

Лемма 3.8. Пусть L – простая классическая группа над полем порядка q и характеристики p , и пусть $t(L) \geq 5$. Пусть ρ – коклика наибольшего размера в $GK(L)$. Если $J(L) = E(L)$, то $E(\rho, L) = E(L)$. Если $J(L) \neq E(L)$, то $E(\rho, L) = E(L) \cup \{j\}$ для некоторого $j \in J(L) \setminus E(L)$. В частности, $|E(L)| \leq t(L) \leq |E(L)| + 1$. Множества $E(L)$, $J(L) \setminus E(L)$ и числа $t(L)$ перечислены в таблице 2.

Доказательство. См. [25, таблицы 2, 3]. Отметим, что [25, таблица 3] содержит опечатку для $L = O_{12}^-(q)$, поскольку $r_4(q)$ и $r_{12}(q)$ смежны в $GK(L)$ по лемме 3.2(в). \square

Таблица 2: Коклики наибольшего размера в $GK(L)$ с $t(L) \geq 5$

L	Условия	$t(L)$	$E(L)$	$J(L) \setminus E(L)$
$U_n(q)$	$n \geq 9$ нечетно $n \geq 10$ четно	$\frac{n+1}{2}$ $\frac{n}{2}$	$\{i \mid \frac{n}{2} < i \leq n\}$ $\{i \mid \frac{n}{2} < i < n\}$	\emptyset $\{\frac{n}{2}, n\}$
$L_n(q)$	$n \geq 9$ нечетно и $(n, q) \neq (9, 2), (11, 2)$ $n = 11$ и $q = 2$ $n \geq 10$ четно и $(n, q) \neq (10, 2), (12, 2)$ $n = 12$ и $q = 2$	$\frac{n+1}{2}$ 5 $\frac{n}{2}$ 6	$\{i \mid \frac{n}{2} < i \leq n\}$ $\{7, 8, 9, 11\}$ $\{i \mid \frac{n}{2} < i < n\}$ $\{7, 8, 9, 10, 11, 12\}$	\emptyset $\{5, 10\}$ $\{\frac{n}{2}, n\}$ \emptyset
$S_{2n}(q)$ или $O_{2n+1}(q)$	$n \geq 8, n \equiv 0 \pmod{4}$ $n \geq 5, n \equiv 1 \pmod{4}$ и $(n, q) \neq (5, 2)$ $n \geq 6, n \equiv 2 \pmod{4}$ и $(n, q) \neq (6, 2)$ $n \geq 7, n \equiv 3 \pmod{4}$ и $(n, q) \neq (7, 2)$ $n = 6$ и $q = 2$ $n = 7$ и $q = 2$	$\frac{3n+4}{4}$ $\frac{3n+5}{4}$ $\frac{3n+2}{4}$ $\frac{3n+3}{4}$ 5 6	$\{i \mid \frac{n}{2} \leq \eta(i) \leq n\}$ $\{i \mid \frac{n}{2} < \eta(i) \leq n\}$ $\{i \mid \frac{n}{2} < \eta(i) \leq n\}$ $\{i \mid \frac{n+1}{2} < \eta(i) \leq n\}$ $\{3, 5, 8, 10, 12\}$ $\{5, 7, 10, 12, 14\}$	\emptyset \emptyset $\{\frac{n}{2}, n\}$ $\{\frac{n-1}{2}, n-1, n+1\}$ $\{3, 8\}$
$O_{2n}^+(q)$	$n \geq 8, n \equiv 0 \pmod{4}$ $n \geq 9, n \equiv 1 \pmod{4}$ $n \geq 10, n \equiv 2 \pmod{4}$ $n \geq 7, n \equiv 3 \pmod{4}$	$\frac{3n}{4}$ $\frac{3n+1}{4}$ $\frac{3n-2}{4}$ $\frac{3n+3}{4}$	$\{i \mid \frac{n}{2} \leq \eta(i) \leq n, i \neq 2n\}$ $\{i \mid \frac{n}{2} < \eta(i) \leq n, i \neq 2n, n+1\}$ $\{i \mid \frac{n}{2} < \eta(i) \leq n, i \neq 2n\}$ $\{i \mid \frac{n-1}{2} \leq \eta(i) \leq n, i \neq 2n, n-1\}$	\emptyset $\{n-1, n+1\}$ $\{\frac{n}{2}, n\}$ \emptyset
$O_{2n}^-(q)$	$n \geq 8, n \equiv 0 \pmod{4}$ $n \geq 9, n \equiv 1 \pmod{4}$ $n = 6, q = 2$ $n = 6, q > 2$ $n \geq 10, n \equiv 2 \pmod{4}$ $n \geq 7, n \equiv 3 \pmod{4}$ и $q \neq 2$ $n = 7, q = 2$	$\frac{3n+4}{4}$ $\frac{3n+1}{4}$ 5 5 $\frac{3n+2}{4}$ $\frac{3n+3}{4}$ 5	$\{i \mid \frac{n}{2} \leq \eta(i) \leq n\}$ $\{i \mid \frac{n}{2} < \eta(i) \leq n, i \neq n, \frac{n+1}{2}\}$ $\{3, 8, 5, 10, 12\}$ $\{8, 5, 10, 12\}$ $\{i \mid \frac{n}{2} < \eta(i) \leq n\}$ $\{i \mid \frac{n-1}{2} \leq \eta(i) \leq n, i \neq n, \frac{n-1}{2}\}$ $\{5, 10, 12, 14\}$	\emptyset $\{\frac{n+1}{2}, n-1\}$ \emptyset $\{3, 6\}$ $\{\frac{n}{2}, n-2, n\}$ \emptyset $\{3, 8\}$

Лемма 3.9. Предположим, что $L = L_n^\varepsilon(q)$, где $\varepsilon \in \{+, -\}$ и $t(L) \geq 5$. Тогда справедливы следующие утверждения.

- (а) Если $r \in R_i(\varepsilon q)$, где $2 \leq i < n/2$, то $t(r, L) \leq i$.
- (б) Если $r \in R_i(\varepsilon q)$, где $n/3 < i < n/2$, то $t(r, L) = i$.

Доказательство. Поскольку $t(L) \geq 5$, согласно таблице 2 видим, что $n \geq 9$. Предположим, что $r \in R_i(\varepsilon q)$, где $2 \leq i < n/2$, и s не смежно с r в $GK(L)$. Согласно таблице 2 видим, что либо $i = 5$ и $L = L_{11}(q)$, либо r мало относительно L . В первом

случае $t(r, L) = 5 = i$, поэтому утверждение верно. Следовательно, можно считать, что r мало. По лемме 3.5(a) получаем, что $s \neq p$. Тогда из леммы 3.3(б) следует, что $j = \varphi(s, L) > n/2 > i$. Из леммы 3.2(a) следует, что s не смежно с r тогда и только тогда, когда $j \in J = \{n, n-1, \dots, n-i+1\}$ и j не делится на i . Очевидно, что в J существует хотя бы одно целое число, делящееся на i . Значит, существует не более $i-1$ вариантов для j и поэтому $t(r, L) \leq i$.

Предположим теперь, что $i > n/3$. Заметим, что если $j \in J$, то $r_j(\varepsilon q)$ большое относительно L согласно таблице 2, поэтому соответствующие простые числа для J вместе с r образуют коклику в $GK(L)$. Очевидно, что $2i$ – единственное целое число, делящееся на i среди элементов J . Следовательно, если $R_j(\varepsilon q) \neq \emptyset$ для всех $j \in J$, то $t(r, L) = i$. Согласно таблице 2 остается рассмотреть случаи $L = L_{11}(2)$ и $L_{12}(2)$. В этих случаях мы видим, что $R_6(2) = \emptyset$ и $i = 4, 5$. Однако мы видим, что 6 не принадлежит множеству $\{n-i+1, \dots, n\}$, так что снова $t(r, L) = i$, как и заявлено. \square

Лемма 3.10.[6, лемма 2.13] Пусть L – простая классическая группа над полем порядка q и характеристики p . Пусть k и l – целые числа, $k \geq 0$, $l > 0$, и $\delta = \delta(L)$. Для $j = 1, \dots, l$ предположим, что попарно различные простые числа r_j лежат в $\pi(L) \setminus (\delta \cup \{p\})$. Положим $\varepsilon = -$, если L – унитарная группа, и $\varepsilon = +$ в противном случае. Обозначим $i_j = e(r_j, \varepsilon q)$. Произведение $p^k r_1 r_2 \cdots r_l$ лежит в $\omega(L)$ тогда и только тогда, когда δ' -часть числа $p^k a$ лежит в $\omega(L)$, где

$$a = \begin{cases} [q^{i_1} - (\varepsilon 1)^{i_1}, q^{i_2} - (\varepsilon 1)^{i_2}, \dots, q^{i_l} - (\varepsilon 1)^{i_l}], & \text{если } L = L_n^\varepsilon(q), \\ [q^{\eta(i_1)} + (-1)^{i_1}, q^{\eta(i_2)} + (-1)^{i_2}, \dots, q^{\eta(i_l)} + (-1)^{i_l}] & \text{иначе.} \end{cases}$$

В частности, если i_1, i_2, \dots, i_l больше 2 и попарно различны, то $p^k r_1 r_2 \cdots r_l \in \omega(L)$ тогда и только тогда, когда $p^k k_{i_1}(\varepsilon q) k_{i_2}(\varepsilon q) \cdots k_{i_l}(\varepsilon q) \in \omega(L)$.

Лемма 3.11.[6, лемма 3.8] Для простой классической группы L над полем порядка q и характеристики p с $\text{rgk}(L) = n \geq 4$ положим

$$j = \begin{cases} n, & \text{если } L \simeq L_n(q); \\ 2n-2, & \text{если либо } L \simeq O_{2n}^+(q), \text{ либо } L \simeq U_n(q) \text{ и } n \text{ четно,} \\ 2n, & \text{в противном случае.} \end{cases}$$

Тогда $(k_j(q), |P|) = 1$ для любой собственной параболической подгруппы P группы L . Если $i \neq j$ и примитивный простой делитель $r_i(q)$ принадлежит $\pi(L)$, то существует собственная параболическая подгруппа P группы L такая, что $k_i(q)$ принадлежит $\omega(P)$. В частности, если два различных простых числа $r, s \in \pi(L)$ не делят порядок никакой собственной параболической подгруппы группы L , то r и s смежны в $GK(L)$.

Лемма 3.12.[6, лемма 3.5] Пусть L – простая классическая группа над полем порядка q и характеристики p , $r \in \pi(L)$, $r^s \in \omega(P)$, где P – собственная параболическая подгруппа группы L , и $(r, 6p(q+1)) = 1$. Если L действует точно на векторном пространстве V над полем характеристики t , отличной от p , то $tr^s \in \omega(V \rtimes L)$.

Лемма 3.13. Предположим, что L – простая классическая группа над полем порядка q и нечетной характеристики p . Если $t(L) \geq 5$ и $t(r, L) = 2$, то r делит $p(q^2 - 1)$.

Доказательство. Предположим, что $r \in \pi(L) \setminus \{p\}$ и r не делит $q^2 - 1$. Обозначим $i = \varphi(r, L)$, если L – линейная или унитарная группа, и $i = e(r, q)$, если L – симплектическая или ортогональная группа. Для доказательства утверждения покажем, что $t(r, L) > 2$.

Если r является большим относительно L , то $t(r, L) = t(L) \geq 5$. Поэтому можно считать, что r мало относительно L .

Предположим, что L – линейная или унитарная группа. Поскольку $(r, p(q^2 - 1)) = 1$, то $i \geq 3$. Согласно таблице 2 видим, что $n \geq 9$ и $i \leq n/2$. Рассмотрим простые числа s_j для $0 \leq j \leq 2$ такие, что $\varphi(s_j, L) = n - j$. Тогда $\varphi(s_j, L) \geq n - 2 > \frac{n}{2} \geq i$. Поскольку $i \geq 3$, не более одного числа из $n, n - 1, n - 2$ делится на i . Из леммы 3.2(а) следует, что r не смежно по крайней мере с двумя простыми числами из $\{s_0, s_1, s_2\}$, и, более того, множество $\{s_0, s_1, s_2\}$ является кокликкой в $GK(L)$. Следовательно, получаем, что $t(r, L) \geq 3$.

Предположим, что $L \simeq \{O_{2n+1}(q), S_{2n}(q)\}$. Поскольку $(r, p(q^2 - 1)) = 1$, то $i \geq 2$. Согласно таблице 2 видим, что $n \geq 5$. По лемме 3.4(а) получаем, что $i < n/2$. Сначала рассмотрим случай $r \in R_4(q)$. Если n нечетно, то $\{r, r_n(q), r_{2n}(q)\}$ – коклика размера 3 в $GK(L)$ по лемме 3.2(б). Аналогично, если n четно, то $\{r, r_{n-1}(q), r_{2n-2}(q)\}$ – коклика размера 3 в $GK(L)$. Теперь рассмотрим случай $r \notin R_4(q)$. Тогда $\eta(i) \geq 3$. Заметим, что не более одного числа среди $2n, 2n - 2, 2n - 4$ делится на i , поэтому r и два простых числа из множества $\{r_{2n}(q), r_{2n-2}(q), r_{2n-4}(q)\}$ образуют коклику размера 3 в $GK(L)$ по лемме 3.2(б).

Предположим, что $L \simeq O_{2n}^\varepsilon(q)$, где $\varepsilon \in \{+, -\}$. Поскольку $(r, p(q^2 - 1)) = 1$ и r мало относительно L , то согласно [25, таблица 3] имеем $i \geq 2$ и $n \geq 6$. Сначала рассмотрим случай $r \in R_4(q)$. Если n нечетно, то $\frac{n-1}{4}$ и $\frac{2n-2}{4}$ не могут быть одновременно нечетными целыми числами, поэтому $\{r, r_n(\varepsilon q), r_{n-1}(q)\}$ или $\{r, r_n(\varepsilon q), r_{2n-2}(q)\}$ – коклика в $GK(L)$ по лемме 3.2(в). Если n четно, то $\{r, r_{n-1}(\varepsilon q), r_{2n-2}(\varepsilon q)\}$ – коклика размера 3 в $GK(L)$ по лемме 3.2(в). Теперь рассмотрим случай $r \notin R_4(q)$. Тогда $\eta(i) \geq 3$. Поскольку r мало относительно L , получаем, что $n \geq 7$ и $i < n/2$. Если n нечетно, то $\frac{n-2}{i}$ и $\frac{2(n-2)}{i}$ не могут быть одновременно нечетными целыми числами, поэтому $\{r, r_n(\varepsilon q), r_{n-2}(\varepsilon q)\}$ или $\{r, r_n(\varepsilon q), r_{2n-4}(\varepsilon q)\}$ – коклика размера 3 в $GK(L)$. Если n четно, то из леммы 3.2(в) следует, что $M = \{r_{2n-4}(q), r_{n-1}(q), r_{2n-2}(q)\}$ – коклика размера 3 в $GK(L)$, и r не смежно по крайней мере с двумя элементами из M , поэтому $t(r, L) \geq 3$, как и утверждалось. \square

4 Доказательство теоремы 3

В этом разделе мы доказываем результаты о строении групп, изоспектральных простым классическим группам. В конце этого раздела доказывается теорема 3.

Предположим, что L – простая классическая группа над полем нечетного порядка q , а G – группа, изоспектральная L . Предположим, что L и G удовлетворяют условию теоремы 3, в частности, $5 \leq t(L) \leq 13$. Обозначим $n = \text{prk } L$. Согласно таблице 2 находим, что $n \geq 9$, если L – линейная или унитарная группа, и $n \geq 5$ в остальных случаях.

Как уже упоминалось во введении, можно считать, что $n \neq 16$, если $S = S_{2n}(q)$ или $S = O_{2n+1}(q)$.

Используя [23, таблица 6], видим, что $t(2, L) \geq 2$. В силу леммы 3.1 существует небелева простая группа S такая, что $S \leq \overline{G} = G/K \leq \text{Aut } S$ для максимальной нормальной разрешимой подгруппы K группы G . По предположению S – простая классическая группа над полем порядка u , взаимно простого с q .

Положим $m = \text{prk}(S)$. Поскольку $t(L) \geq 5$, согласно таблице 2 существует коклика размера 5 в $GK(L)$, не содержащая простого числа 3. Из леммы 3.1 следует, что по

крайней мере четыре простых числа из этой коклики принадлежат $\pi(S)$. Это вместе с [25, таблицы 2, 3] влечет, что $m \geq 4$. Мы фиксируем эти обозначения и ограничения далее в этом разделе.

Лемма 4.1. Если S – классическая группа над полем характеристики v и $r \in \pi(K) \setminus \{v\}$, то $t(r, L) = 2$ и r делит $p(q^2 - 1)$.

Доказательство. Зафиксируем простое число $r \in \pi(K) \setminus \{v\}$. Из [6, лемма 2.10] следует, что $t(r, L) \geq 2$. Сначала покажем, что $t(r, L) = 2$.

Предположим, что $t(r, L) \geq 3$. Тогда существуют $s_1, s_2 \in \pi(L) \setminus \{r\}$ такие, что $\{r, s_1, s_2\}$ – коклика размера 3 в $GK(L)$. Если r большое относительно L или $r = p$, то можно считать, что s_1 и s_2 являются большими относительно L , поэтому они нечетны. Если r мало относительно L , из леммы 3.5(а) следует, что $s_1, s_2 \neq p$. Согласно таблице 2 получаем, что $\varphi(r, L) < \frac{n}{2}$. По лемме 3.3(б) справедливы неравенства $\varphi(s_1, L) > n/2$ и $\varphi(s_2, L) > n/2$. Значит, s_1 и s_2 нечетны во всех случаях. Из леммы 3.1 следует, что $s_1, s_2 \in \pi(S)$. По лемме 3.1 верно, что $t(S) \geq 4$. Значит, $S \neq L_2(v)$ согласно [25, таблица 2]. Тогда силовские $\{v\}$ -подгруппы группы S нециклические, и, следовательно, если $v = s_1$ или $v = s_2$, то $rs_1 \in \omega(G) \setminus \omega(L)$ или $rs_2 \in \omega(G) \setminus \omega(L)$ (см. напр. [22, лемма 2.13]). Поэтому можно считать, что $s_1, s_2 \neq v$. Из леммы 3.11 следует, что s_1 или s_2 делит порядок собственной параболической подгруппы группы S . По [22, лемма 2.16] получаем, что $rs_1 \in \omega(G) \setminus \omega(L)$ или $rs_2 \in \omega(G) \setminus \omega(L)$; противоречие.

Следовательно, верно, что $t(r, L) = 2$. По лемме 3.13 получаем, что r делит $p(q^2 - 1)$, что и требовалось показать. \square

Лемма 4.2. Предположим, что простое число $r \neq p$ делит $|\overline{G}/S|$.

(а) Если существует целое число $i \geq 3$ такое, что $k_i(\varepsilon q)$ взаимно просто с $|\overline{G}/S| \cdot |K| \cdot v$, где $\varepsilon \in \{+, -\}$, и для каждого $r_i \in R_i(\varepsilon q)$ верно, что $\varphi(r_i, S) > m/2$ и $rr_i \notin \omega(L)$, то r делит $k_i(\varepsilon q) - 1$.

(б) Если существуют различные i и j такие, что $i, j \geq 3$ и $\{r, r_i(\varepsilon q), r_j(\varepsilon q)\}$, где $\varepsilon \in \{+, -\}$, является кокликой размера 3 в $GK(L)$, то r делит $(k_i(\varepsilon q) - 1)(k_j(\varepsilon q) - 1)$.

Доказательство. Предположим, что существует $i \geq 3$ такое, что $k_i(\varepsilon q)$ взаимно просто с $|\overline{G}/S| \cdot |K| \cdot v$ и для каждого $r_i \in R_i(\varepsilon q)$ верно, что $\varphi(r_i, S) > m/2$ и $rr_i \notin \omega(L)$. По лемме 3.3(в) заключаем, что $e(r_i, u)$ одинаково для всех $r_i \in R_i(\varepsilon q)$. Положим $t = e(r_i, u)$ и заметим, что S имеет циклическую холлову подгруппу порядка $k_i(u)$ по [6, лемма 2.12]. Пусть $s \in \pi(k_i(\varepsilon q))$ и $P \in Syl_s(S)$. По аргументу Фраттини число r делит $|N_{\overline{G}}(P)|$. Выберем $x \in N_{\overline{G}}(P)$ так, чтобы $|x| = r$. Тогда $P\langle x \rangle$ – группа Фробениуса с ядром P и дополнением $\langle x \rangle$, и, следовательно, $|P| \equiv 1 \pmod{r}$. Мы знаем, что $(s, |\overline{G}/S| \cdot |K|) = 1$, поэтому силовские s -подгруппы групп G и S изоморфны. Поскольку s – произвольный элемент множества $\pi(k_i(\varepsilon q))$, получаем, что $k_i(\varepsilon q) - 1$ делится на r .

Предположим, что существуют различные i и j такие, что $i, j \geq 3$ и $\{r, r_i(\varepsilon q), r_j(\varepsilon q)\}$ – коклика в $GK(L)$. Тогда получаем, что $3 \notin \{r_i(\varepsilon q), r_j(\varepsilon q)\}$. Поскольку r делит $|\overline{G}/S|$, из леммы 3.1 следует, что $(k_i(\varepsilon q)k_j(\varepsilon q), |\overline{G}/S| \cdot |K|) = 1$ и, следовательно, $R_j(\varepsilon q) \cup R_i(\varepsilon q) \subseteq \pi(S)$. Теперь покажем, что существует $\ell \in \{i, j\}$ такое, что если $r_\ell \in R_\ell(\varepsilon q)$, то $r_\ell \neq v$ и $\varphi(r_\ell, S) > m/2$. Сначала предположим, что $v \in R_i(\varepsilon q) \cup R_j(\varepsilon q)$. Без ограничения общности пусть $r_i = v$. Тогда, поскольку r_i и r_j не смежны в $GK(S)$, используя [23, таблица 4], находим, что $\varphi(r_j, S) > m/2$, поэтому можно взять $\ell = j$. Если $v \notin R_i(\varepsilon q) \cup R_j(\varepsilon q)$ и хотя бы для одного $r_i \in R_i(\varepsilon q)$ верно, что $\varphi(r_i, S) \leq m/2$, то по лемме 3.3(б)

для каждого $r_j \in R_j(\varepsilon q)$ верно неравенство $\varphi(r_j, S) > m/2$. Следовательно, число j удовлетворяет условию пункта (а) и поэтому r делит $k_j(\varepsilon q) - 1$. \square

Предложение 4.3. Предположим, что $L = L_n^\varepsilon(q)$, где $\varepsilon \in \{+, -\}$. Если $r_i = r_i(\varepsilon q) \in \pi(\overline{G}/S)$ и $4 \leq i \leq n$, то выполняется одно из следующих утверждений.

- (а) $i = 4$ и либо $r_i = 61$ и $11 \leq n \leq 12$, либо $r_i = 5$ и $9 \leq n \leq 12$, либо $n \geq 13$;
- (б) $i = 5$ и либо $n \geq 23$, либо $r_i = 11$ и $n \in \{13, 21, 22\}$;
- (в) $i = 6$, $r_i = 31$, $n = 9$, $(q - \varepsilon 1, 5) = 5$, и $\varphi(s, S) \leq m/2$ для некоторого $s \in R_8(\varepsilon q)$;
- (г) $i = 6$, $r_i = 7$, $11 \leq n \leq 13$, $(q + \varepsilon 1, 5) = 5$, $(q - \varepsilon 1, 11) = 11$, и $\varphi(s, S) \leq m/2$ для некоторого $s \in R_8(\varepsilon q)$;
- (д) $i = 6$ и $n \geq 14$.

Доказательство. Поскольку $5 \leq t(L) \leq 13$, согласно таблице 2 получаем $9 \leq n \leq 26$.

Пусть j – целое число и $3 \leq j \leq n$. Обозначим через $r(j)$ наибольший простой делитель числа j , а через $d(j) = (r(j), \Phi_{j_{\{r(j)\}}}(\varepsilon q))$. Рассмотрим многочлен $f_j(x) = \frac{1}{d(j)} \cdot \Phi_j(x) - 1$. В силу равенства (1) и леммы 2.4(в) получаем, что $f_j(\varepsilon q) = k_j(\varepsilon q) - 1$. Предположим, что $\Phi_i(x)$ и $f_j(x)$ взаимно просты как элементы $\mathbb{Q}[x]$. Тогда согласно расширенному алгоритму Евклида существуют единственные многочлены $u_j(x), v_j(x) \in \mathbb{Q}[x]$ такие, что $u_j(x)\Phi_i(x) + v_j(x)f_j(x) = 1$, $\deg u_j < \deg f_j$ и $\deg v_j < \deg \Phi_i$. Следовательно, существует положительное целое число $c(j)$ такое, что $c(j)u_j(x) \in \mathbb{Z}[x]$ и $c(j)v_j(x) \in \mathbb{Z}[x]$, поэтому $c(j)u_j(x)\Phi_i(x) + c(j)v_j(x)f_j(x) = c(j)$.

Предположим, что существуют различные целые числа j_1 и j_2 такие, что $3 \leq j_1, j_2 \leq n$ и $\{r_i, r_{j_1}(\varepsilon q), r_{j_2}(\varepsilon q)\}$ – коклика размера 3 в $GK(L)$. По лемме 4.2 получаем, что r_i делит $(k_{j_1}(\varepsilon q) - 1)(k_{j_2}(\varepsilon q) - 1)$. Это означает, что если $f_{j_1}(x)$ и $f_{j_2}(x)$ взаимно просты с $\Phi_i(x)$ в $\mathbb{Q}[x]$, то r_i делит $c(j_1)c(j_2)$.

Теперь докажем утверждение при $i \geq 7$. Для каждой пары (i, n) в таблице 3 перечислены либо две пары целых чисел $(j_1, c(j_1))$ и $(j_2, c(j_2))$, либо три пары целых чисел $(j_1, c(j_1))$, $(j_2, c(j_2))$ и $(j_3, c(j_3))$. В первом случае пары выбираются так, что $\{r_i, r_{j_1}(\varepsilon q), r_{j_2}(\varepsilon q)\}$ является кокликой в $GK(L)$ и $\pi(c(j_1)c(j_2)) \cap R_i(\varepsilon q) = \emptyset$. Во втором случае пары выбираются так, что либо $\{r_i, r_{j_1}(\varepsilon q), r_{j_2}(\varepsilon q), r_{j_3}(\varepsilon q)\}$ является кокликой в $GK(L)$ и $\pi(c(j_1)c(j_2)) \cap \pi(c(j_1)c(j_3)) \cap \pi(c(j_2)c(j_3)) \cap R_i(\varepsilon q) = \emptyset$, либо $\{r_i, r_{j_1}(\varepsilon q), r_{j_2}(\varepsilon q)\}$ и $\{r_i, r_{j_1}(\varepsilon q), r_{j_3}(\varepsilon q)\}$ являются кокликами в $GK(L)$ и $\pi(c(j_1)c(j_2)) \cap \pi(c(j_1)c(j_3)) \cap R_i(\varepsilon q) = \emptyset$. Предыдущее рассуждение показывает, что r_i принадлежит соответствующим пересечениям, поэтому эти пары чисел противоречат существованию r_i .

Все проверки выполняются понятным образом: если имеются пары $(j_1, c(j_1))$, $(j_2, c(j_2))$ для фиксированных i и n , то, чтобы убедиться, что $\{r_i, r_{j_1}(\varepsilon q), r_{j_2}(\varepsilon q)\}$ – коклика в $GK(L)$, достаточно проверить, что числа i , j_1 и j_2 не делят друг друга и что $i + j_1 > n$, $i + j_2 > n$, $j_1 + j_2 > n$ по лемме 3.2. Аналогичная проверка проводится в случае трех индексов j_1 , j_2 и j_3 . Теперь, как было упомянуто выше, расширенный алгоритм Евклида дает единственные многочлены $u_{j_1}(x)$, $u_{j_2}(x)$, $v_{j_1}(x)$, $v_{j_2}(x)$ и нам остается только проверить, что перечисленные числа $c(j_1)$ и $c(j_2)$ удовлетворяют следующим условиям: $c(j_1)u_{j_1}(x)$, $c(j_1)v_{j_1}(x)$, $c(j_2)u_{j_2}(x)$, $c(j_2)v_{j_2}(x) \in \mathbb{Z}[x]$. Заметим, что если $j_{1\{r(j_1)\}}$ делит $r(j_1) - 1$ (и аналогично для j_2 и j_3), то нужно рассмотреть два случая: $d(j_1) = 1$ и, следовательно, $f_{j_1}(x) = \Phi_{j_1}(x) - 1$, или $d(j_1) = r(j_1)$ и, следовательно, $f_{j_1}(x) = \frac{1}{r(j_1)}\Phi_{j_1}(x) - 1$.

Числа $c(j_1)$ выбраны так, чтобы $c(j_1)u_{j_1}$, $c(j_1)v_{j_1}$ в обоих случаях были многочленами с целыми коэффициентами.

В качестве примера рассмотрим случай, когда $i = 7$ и $9 \leq n \leq 12$. Используем целые числа $j_1 = 8$, $j_2 = 6$ и $j_3 = 9$. Поскольку $6 + 7 > 12$ и $6, 7, 8, 9$ не делят друг друга, множества $\{r_7, r_8(\varepsilon q), r_6(\varepsilon q)\}$ и $\{r_7, r_8(\varepsilon q), r_9(\varepsilon q)\}$ являются кокликками в $GK(L)$. Следовательно, заключаем, что r_7 делит $(k_8(\varepsilon q) - 1)(k_6(\varepsilon q) - 1)$ и $(k_8(\varepsilon q) - 1)(k_9(\varepsilon q) - 1)$. Поскольку q нечетно, находим, что $d(8) = 2$ и $k_8(\varepsilon q) - 1 = \frac{1}{2}\Phi_8(\varepsilon q) - 1$. Легко видеть, что если $u(x) := \frac{1}{7}(2x^3 + 2x^2 - 5x + 2)$ и $v(x) := \frac{1}{7}(-4x^5 - 8x^4 + 2x^3 - 2x^2 - 6x - 10)$, то $u(x)\Phi_7(x) + v(x)(\frac{1}{2}\Phi_8(x) - 1) = 1$. Поэтому можно взять $c(8) = 7$. Это означает, что если r_7 делит $k_8(\varepsilon q) - 1$, то r_7 делит 7. Поскольку $r_7 \equiv 1 \pmod{7}$, получаем, что $\pi(k_8(\varepsilon q) - 1) \cap R_7(\varepsilon q) = \emptyset$. Теперь $k_6(\varepsilon q) - 1$ равно либо $\Phi_6(\varepsilon q) - 1$, либо $\frac{1}{3}\Phi_6(\varepsilon q) - 1$. В первом случае получаем, что $u(x)\Phi_7(x) + v(x)(\Phi_6(x) - 1) = 1$ для $u(x) := \frac{1}{7}(-6x + 7)$ и $v(x) := \frac{1}{7}(6x^5 + 5x^4 + 4x^3 + 3x^2 + 2x + 1)$, а во втором случае видим, что $u(x)\Phi_7(x) + v(x)(\frac{1}{3}\Phi_6(x) - 1) = 1$ для $u(x) := \frac{1}{127}(-42x + 85)$ и $v(x) := \frac{1}{127}(126x^5 - 3x^4 + 120x^3 - 15x^2 + 96x - 63)$. Следовательно, если r_7 делит $k_6(\varepsilon q) - 1$, то r_7 делит $7 \cdot 127$, и, следовательно, $r_7 = 127$. Аналогично, имеем $k_9(\varepsilon q) - 1$ равно либо $\Phi_9(\varepsilon q) - 1$, либо $\frac{1}{3}\Phi_9(\varepsilon q) - 1$. В первом случае получаем, что $u(x)\Phi_7(x) + v(x)(\Phi_9(x) - 1) = 1$ для $u(x) := -x^4 - x + 1$ и $v(x) := x^4 + x^3 + x^2 + x$, а во втором случае видим, что $u(x)\Phi_7(x) + v(x)(\frac{1}{3}\Phi_9(x) - 1) = 1$ для $u(x) := \frac{1}{7 \cdot 43}(-38x^5 - 31x^4 + 46x^3 - 48x^2 - 55x + 169)$ и $v(x) := \frac{1}{7 \cdot 43}(114x^5 + 207x^4 + 69x^3 + 99x^2 + 171x - 198)$. Следовательно, если r_7 делит $k_9(\varepsilon q) - 1$, то r_7 делит $7 \cdot 43$ и поэтому $r_7 = 43$. Приходим к противоречию, поскольку r_7 не может быть равно одновременно 127 и 43. Информация, которую можно использовать для воспроизведения этого рассуждения, представлена в таблице 3: мы добавляем пары $(8, 7)$, $(6, 7 \cdot 127)$ и $(9, 7 \cdot 43)$ в ячейку, соответствующую $i = 7$ и $9 \leq n \leq 12$. Другие случаи проверяются аналогично. Явные значения многочленов $u(x)$ и $v(x)$ для всех случаев записаны в отдельных файлах для каждого i [27]. Как упоминалось выше, эти многочлены можно найти с помощью расширенного алгоритма Евклида. Заметим, что мы используем те же j_1 и j_2 , если $i \in \{13, 14, 15, 17\}$, а также если $i \in \{18, 19, 20, 21, 22, 23, 25, 26\}$. Поэтому мы пишем * вместо $c(j_1)$ и $c(j_2)$ в соответствующих ячейках таблицы. Это означает, что $c(j_1)$ и $c(j_2)$ зависят от i , но всегда имеем $\pi(c(j_1)c(j_2)) \cap R_i(\varepsilon q) = \emptyset$.

Случаи $i = 4, 5$ рассматриваются аналогично, с той лишь разницей, что некоторые пересечения множеств непусты, поэтому простые числа из этих пересечений дают возможные исключения. Рассмотрим в качестве примера случай $i = 4$ и $n = 9, 10$. Мы используем коклику $\{r_4, r_7(\varepsilon q), r_9(\varepsilon q)\}$ из $GK(L)$. Заметим, что $k_7(\varepsilon q) - 1$ равно либо $\Phi_7(\varepsilon q) - 1$, если $d(7) = 1$, либо $\frac{1}{7}\Phi_7(\varepsilon q) - 1$, если $d(7) = 7$. Легко проверить, что если $u(x) = \frac{1}{2}(x^5 + 2x^4 + x^3 + x + 2)$ и $v(x) = \frac{1}{2}(-x - 1)$ или $u(x) = \frac{1}{50}(x^5 + 8x^4 + 7x^3 + x + 8)$ и $v := \frac{1}{50}(-7x - 49)$ соответственно, то $u(x)\Phi_4(x) + v(x)(\frac{1}{7}\Phi_7(x) - 1) = 1$. Следовательно, можно взять $c(7) = 50$. Аналогично получаем, что $c(9) = 10$. Это означает, что $r_4 \in \{\pi(50) \cup \pi(10)\} \cap R_4(\varepsilon q) \subseteq \{5\}$. Таким образом, можно гарантировать лишь невозможность случаев $r_4 \neq 5$.

Наконец, рассмотрим случай $i = 6$. По предположению, $9 \leq n \leq 13$. Пусть сначала $n = 9$. Согласно таблице 3 мы используем $j_1 = 8$ и $j_2 = 5$. Если $(q - \varepsilon 1, 5) = 1$, то $d(5) = 1$ и видим, что $c(8) = c(5) = 3$, и, следовательно, $r \in \{3\} \cap R_6(\varepsilon q) = \emptyset$. Таким образом, верно, что $(q - \varepsilon 1, 5) = 5$. Тогда $c(5) = 3 \cdot 31$, и, следовательно, $r \in \{3, 31\} \cap R_6(\varepsilon q) \subseteq \{31\}$. Значит, r может быть равно только 31. Согласно таблице 2 видим, что $\{r_5(\varepsilon q), r_6(\varepsilon q), r_7(\varepsilon q), r_8(\varepsilon q), r_9(\varepsilon q)\}$ – коклика в $GK(L)$. Из леммы 3.1 следует, что $r_5(\varepsilon q), r_7(\varepsilon q), r_8(\varepsilon q), r_9(\varepsilon q) \in \pi(S)$. Предположим, что $v \in R_8(\varepsilon q)$. Если $k_6(\varepsilon q) = 31^m$,

где m – положительное целое число, то из леммы 2.12 следует, что $m = 1$ и $\varepsilon q = 5$; противоречие с $(q - \varepsilon 1, 5) = 5$. Значит, существует $s \in R_6(\varepsilon q)$ такое, что $s \neq 31$. Мы уже знаем, что $(s, |\overline{G}/S|) = 1$. Лемма 4.1 влечет, что $(s, |K|) = 1$. Это означает, что $s \in \pi(S)$ и поэтому $t(v, S) \geq 5$. С другой стороны, $t(v, S) \leq 4$ согласно лемме 3.5; противоречие. Следовательно, $v \notin R_8(\varepsilon q)$. Значит, существует $r_8(\varepsilon q)$ такое, что $\varphi(r_8(\varepsilon q), S) \leq m/2$, поскольку в противном случае из леммы 4.2(а) следует, что r делит $k_8(\varepsilon q) - 1 = \frac{1}{2}(q^4 - 1)$, поэтому $i \neq 6$.

Предположим, что $n = 10$. Согласно таблице 3 используем $j_1 = 8, j_2 = 5$ и $j_3 = 10$. Легко видеть, что $\{r, r_8(\varepsilon q), r_5(\varepsilon q)\}$ и $\{r, r_8(\varepsilon q), r_{10}(\varepsilon q)\}$ – коклики в $GK(L)$. Поскольку $c(8) = 3, c(5) = 3 \cdot 31$ и $c(10) = 3 \cdot 7$, получаем, что $r \in \pi(3 \cdot 31) \cap \pi(3 \cdot 7) \cap R_6(\varepsilon q) = \emptyset$; противоречие.

Предположим, что $11 \leq n \leq 13$. Согласно таблице 3 используем $j_1 = 8, j_2 = 10$ и $j_3 = 11$. Легко видеть, что $\{r, r_8(\varepsilon q), r_{10}(\varepsilon q), r_{11}(\varepsilon q)\}$ – коклика в $GK(L)$. Заметим, что $c(8) = 3$. Теперь, если $(q + \varepsilon 1, 5) = 1$, то $d(10) = 1$ и $c(10) = 1$, поэтому $r \in \pi(3) \cap R_6(\varepsilon q) = \emptyset$; противоречие. Следовательно, получаем, что $(q + \varepsilon 1, 5) = 5$ и $c(10) = 3 \cdot 7$. Аналогично, если $(q - \varepsilon 1, 11) = 1$, то $d(11) = 1$ и $c(11) = 3$, поэтому $r \in \pi(3) \cap R_6(\varepsilon q) = \emptyset$. Следовательно, получаем, что $(q - \varepsilon 1, 11) = 1$ и $c(11) = 3 \cdot 7 \cdot 19$. Тогда $r \in \pi(3 \cdot 7) \cap \pi(3 \cdot 7 \cdot 19) \cap R_6(\varepsilon q) \subseteq \{7\}$. Это означает, что $r = 7$, как и было заявлено. Заметим, что $v \notin R_8(q)$, поскольку в противном случае лемма 3.1 влечет, что $t(v, S) \geq t(L) - 1 = 5$, а это неравенство противоречит лемме 3.5. Как и выше, видим, что из леммы 4.2(а) следует существование $r_8(\varepsilon q)$ такого, что $\varphi(r_8(\varepsilon q), S) \leq m/2$, что и требовалось доказать. \square

Предложение 4.4. Предположим, что L – симплектическая или ортогональная группа. Если $r_i = r_i(q) \in \pi(\overline{G}/S)$ и $3 \leq \eta(i) \leq n$, то выполняется одно из следующих утверждений.

- (а) $\eta(i) = 3$ и $n \geq 8$;
- (б) $i = 8$ и $n \geq 11$.

Доказательство. В случае симплектических и ортогональных групп рассуждаем аналогично доказательству предложения 4.3, в частности, используем те же обозначения для чисел $c(j)$ и $d(j)$, определяемых целым числом j . Для каждой пары (i, n) в таблице 4 приведены либо две пары целых чисел $(j_1, c(j_1))$ и $(j_2, c(j_2))$ такие, что $\{r_i, r_{j_1}(\varepsilon q), r_{j_2}(\varepsilon q)\}$ – коклика, и $\pi(c(j_1)c(j_2)) \cap R_i(\varepsilon q) = \emptyset$ либо три пары целых чисел $(j_1, c(j_1)), (j_2, c(j_2))$ и $(j_3, c(j_3))$ такие, что $\{r_i, r_{j_1}(\varepsilon q), r_{j_2}(\varepsilon q)\}$ и $\{r_i, r_{j_1}(\varepsilon q), r_{j_3}(\varepsilon q)\}$ являются кокликами в $GK(L)$ и $\pi(c(j_1)c(j_2)) \cap \pi(c(j_1)c(j_3)) \cap R_i(\varepsilon q) = \emptyset$. Если $n > 5$, то используются j_1, j_2, j_3 такие, что $\eta(j_1), \eta(j_2), \eta(j_3) < n$, это гарантирует, что $r_i \in \pi(L)$ для всех ортогональных и симплектических групп L с $\text{prk } L = n$. Если $n = 5$, мы иногда выбираем $j_2 = 5$ и $j_3 = 10$. Это возможно, поскольку $\text{prk } L = 5$ и $t(L) \geq 5$ влечет, что $L \in \{O_{11}(q), S_{10}(q)\}$ согласно таблице 2, поэтому $r_5(q), r_{10}(q) \in \pi(L)$. Для проверки несмежности двух простых чисел в $GK(L)$ можно воспользоваться леммой 3.2. Если $i = 3$ или $i = 6$, то рассматриваются только случаи $5 \leq n \leq 7$, если $i = 8$, то рассматриваются только случаи $5 \leq n \leq 10$. Для других значений i ограничений на n нет.

Имеется следующее отличие от случая линейных и унитарных групп. Предположим, что i делится на 4, j – степень нечетного простого числа s , и $u(x)\Phi_i(x) + v(x)(\Phi_j(x) - 1) = 1$ для многочленов $u(x), v(x) \in \mathbb{Q}[x]$. Из определения круговых многочленов следует, что $\Phi_i(\varepsilon q) = \Phi_i(-\varepsilon q)$ и $\Phi_j(\varepsilon q) = \Phi_{2j}(-\varepsilon q)$. С другой стороны, $k_j(\varepsilon q) = \frac{\Phi_j(\varepsilon q)}{(\varepsilon q - 1, s)}$ и $k_{2j}(\varepsilon q) =$

$\frac{\Phi_{2j}(\varepsilon q)}{(\varepsilon q+1, s)} = \frac{\Phi_j(-\varepsilon q)}{(\varepsilon q+1, s)}$. Очевидно, $(\varepsilon q - 1, s) = 1$ или $(\varepsilon q + 1, s) = 1$. В зависимости от этого мы выбираем j или $2j$ соответственно и записываем $(j^*, c(j))$ в таблицу 4. Это позволяет считать, что $d(j) = 1$. Аналогично, мы рассматриваем i и $2i$ одновременно, если i нечетно. Действительно, если есть равенство $u(x)\Phi_i(x) + v(c)(\frac{1}{d(j)}\Phi_j(x) - 1) = c(j)$, то оно выполняется как для q , так и для $-q$, то есть для $r_i(q)$ и $r_i(-q) \in R_{2i}(q)$. Это означает, что если мы записываем пару $(j, c(j))$, то мы используем $r_j(q)$ для $r_i(q)$ и $r_j(-q)$ для $r_{2i}(q)$.

Наконец, если $i \in \{20, 32, 11, 22, 13, 26, 15, 30, 17, 34\}$, то мы используем одинаковые числа j_1 и j_2 , поэтому значения $c(j_1)$ и $c(j_2)$ не указываются. Это означает, что в каждом случае $\pi(c(j_1)c(j_2)) \cap R_i(q) = \emptyset$, что гарантирует противоречие с существованием r . Явные многочлены $u(x)$ и $v(x)$ для всех случаев записаны в отдельные файлы для каждого i [27]. \square

Таблица 3: Индексы для линейных и унитарных групп

$r_4 :$	$n = 9, 10$	$n = 11, 12$	
$(j, c(j))$	$(7, 2 \cdot 5^2), (9, 2 \cdot 5)$	$(9, 2 \cdot 5), (11, 2 \cdot 61)$	
$r_5 :$	$n = 9, 10, 11$	$n = 12$	$n = 13$
$(j, c(j))$	$(8, 5), (7, 5 \cdot 311),$ $(9, 5 \cdot 11)$	$(8, 5), (12, 5)$	$(9, 5 \cdot 11), (12, 5)$
$(j, c(j))$	$n = 14, 15, 16$ $(12, 5),$ $(14, 5 \cdot 3011),$ $(13, 5 \cdot 11^2 \cdot 41)$	$n = 17, 18$ $(16, 5),$ $(14, 5 \cdot 3011),$ $(17, 5 \cdot 11 \cdot 31 \cdot 41)$	$n = 19, 20$ $(16, 5),$ $(18, 5 \cdot 31),$ $(19, 5 \cdot 11 \cdot 2251)$
$(j, c(j))$	$n = 21, 22$ $(21, 5 \cdot 11^2),$ $(18, 5 \cdot 31),$ $(19, 5 \cdot 11 \cdot 2251)$		
$r_6 :$	$n = 9$	$n = 10$	$11 \leq n \leq 13$
$(j, c(j))$	$(8, 3), (5, 3 \cdot 31)$	$(8, 3), (5, 3 \cdot 31),$ $(10, 3 \cdot 7)$	$(8, 3), (10, 3 \cdot 7),$ $(11, 3 \cdot 7 \cdot 19)$
$r_7 :$	$9 \leq n \leq 12$	$n = 13, 14$	$15 \leq n \leq 18$
$(j, c(j))$	$(8, 7), (6, 7 \cdot 127),$ $(9, 7 \cdot 43)$	$(8, 7), (12, 7)$	$(12, 7), (15, 2 \cdot 7)$
$(j, c(j))$	$19 \leq n \leq 21$ $(15, 2 \cdot 7), (16, 7)$	$22 \leq n \leq 24$ $(18, 7 \cdot 127),$ $(20, 7 \cdot 43 \cdot 197),$ $(19, 7 \cdot 1723 \cdot 3529)$	$n = 25, 26$ $(24, 7),$ $(20, 7 \cdot 43 \cdot 197),$ $(23, 7 \cdot 16968421)$
$r_8 :$	$9 \leq n \leq 10$	$11 \leq n \leq 16$	$17 \leq n \leq 19$
$(j, c(j))$	$(5, 2 \cdot 97), (6, 2 \cdot 17),$ $(7, 2 \cdot 1201)$	$(9, 2 \cdot 17), (10, 2 \cdot 97),$ $(11, 2 \cdot 3 \cdot 569)$	$(12, 2), (15, 2)$
$(j, c(j))$	$20 \leq n \leq 22$ $(15, 2), (18, 2 \cdot 17),$ $(19, 2 \cdot 41 \cdot 1289)$	$23 \leq n \leq 26$ $(21, 2 \cdot 5^2),$ $(22, 2 \cdot 3 \cdot 569),$ $(23, 2 \cdot 139921)$	
$r_9 :$	$9 \leq n \leq 12$	$13 \leq n \leq 19$	$20 \leq n \leq 23$

$(j, c(j))$	$(8, 3), (6, 3 \cdot 73),$ $(7, 3 \cdot 109 \cdot 127)$	$(12, 3),$ $(11, 3 \cdot 333667),$ $(13, 3 \cdot 440677)$	$(15, 3), (16, 3)$
$(j, c(j))$	$24 \leq n \leq 26$ $(20, 3 \cdot 4051),$ $(21, 3 \cdot 9811),$ $(24, 3)$		
$r_{10} :$	$10 \leq n \leq 14$	$15 \leq n \leq 21$	$22 \leq n \leq 24$
$(j, c(j))$	$(8, 5), (9, 5 \cdot 31),$ $(7, 5 \cdot 3011)$	$(12, 5), (15, 5)$	$(15, 5), (16, 5)$
$(j, c(j))$	$n = 25, 26$ $(18, 5 \cdot 11), (24, 5),$ $(23, 5 \cdot 71 \cdot 3301)$		
$r_{11} :$	$11 \leq n \leq 16$	$17 \leq n \leq 22$	$23 \leq n \leq 24$
$(j, c(j))$	$(8, 11), (9, 11 \cdot 683),$ $(10, 11 \cdot 23 \cdot 199 \cdot 463)$	$(12, 11), (16, 11)$	$(16, 11),$ $(18, 11 \cdot 23 \cdot 89),$ $(14, 11 \cdot 353 \cdot 361219)$
$(j, c(j))$	$n = 25, 26$ $(16, 11), (24, 11)$		
$r_{12} :$	$12 \leq n \leq 16$	$17 \leq n \leq 26$	
$(j, c(j))$	$(8, 3), (9, 2 \cdot 5)$	$(15, 3), (16, 3)$	
$r_{13}, r_{14},$ r_{15}, r_{17}	$13 \leq n \leq 19$	$20 \leq n \leq 24$	$n = 25, 26$
$(j, c(j))$	$(8, *), (12, *)$	$(12, *), (16, *)$	$(16, *), (24, *)$
$r_{16} :$	$16 \leq n \leq 21$	$22 \leq n \leq 26$	
$(j, c(j))$	$(12, 2), (15, 2 \cdot 17),$ $(10, 2 \cdot 7 \cdot 353)$	$(15, 2 \cdot 17), (20, 2 \cdot 97),$ $(18, 2 \cdot 257)$	
$r_{18}, r_{19},$ $r_{20}, r_{21},$ $r_{22}, r_{23},$ $r_{25}, r_{26} :$	$18 \leq n \leq 26$		
$(j, c(j))$	$(12, *), (16, *)$		
r_{24}	$24 \leq n \leq 26$		
$(j, c(j))$	$(15, 5), (16, 3)$		

Таблица 4: Индексы для симплектических и ортогональных групп

$r_3, r_6 :$	$n = 5, 6$	$n = 7$	
$(j, c(j))$	$(8, 3), (5, 3 \cdot 7),$ $(10, 3 \cdot 31)$	$(12, 3), (5, 3 \cdot 7),$ $(10, 3 \cdot 31)$	
$r_8 :$	$n = 5, 6$	$n = 7, 8$	$n = 9$
$(j, c(j))$	$(3^*, 2), (5^*, 2)$	$(12, 2), (5^*, 2)$	$(12, 2), (7^*, 2)$
$(j, c(j))$	$n = 10$ $(7^*, 2), (9^*, 2)$		
$r_5, r_{10} :$	$n = 5, 6$	$n = 7, 8$	$n = 9, 10$

$(j, c(j))$	$(8, 5), (3, 5 \cdot 11),$ $(6, 5 \cdot 31)$ $n = 11, 12$	$(8, 5), (12, 5)$ $n = 13$	$(12, 5), (16, 5)$ $n = 14$
$(j, c(j))$	$(16, 5), (9, 5 \cdot 11),$ $(18, 5 \cdot 31)$ $n = 15, 16$	$(24, 5), (9, 5 \cdot 11),$ $(18, 5 \cdot 31)$ $n = 17, 18$	$(24, 5), (20, 5 \cdot 421),$ $(13, 5 \cdot 11^2 \cdot 41)$
$(j, c(j))$	$(24, 5),$ $(28, 5)$	$(32, 5),$ $(28, 5)$	
r_{12}	$n = 6, 7, 8$	$n = 9, 10, 11, 12$	$n = 13, 14, 15, 16$
$(j, c(j))$	$(5^*, 3), (8, 3)$ $n = 17, 18$	$(7^*, 2), (16, 3)$	$(11^*, 1), (24, 3)$
$(j, c(j))$	$(32, 3), (30, 3)$		
$r_7, r_{14} :$	$n = 7, 8, 9$	$n = 10, 11, 12$	$n = 13, 14$
$(j, c(j))$	$(8, 7), (12, 7)$ $15 \leq n \leq 18$	$(12, 7), (16, 7)$	$(24, 7), (16, 7)$
$(j, c(j))$	$(28, 7), (24, 7)$		
r_{16}	$8 \leq n \leq 12$	$n = 13 \leq n \leq 18$	
(j, gcd)	$(12, 2), (7^*, 2)$	$(24, 2), (11^*, 2)$	
r_9, r_{18}	$9 \leq n \leq 13$	$n = 14 \leq n \leq 16$	$n = 17, 18$
$(j, c(j))$	$(12, 3), (16, 3)$	$(24, 3), (16, 3)$	$(32, 3), (24, 3)$
$r_{24}, r_{28},$ r_{36}	$12 \leq n \leq 18$		
$(j, c(j))$	$(16, 3 \cdot 7), (11^*, 1)$		
$r_{20}, r_{32},$ $r_{11}, r_{22},$ $r_{13}, r_{26},$ $r_{15}, r_{30},$ $r_{17}, r_{34},$	$10 \leq n \leq 13$	$n = 14 \leq n \leq 17$	$n = 18$
$(j, c(j))$	$(12, *), (16, *)$	$(16, *), (24, *)$	$(24, *), (28, *)$

Лемма 4.5. Предположим, что $r \in R_i(q)$, $\varphi(r, L) \geq 4$, если L – линейная или унитарная группа, и $\varphi(r, L) \geq 3$ в противном случае.

(а) Если r большое относительно L и делит $|\overline{G}/S|$, то $L = L_n^\varepsilon(q)$, $r \in R_6(\varepsilon q)$, и либо $r = 7$ и $11 \leq n \leq 12$, либо $r = 31$ и $n = 9$.

(б) Если r большое относительно L , то существует $s \in R_i(q)$ такое, что $s \notin \pi(\overline{G}/S)$.

(в) Если $r \in \pi(S)$, то $t(r, S) \geq t(r, L)$, в частности, $t(S) \geq t(L)$.

Доказательство. Предположим, что r является большим относительно L и делит $|\overline{G}/S|$. Если $L = L_n^\varepsilon(q)$, то, согласно таблице 2 получаем, что $n \geq 9$ и $\varphi(r, L) \geq n/2$. По предложению 4.3, находим, что $\varphi(r, L) = 6$ и либо $r = 7$ и $11 \leq n \leq 12$, либо $r = 31$ и $n = 9$. Если L – симплектическая или ортогональная группа, то согласно таблице 2 получаем, что $\eta(i) \geq 3$. По предложению 4.4 мы знаем, что либо $\eta(i) = 3$ и $n \geq 8$, либо $i = 8$ и $n \geq 11$. Используя таблицу 2, находим, что в этих случаях r мало относительно L ; противоречие.

Теперь докажем (б). Предположим, что r является большим относительно L . В силу (а) нам нужно рассмотреть только случаи, когда $L = L_n^\varepsilon(q)$, $\varphi(r, L) = 6$, и либо $r = 7$ и $11 \leq n \leq 12$, либо $r = 31$ и $n = 9$. Покажем, что существует $s \in R_6(\varepsilon q)$

такое, что $s \neq r$, и, следовательно, $s \notin \pi(\overline{G}/S)$ по предложению 4.3. Предположим противное, что $k_6(\varepsilon q) = r^m$, где $m \geq 1$. Из леммы 2.12 следует, что $(r, m, \varepsilon q) \in \{(7, 1, 5), (7, 1, 3), (7, 3, 19), (31, 1, -5)\}$. С другой стороны, по предложению 4.3(в),(г) верно, что $q \equiv \varepsilon 1 \pmod{5}$, если $r = 31$ и $q \equiv \varepsilon 1 \pmod{11}$, если $r = 7$; противоречие.

Предположим, что $r \in \pi(S)$. Покажем, что $t(r, S) \geq t(r, L)$. Рассмотрим $\{r\}$ -кокклику ρ в $GK(L)$ размера $t(r, L)$. Мы утверждаем, что каждый элемент из $\rho \setminus \{r\}$ является большим относительно L . Если r большое относительно L , это очевидно. Если $r = p$, то это верно по лемме 3.5(а). Пусть $r \neq p$ мало относительно L . Тогда $\varphi(r, L) < n/2$ по лемме 3.4(а). Заметим, что $p \notin \rho$ по лемме 3.5. Это означает, что если $s \in \rho \setminus \{r\}$, то $\varphi(s, L) > n/2$ по лемме 3.3(б), и, следовательно, s большое относительно L по лемме 3.4(а). Значит, имеем, что каждый элемент $\rho \setminus \{r\}$ является большим относительно L . Согласно таблице 2, видим, что если s является большим относительно L , то $\varphi(s, L) \geq 4$, если L – линейная или унитарная группа, и $\varphi(s, L) \geq 3$ в противном случае. По пункту (б) можно предполагать, что каждый элемент $\rho \setminus \{r\}$ не делит $|\overline{G}/S|$. Если $(\rho \setminus \{r\}) \cap \pi(K) = \emptyset$, то получаем, что $\rho \subseteq \pi(S)$ и поэтому $t(r, S) \geq t(r, L)$, что и требовалось показать. Остается рассмотреть случай, когда $(\rho \setminus \{r\}) \cap \pi(K) \neq \emptyset$. Тогда из леммы 4.1 следует, что $(\rho \setminus \{r\}) \cap \pi(K) = \{v\}$. Поскольку $v \in \pi(S)$, получаем, что $\rho \subseteq \pi(S)$, и, следовательно, $t(r, S) \geq t(r, L)$, как и утверждалось.

Поскольку $t(L) \geq 5$, лемма 3.1 влечет существование $r \in \pi(S)$, которое является большим относительно L . Используя пункт (в), получаем, что $t(S) \geq t(r, S) \geq t(r, L) = t(L)$. \square

По лемме 4.5 получаем, что $t(S) \geq t(L)$. В дальнейшем будем использовать этот факт, не упоминая лемму.

Лемма 4.6. Пусть r – простое число, большое относительно S . Если S – линейная или унитарная группа, то $\varphi(r, S) \geq t(L) \geq n/2$ и $r \geq n/2 + 1$. Если S – симплектическая или ортогональная группа, то $\varphi(r, S) \geq (2t(L) - 4)/3 \geq (n - 4)/3$ и $r > n/2$.

Доказательство. Если S линейная или унитарная, то из леммы 3.4(в) следует, что $\varphi(r, S) \geq t(S) \geq t(L) \geq n/2$. По лемме 3.6 получаем, что $r \geq \varphi(r, S) + 1 \geq n/2 + 1$. Если S симплектическая или ортогональная, то согласно таблице 2 получаем, что $\varphi(r, S) \geq 3$ и, следовательно, $r \geq 7$ по лемме 3.6. Из леммы 3.4(в) следует, что $\varphi(r, S) \geq (2t(S) - 4)/3 \geq (2t(L) - 4)/3 \geq (n - 4)/3$. Осталось показать, что $r > n/2$. Если $n \leq 13$, то $r \geq 7 > n/2$. Если $n \geq 14$, то лемма 3.6 влечет, что $r \geq 2\varphi(r, S) + 1 \geq (2n - 5)/3 > n/2$. \square

Определение 4.7. Будем говорить, что натуральное число j является J -индексом (относительно G), если оно удовлетворяет следующим условиям.

(а) Каждое число $r \in R_j(u)$ является большим относительно S и делит $|\overline{G}/S| \cdot |K|$.

(б) Если $t(S) > t(L)$ и каждая кокклика ρ наибольшего размера в $GK(L)$ содержит простое число s такое, что $s \in \pi(S)$ и $\varphi(s, S) \leq m/2$, то $\varphi(r, S) > m/2$ для всех $r \in R_j(u)$.

Следующие три леммы являются аналогами [6, леммы 6.1, 6.2, 6.4] соответственно.

Лемма 4.8. Существует множество M натуральных чисел размера $t(S) - t(L)$ такое, что каждый элемент из M является J -индексом.

Доказательство. Можно считать, что $t(S) > t(L)$. Обозначим $t = t(S)$ и $\ell = t(L)$. Рассмотрим кокклику $\rho = \{r_{i_1}(u), \dots, r_{i_t}(u)\}$ размера t в $GK(S)$. Предположим, что существует $\ell + 1$ индекс $i \in I = \{i_1, \dots, i_t\}$ такие, что некоторое числа $r_i \in R_i(u)$ взаимно просты с $|K| \cdot |\overline{G}/S|$. Тогда соответствующие $\ell + 1$ простых чисел r_i образуют кокклику

размера $\ell + 1$ в $GK(L)$; противоречие. Следовательно, существует подмножество M множества I , содержащее не менее $t - \ell$ элементов и такое, что если $i \in M$, то каждое число $r_i(u) \in R_i(u)$ делит $|K| \cdot |\overline{G}/S|$. Покажем, что множество M можно выбрать так, чтобы каждый его элемент удовлетворял второму условию определения 4.7.

Предположим, что каждая коклика наибольшего размера в $GK(L)$ содержит простое число s с $\varphi(s, S) \leq m/2$. Из леммы 3.3(б) следует, что множество I включает в себя подмножество I' размера не менее $t - 1$ такое, что для любого простого числа $r \in R_i(u)$ с $i \in I'$ выполняется неравенство $\varphi(r, S) > m/2$. Если $I' = I$, то мы можем взять M , как и выше. Поэтому можно считать, что $|I'| = t - 1$. Предположим, что существуют ℓ чисел $i \in I'$ с $\tilde{R}_i(u) = R_i(u) \setminus (\pi(K) \cup \pi(\overline{G}/S)) \neq \emptyset$. Тогда множество ρ , состоящее из ℓ простых чисел из различных $\tilde{R}_i(u)$, образует коклику в $GK(L)$, которая не содержит простого числа s с $\varphi(s, S) \leq m/2$; противоречие. Таким образом, существует подмножество M множества I' такое, что $|M| = t - 1 - (\ell - 1) = t - \ell \geq 1$, и для любого $j \in M$ каждое простое число r из $R_j(u)$ является большим относительно S , делит $|\overline{G}/S| \cdot |K|$ и удовлетворяет условию $\varphi(r, S) > m/2$. Лемма доказана. \square

Лемма 4.9. Предположим, что j – это J -индекс. Тогда для любого $r \in R_j(u)$ существует большое относительно L простое число s такое, что $rs \in \omega(L) \setminus \omega(S)$ и $s \notin \pi(\overline{G}/S)$.

Доказательство. Обозначим $\ell = t(L)$ и $t = t(S)$. Зафиксируем $r \in R_j(u)$. Пусть $\rho = \{s_1, \dots, s_\ell\}$ – коклика размера ℓ в $GK(L)$. По леммам 4.1 и 4.5(б) можно считать, что каждое простое число из ρ не делит $|\overline{G}/S| \cdot |K|$. Заметим, что $v \notin \rho$, так как $t(L) \geq 5$. Пусть $\tau = -$, если S – унитарная группа, иначе положим $\tau = +$. Обозначим $I = \{e(s, \tau u) \mid s \in \rho\}$. Тогда $j' = e(r, \tau u) \notin I$, поскольку каждый элемент из $R_j(u)$ делит произведение $|\overline{G}/S| \cdot |K|$.

Выберем коклику σ размера t в $GK(S)$, содержащую r , и положим $Y = \{e(w, \tau u) \mid w \in \sigma\}$.

Если $t = \ell$, то ρ также является кокликой наибольшего размера в $GK(S)$. Лемма 3.8 влечет, что $I \cap Y = Y \setminus \{j'\}$. Следовательно, ρ содержит подмножество ρ' размера $\ell - 1$ такое, что множество $M = \{r\} \cup \rho'$ является кокликой в $GK(S)$. Если r мало относительно L , то M не может быть кокликой в $GK(L)$, поскольку $|M| = \ell$. Следовательно, существует $s \in \rho$ с $rs \in \omega(L) \setminus \omega(S)$. Теперь покажем, что r не может быть большим относительно L . Предположим от противного, что r таково. Тогда из леммы 4.5 следует, что $L = L_n^\varepsilon(q)$, где $\varepsilon \in \{+, -\}$, $r \in R_6(\varepsilon q)$ и либо $11 \leq n \leq 12$ и $r = 7$, либо $n = 9$ и $r = 31$. Поскольку $\rho \cup \{r\}$ не является кокликой в $GK(S)$, заключаем, что r смежно с некоторым $s \in \rho$ в $GK(S)$. Согласно таблице 2 верно, что $s \in R_6(\varepsilon q) \cup R_{12}(\varepsilon q)$. Поскольку $j' \notin I$, получаем, что $e(s, u) \neq j$. Поскольку r и s смежны в $GK(S)$, из леммы 3.3(в) следует, что $\varphi(r, S) \leq m/2$ или $\varphi(s, S) \leq m/2$. По предложению 4.3(в),(г) существует число $r_8(\varepsilon q) \in R_8(\varepsilon q)$ такое, что $\varphi(r_8(\varepsilon q), S) \leq m/2$. По лемме 3.3(б) получаем, что $rr_8(\varepsilon q) \in \omega(S) \setminus \omega(L)$ или $sr_8(\varepsilon q) \in \omega(S) \setminus \omega(L)$; противоречие. Таким образом, можно считать, что $t > \ell$.

Предположим, что $\varphi(r, S) > m/2$. По лемме 3.3(б) множество ρ содержит подмножество ρ' размера $\ell - 1$, такое, что $\varphi(s, S) > m/2$ для любого $s \in \rho'$. Поскольку $j' \notin I$, из леммы 3.3(в) следует, что $\{r\} \cup \rho'$ – коклика в $GK(S)$. Если r мало относительно L , то $\{r\} \cup \rho'$ не является кокликой в $GK(L)$, поэтому утверждение леммы в этом случае выполняется. Следовательно, можно считать, что r большое относительно L , и $\{r\} \cup \rho'$ – коклика в $GK(L)$. По лемме 4.5(а) получаем, что $L = L_n^\varepsilon(q)$, где $\varepsilon \in \{+, -\}$, $n \leq 12$ и

$r \in R_6(\varepsilon q)$. Мы знаем, что $|\{r\} \cup \rho'| = \ell$. Согласно таблице 2 получаем, что $r_8(\varepsilon q) \in \rho'$, поэтому $t(r_8(\varepsilon q), S) > m/2$. Это противоречит предложению 4.3(в),(г).

Пусть теперь $\varphi(r, S) \leq m/2$. Предположим, что r является большим относительно L . Тогда получаем, что $L = L_n^\varepsilon(q)$, где $\varepsilon \in \{+, -\}$ и $n \leq 12$, $r \in R_6(\varepsilon q)$ и $\varphi(r_8(\varepsilon q), S) \leq m/2$ для хотя бы одного $r_8(\varepsilon q)$. Из леммы 3.3(в) следует, что $rr_8(\varepsilon q) \in \omega(S) \setminus \omega(L)$; противоречие. Значит, r мало относительно L . По определению J -индекса множество ρ можно выбрать таким образом, что либо $\varphi(s, S) > m/2$ для любого $s \in \rho$, либо некоторое $s \in \rho$ не принадлежит $\pi(S)$. Рассмотрим первый случай. Используя таблицу 2, видим, что существует коклика σ' наибольшего размера в $GK(S)$ с $\rho \subseteq \sigma'$. Положим $X = \{e(w, \tau u) \mid w \in \sigma'\}$. Применяя лемму 3.8, получаем, что $Y \cap X \supseteq Y \setminus \{j'\}$. Следовательно, ρ включает подмножество ρ' размера $\ell - 1$ такое, что $\{r\} \cup \rho'$ является кокликкой в $GK(S)$ и не является кокликкой в $GK(L)$. Значит найдется число $s \in \rho'$ такое, что $rs \in \omega(L) \setminus \omega(S)$. Если $s \notin \pi(\overline{G}/S)$, то оно является требуемым числом. Пусть теперь $s \in \pi(\overline{G}/S)$. Тогда получаем, что $L = L_n^\varepsilon(q)$, где $s \in R_6(\varepsilon q)$, и либо $n = 9$, либо $11 \leq n \leq 12$. Более того, существует число $r_8 \in R_8(\varepsilon q)$ такое, что $\varphi(r_8, S) \leq m/2$. Следовательно, r смежно с $r_8(\varepsilon q)$ и $r_6(\varepsilon q)$ в $GK(L)$. Используя критерий смежности в $GK(L)$, находим, что если $n = 9$, то $r \in \{p, r_1(\varepsilon q), r_2(\varepsilon q)\}$ и поэтому r смежно с $r_5(\varepsilon q)$ и $r_7(\varepsilon q)$ в $GK(L)$. Таким образом, хотя бы одно из чисел $r_5(\varepsilon q)$ и $r_7(\varepsilon q)$ принадлежит ρ' и является требуемым. Аналогично, если $n = 11, 12$, то $r \in \{p, r_1, r_2, r_3, r_4\}$, поэтому r смежно с $r_7(\varepsilon q)$ и $r_8(\varepsilon q)$, хотя бы одно из которых принадлежит ρ' .

Наконец, предположим, что существует коклика ρ в $GK(L)$ размера ℓ такая, что для некоторого $s \in \rho$ верно, что $s \notin \pi(S)$. Из лемм 4.1 и 4.5 получаем, что $L = L_n^\varepsilon(q)$, где $s \in R_6(\varepsilon q)$, и либо $n = 9$, либо $11 \leq n \leq 12$. Более того, мы знаем, что существует $r_8 \in R_8(\varepsilon q)$ такое, что $\varphi(r_8, S) \leq m/2$ по предложению 4.3(в),(г). Поскольку $\varphi(r_8, S) \leq m/2$ и $\varphi(r, S) \leq m/2$, по лемме 3.3(б) получаем $rr_8 \in \omega(S)$. Это означает, что либо $r = p$, либо $\varphi(r, L) \in \{1, 2, 4\}$, если $n = 9$, и $\varphi(r, L) \in \{1, 2, 3, 4\}$, если $n = 11, 12$. По лемме 3.1 находим, что $r \notin R_4(\varepsilon q)$, если $n = 9$, поскольку $\{r_4(\varepsilon q), r_6(\varepsilon q), r_7(\varepsilon q)\}$ – коклика в $GK(L_9^\varepsilon(q))$. Из леммы 4.5 следует, что можно выбрать $r_6 \in R_6(\varepsilon q)$ и $r_7 \in R_7(\varepsilon q)$ таким образом, что $(r_6 r_7, |K| \cdot |\overline{G}/S|) = 1$. Поскольку $\varphi(r_8, S) \leq m/2$, из леммы 3.3(б) следует, что $\varphi(r_6, S) > m/2$ и $\varphi(r_7, S) > m/2$. По лемме 3.4(а) получаем, что r_6 и r_7 являются большими относительно S . Используя [23, таблица 4] и лемму 3.2, получаем, что r смежно как с r_6 , так и с r_7 в $GK(L)$. Если $rr_7, rr_6 \in \omega(S)$, то из леммы 3.8 следует, что $e(r_6, \tau u), e(r_7, \tau u) \in J(S) \setminus E(S)$, и, следовательно, r_6 и r_7 смежны в $GK(S)$; противоречие. Значит, $rr_7 \in \omega(L) \setminus \omega(S)$ или $rr_6 \in \omega(L) \setminus \omega(S)$. Лемма доказана. \square

Лемма 4.10. Предположим, что $r \in R_j(u)$, где j – это J -индекс. Тогда выполняется одно из следующих утверждений.

- (а) $k_j(u)$ делит $(q^2 - 1) \log_v u$.
- (б) $k_j(u)$ делит $p(q^2 - 1) \log_v u$, и p делит $k_j(u)$ и $\log_v u$.
- (в) $k_j(u)$ делит $p(q^2 - 1)$, при этом $p < 31$.

Доказательство. Положим $(k_j(u))_{\{r\}} = r^\gamma$. Поскольку r является большим относительно S , находим, что $r \geq 5$ и $r \neq v$. Применяя лемму 2.5, получаем, что $r^\gamma = \exp_r(S)$.

Предположим, что r делит $|K|$. Поскольку $r \neq v$, из леммы 4.1 следует, что r делит $p(q^2 - 1)$ и $t(r, L) = 2$. Равенство $t(r, L) = 2$ влечет, что r мало относительно L . По [6, лемма 2.10(б)] существует $s \in \pi(L) \setminus \{r, p\}$ такое, что s и r не смежны в $GK(L)$. Используя леммы 3.4(а) и 3.3(б), получаем, что s большое относительно L . По лемме 4.5(б),(в) можно считать, что $s \in \pi(S)$ и $t(s, S) \geq 5$. Следовательно, $s \neq v$ по лемме 3.5. Теперь

[22 лемма 2.16] влечет, что s не делит порядки собственных параболических подгрупп группы S . По лемме 3.11 существует собственная параболическая подгруппа P группы S такая, что $r^\gamma \in \omega(P)$. Если R – силовская r -подгруппа группы K (напомним, что K нильпотентна), то S действует на $R/\Phi(R)$ сопряжением. Это действие должно быть точным, поскольку r и s несмежны. Более того, поскольку r большое относительно S , имеем $(r, 6u(u^2 - 1)) = 1$. Применяя лемму 3.12, получаем $r^{\gamma+1} \in \omega(G) = \omega(L)$.

По лемме 4.6 получаем неравенство $r > n/2$. Предположим, что $r = p$. Поскольку $t(p, L) = 2$, из леммы 3.5 следует, что $L \in \{O_{2n+1}(q), S_{2n}(q)\}$, где n – четное число. По предположению $t(L) \leq 13$ и $n \neq 16$, поэтому $n \leq 14$ согласно таблице 2. Мы знаем, что $p^2 \in \omega(L)$, поэтому $p < 29$ по лемме 2.13. Поскольку $n^2/4 > 2n-1$ при $n \geq 8$ и $5^2 > 2 \cdot 8 - 1$, то $p^2 > 2n - 1$. Из леммы 2.13 следует, что $\text{exp}_p(L)$ не превосходит p^2 . Тогда $p^2 \geq p^{\gamma+1}$, откуда $k_j(u)_{\{p\}} \leq p$. Следовательно, $k_j(u)_{\{r\}}$ делит p в этом случае. Предположим, что r делит $(q^2 - 1)$ и положим $(q^2 - 1)_{\{r\}} = r^\delta$. Используя неравенство $r > n/2$ и лемму 2.5, получаем, что $\text{exp}_r(L)$ не превосходит $r^{\delta+1}$. Следовательно, $r^{\delta+1} \geq r^{\gamma+1}$. Таким образом, для любого $j \in J$ и любого $r \in R_j(u) \cap \pi(K)$ число $(k_j(u))_{\{r\}}$ делит $p(q^2 - 1)$, а если $p \in R_j(u)$, то $p < 31$.

Предположим теперь, что r не делит $|K|$. Тогда $|\overline{G}/S|_{\{r\}} = r^\kappa > 1$. Следовательно, \overline{G} содержит подгруппу, изоморфную расширению S посредством автоморфизма τ порядка r^κ , где $\kappa \geq 1$. Поскольку r нечетно и взаимно просто с $|\text{Inndiag}(S)/S|$, можно считать, что τ – полевой автоморфизм. Если $u = v^\beta$ и $\beta = r^\mu \cdot l$, где $(r, l) = 1$, то $\mu \geq \kappa \geq 1$. Если r не делит $v^{lj} - 1$, то r не делит $v^{r^\mu \cdot lj} - 1 = u^j - 1$, что неверно. Следовательно, $r^\gamma = (k_j(u))_{\{r\}} = (u^j - 1)_{\{r\}} = (v^{r^\mu \cdot lj} - 1)_{\{r\}} = r^\mu (v^{lj} - 1)_{\{r\}} > r^\kappa$ по лемме 2.5. Кроме того, r^γ – это наибольшая степень числа r , лежащая в $\omega(S)$. В силу [6, лемма 3.10] получаем, что r^γ равно $\text{exp}_r(\overline{G})$, значит, и $\text{exp}_r(G)$. Если $r \neq p$ и $k = e(r, q) \geq 3$, то неравенство $r > n/2$ влечет, что $(q^k - 1)_{\{r\}}$ равно $\text{exp}_r(L)$. По лемме 4.9 существует большое относительно L простое число s такое, что $rs \in \omega(L) \setminus \omega(S)$ и $s \notin \pi(\overline{G}/S)$. Лемма 4.1 влечет, что $s \notin \pi(K)$. Из леммы 3.10 следует, что $r^\gamma s \in \omega(L)$. Поскольку $(rs, |K|) = 1$, группа \overline{G} содержит элемент x порядка $r^\gamma s$. Тогда элемент $y = x^{r^\kappa}$ имеет порядок $r^{\gamma-\kappa} s$ и принадлежит S , что невозможно, поскольку $\gamma > \kappa$. Таким образом, r делит $p(q^2 - 1)$.

Если r делит $q^2 - 1$, то снова неравенство $r > n/2$ и лемма 2.5 влекут, что $r^\gamma \leq r(q^2 - 1)_{\{r\}}$. Предположим, что $r = p$, в частности, p делит $\log_v u$. Заметим, что число $\text{exp}_p(L)$ не превосходит p^2 , поскольку $p > n/2$ и $r \geq 5$. Поскольку произведение различных простых чисел из $R_j(u)$, делящих $|\overline{G}/S|$, делит число $\log_v u$, получаем, что $k_j(u)$ делит $p(q^2 - 1) \log_v u$. \square

Лемма 4.11. Пусть $d = t(S) - t(L)$ и $d > 0$. Предположим, что $t(S) \geq 7$, и S содержит элемент порядка, большего q^α , где $\alpha > 2$. Тогда справедливы следующие утверждения.

- (а) $u^{3d} < q^2$.
- (б) $d < \frac{4t(L)}{3(\alpha-2)}$.

Доказательство. По лемме 4.8 существует множество M натуральных чисел такое, что $|M| = d$ и каждый элемент M является J -индексом. Поскольку $t(S) \geq 7$, находим, что $\varphi(j) \geq 4$ для каждого $j \in J$ согласно таблице 2. В силу лемм 4.10 и 2.10 получаем, что $u^{3d} < q^2$.

Из леммы 3.7 следует неравенство $q^\alpha < \frac{u}{u-1} u^m \leq u^{m+1}$. Это означает, что $u^{(3\alpha d)/2} < u^{m+1}$. Предположим, что $\alpha \geq 2 + \frac{4t(L)}{3d}$. Тогда $u^{3d+2t(L)} < u^{m+1}$. Следовательно, $m \geq 3d + 2t(L) = d + 2t(S)$ и поэтому $t(S) \leq (m - 1)/2$. Согласно таблице 2 получаем, что

$t(S) \geq \frac{m}{2}$, если S – линейная или унитарная группа, и $t(S) \geq \frac{3m-2}{4} > \frac{m-1}{2}$, если S – симплектическая или ортогональная группа; противоречие. Таким образом, получаем, что $\alpha < 2 + \frac{4t(L)}{3d}$, и, следовательно, $d < \frac{4t(L)}{3(\alpha-2)}$. \square

Теперь мы готовы доказать теорему 3.

Доказательство теоремы 3. Обозначим $d = t(S) - t(L)$. Напомним, что $d \geq 0$. Можно считать, что $d \geq 1$, иначе доказывать нечего.

Предположим, что L – линейная или унитарная группа и $t(L) \geq 6$. Пусть j – наибольшее простое число, меньшее или равное n . Легко видеть, что $j > n/2$ и, следовательно, $r_j(\varepsilon q)$ большое относительно L согласно таблице 2. По предложению 4.3 и лемме 4.1 получаем, что $k_j(\varepsilon q) \in \omega(S)$. По лемме 2.6 мы знаем, что $k_j(\varepsilon q) > q^{j-2}$. Следовательно, по лемме 4.11 получаем, что $d < \frac{4t(L)}{3(j-4)}$, если $t(S) \geq 7$. Если $23 \leq n \leq 26$, то $t(L) \leq 13$ и $j \geq 23$, поэтому находим, что $d < \frac{18}{19} < 1$. Если $19 \leq n \leq 22$, то $t(L) \leq 11$ и $j \geq 19$, поэтому $d < \frac{14.7}{15} < 1$. Аналогично, если $17 \leq n \leq 18$, то $t(L) \leq 9$ и $j = 17$, поэтому получаем, что $d < \frac{12}{13} < 1$. Пусть теперь $13 \leq n \leq 16$. Тогда $t(L) \leq 8$ и $j = 13$, поэтому $d < \frac{11}{9} < 2$. Если $11 \leq n \leq 12$, то $t(L) = 6$, $t(S) \geq 7$ и $j = 11$, следовательно $d < \frac{8}{7} < 2$. Осталось рассмотреть случай $d = 1$, если $6 \leq t(L) \leq 8$. В этом случае из лемм 4.10 и 2.9 следует, что $2u^3 < q^2$. Как и выше, возьмем наибольшее простое число j , меньшее или равное n . Используя равенство (1), находим, что $k_j(\varepsilon q) \geq \frac{q-1}{qj} q^{j-1}$. Из леммы 3.7 следует, что $q^{j-1} < j \frac{q}{q-1} \frac{u}{u-1} u^{\text{prk} S}$. Поскольку $q \geq 3$ и $u \geq 2$, получаем неравенство $q^{j-1} < 3ju^{\text{prk} S}$. Если $t(L) = 8$, то $j = 13$ и $\text{prk} S \leq 18$, поэтому $q^{12} < 39u^{18}$; противоречие с $2u^3 < q^2$. Если $t(L) = 7$, то $j = 13$ и $\text{prk} S \leq 16$, поэтому $q^{12} < 39u^{16}$; противоречие с $2u^3 < q^2$. Наконец, если $t(L) = 6$, то $j = 11$ и $\text{prk} S \leq 14$, значит, $q^{10} < 33u^{14}$; противоречие с $2u^3 < q^2$.

Предположим, что L – линейная или унитарная группа и $t(L) = 5$. Тогда $9 \leq n \leq 10$. Согласно таблице 2 видим, что $r_9(\varepsilon q)$ и $r_7(\varepsilon q)$ большие относительно S . Из предложения 4.3 и леммы 4.1 следует, что $k_9(\varepsilon q), k_7(\varepsilon q) \in \omega(S)$. По лемме 2.7 находим, что $\omega(S)$ содержит элемент, больший $q^{5.5}$. Предположим, что $d \geq 2$, поэтому $t(S) \geq 7$. Тогда из леммы 4.11 следует, что $d < \frac{6.7}{3.5} < 2$; противоречие. Значит, в этом случае $d \leq 1$. Это завершает рассмотрение случая линейных и унитарных групп.

Предположим, что L – симплектическая или ортогональная группа. Пусть сначала $11 \leq t(L) \leq 13$. Согласно таблице 2 видим, что $k_{13}(q) \in \omega(L)$. По лемме 2.6 мы знаем, что $k_{13}(q) > q^{11}$. Из предложения 4.4 и леммы 4.1 следует, что $\omega(S)$ содержит элемент, больший q^{11} . Используя лемму 4.11, получаем, что $d < \frac{17.4}{9} < 2$. Если $9 \leq t(L) \leq 10$, то $k_{11}(q) \in \omega(L)$ или $k_{11}(-q) \in \omega(L)$ согласно таблице 2. По лемме 2.6 оба этих числа больше q^9 . Из предложения 4.4 и леммы 4.1 следует, что $\omega(S)$ содержит элемент, больший q^9 . По лемме 4.11 верно неравенство $d < \frac{13.4}{7} < 2$. Если $7 \leq t(L) \leq 8$, то $k_{16}(q) \in \omega(L)$ согласно таблице 2. Заметим, что $k_{16}(q) = \frac{1}{2}(q^8 + 1) > q^{7.35}$, поскольку $3^{0.65} > 2$. Из предложения 4.4 и леммы 4.1 следует, что $\omega(S)$ содержит элемент, больший $q^{7.35}$. Используя лемму 4.11, получаем, что $d < \frac{10.7}{5.35} = 2$. Предположим, что $t(L) = 6$. Тогда видим, что $k_7(q) \in \omega(L)$ или $k_{14}(q) \in \omega(L)$ согласно таблице 2. Используя лемму 2.6, получаем, что $\omega(S)$ содержит элемент, больший q^5 . Из леммы 4.11 следует, что $d < \frac{8}{3} < 3$. Предположим, что $t(L) = 5$. Тогда видим, что $k_8(q) \in \omega(L)$. Заметим, что $k_8(q) = (q^4 + 1)/2 > q^{3.35}$. Это означает, что $\omega(S)$ содержит элемент, больший $q^{3.35}$. Из леммы 4.11 следует, что $d < \frac{6.7}{1.35} < 5$. Предположим, что $d = 4$. Тогда по лемме 4.11 мы знаем, что $u^{12} < q^2$. Поскольку $k_8(q) \in \omega(S)$, лемма 3.7 влечет, что $(u^{24} + 1)/2 < (q^4 + 1)/2 = k_8(q) \leq$

$2u^{\text{prk } S}$. Согласно таблице 2 получаем, что $\text{prk } S \leq 18$. Следовательно, верно неравенство $u^{24} + 1 < 4u^{18}$; противоречие. Предположим, что $d = 3$. Тогда $u^9 < q^2$ по лемме 4.11. Поскольку $k_8(q) \in \omega(S)$, лемма 3.7 влечет, что $(u^{18} + 1)/2 < (q^4 + 1)/2 = k_8(q) \leq 2u^{\text{prk } S}$. Согласно таблице 2 видим, что $\text{prk } S \leq 16$. Следовательно, получаем неравенство $u^{18} + 1 < 4u^{16}$; противоречие с $u \geq 2$. Значит, в этом случае имеем неравенство $d \leq 2$. Это завершает рассмотрение случая ортогональных и симплектических групп. \square

5 Доказательство теоремы 2

В этом разделе мы докажем теорему 2. Предположим, что L изоморфна $L_n(q)$ или $U_n(q)$, где q нечетно и $12 \leq n \leq 26$. Это означает, что $6 \leq t(L) \leq 13$. Если G – группа, изоспектральная L , то, как и в предыдущем разделе, получаем, что существует неабелева простая группа S , такая, что $S \leq \overline{G} = G/K \leq \text{Aut } S$ для максимальной нормальной разрешимой подгруппы K группы G . Предположим, что S – простая классическая группа над полем порядка u , взаимно простого с q . В силу теоремы 3 получаем, что $0 \leq t(S) - t(L) \leq 1$. Чтобы использовать множество $J(S)$, положим $\nu = -$, если S – унитарная группа, иначе определим $\nu = +$. Мы фиксируем эти обозначения и ограничения на протяжении этого раздела. Отметим, что ограничения в этом разделе строже, чем в предыдущем, поэтому мы можем использовать все результаты раздела 4. По [5, теорема 1] можно считать, что n не является простым числом.

Лемма 5.1. Предположим, что $t(L) = t(S)$.

(а) Если $(n, i) \neq (12, 6)$ и $r_i(\varepsilon q)$ лежит в $\pi(S)$ и большое относительно L , то $r_i(\varepsilon q)$ большое относительно S , и либо $k_i(\varepsilon q)$ делит $k_j(u)$ для некоторого целого числа j , либо $k_i(\varepsilon q)$ делит $k_{j_1}(\nu u)k_{j_2}(\nu u)$, где $j_1, j_2 \in J(S) \setminus E(S)$.

(б) Если не существует J -индексов относительно G и L , то $|J(S) \setminus E(S)| \leq 2$.

Доказательство. Предположим, что $(n, i) \neq (12, 6)$ и $r_i(\varepsilon q)$ большое относительно L . По леммам 4.5 и 4.1 получаем, что каждый элемент $r_i(\varepsilon q)$ взаимно прост с $|\overline{G}/S| \cdot |K|$ и $t(r_i(\varepsilon q), S) \geq t(r_i(\varepsilon q), L) = t(S)$. Следовательно, $r_i(\varepsilon q)$ является большим относительно S . Поскольку любые два элемента из $R_i(\varepsilon q)$ смежны в $GK(S)$ и большие относительно S , то либо существует целое число j такое, что $R_i(\varepsilon q) \subseteq R_j(u)$, либо $R_i(\varepsilon q) \subseteq \bigcup_{j \in J(S) \setminus E(S)} R_j(\nu u)$. В первом случае получаем, что $k_i(\varepsilon q)$ делит $k_j(u)$. Во втором случае

предположим, что существуют три различных целых числа $j_1, j_2, j_3 \in J(S) \setminus E(S)$, такие, что некоторые $r_{j_1}(\nu u), r_{j_2}(\nu u), r_{j_3}(\nu u)$ принадлежат $R_i(\varepsilon q)$. Тогда $r_{j_1}(\nu u)r_{j_2}(\nu u)r_{j_3}(\nu u)$ делит $k_i(\varepsilon q)$ и, следовательно, $r_{j_1}(\nu u)r_{j_2}(\nu u)r_{j_3}(\nu u) \in \omega(S)$. Используя таблицу 2, видим, что либо $S \in \{S_{2m}(u), O_{2m+1}(u)\}$, где $m \equiv 3 \pmod{4}$ и $\{j_1, j_2, j_3\} = \{\frac{m-1}{2}, m-1, m+1\}$, либо $S = O_{2m}^-(u)$, где $m \equiv 2 \pmod{4}$ и $\{j_1, j_2, j_3\} = \{\frac{m}{2}, m-2, m\}$. В обоих случаях находим, что $r_{j_1}(u)r_{j_2}(u)r_{j_3}(u) \notin \omega(S)$ по [28, следствия 2, 3] и [28, следствия 4, 8, 9] соответственно; противоречие. Это означает, что либо $R_i(\varepsilon q) \subseteq R_j(\nu u)$, где $j \in J(S) \setminus E(S)$, либо $R_i(\varepsilon q) \subseteq R_{j_1}(\nu u) \cup R_{j_2}(\nu u)$, где $j_1, j_2 \in J(S) \setminus E(S)$. Значит, приходим к выводу, что $k_i(\varepsilon q)$ делит $k_j(\nu u)$ или $k_{j_1}(\nu u)k_{j_2}(\nu u)$ соответственно.

Предположим, что не существует J -индексов и $|J(S) \setminus E(S)| \geq 3$. Из определения 4.7 получаем, что для каждого $j \in J(S)$ существует число $r_j(\nu u) \in R_j(\nu u)$, взаимно простое с $|K| \cdot |\overline{G}/S|$. Поскольку $t(L) = t(S)$, получаем, что каждое $r_j(\nu u)$ является большим относительно L . Выберем различные числа $j_1, j_2, j_3 \in J(S) \setminus E(S)$. Как и выше, видим, что $r_{j_1}(\nu u)r_{j_2}(\nu u)r_{j_3}(\nu u) \notin \omega(S)$. С другой стороны, простые числа $r_{j_1}(\nu u), r_{j_2}(\nu u)$ и $r_{j_3}(\nu u)$

попарно смежны в $GK(S)$ и, следовательно, попарно смежны в $GK(L)$. Согласно таблице 2 видим, что либо существует целое число i такое, что $r_{j_1}(\nu u), r_{j_2}(\nu u), r_{j_3}(\nu u) \in R_i(\varepsilon q)$, либо n четно и $r_{j_1}(\nu u), r_{j_2}(\nu u), r_{j_3}(\nu u) \in R_{n/2}(\varepsilon q) \cup R_n(\varepsilon q)$. Тогда $r_{j_1}(\nu u)r_{j_2}(\nu u)r_{j_3}(\nu u)$ делит $k_i(\varepsilon q)$ или $k_{n/2}(\varepsilon q)k_n(\varepsilon q)$. Заметим, что $k_{n/2}(\varepsilon q)k_n(\varepsilon q) \in \omega(L)$ по лемме 3.10. Следовательно, получаем, что $r_{j_1}(\nu u)r_{j_2}(\nu u)r_{j_3}(\nu u) \in \omega(S)$; противоречие. \square

Лемма 5.2. Предположим, что $t(L) = t(S)$ и $S = L_m^\tau(u)$, где $\tau \in \{+, -\}$. Тогда $m \geq n$.

Доказательство. Предположим от противного, что $m < n$. Тогда $n = 2s$ и $m = 2s - 1$ для целого числа $s \geq 6$. Заметим, что $r_s(\varepsilon q)$ и $r_{2s}(\varepsilon q)$ смежны в $GK(L)$. Поскольку $r_s(\varepsilon q)$ и $r_{2s}(\varepsilon q)$ большие относительно L , в силу лемм 4.5 и 4.1 можно предполагать, что $r_s(\varepsilon q)$ и $r_{2s}(\varepsilon q)$ взаимно просты с $|\overline{G}| \cdot |K|$ и большие относительно S . Согласно таблице 2 видим, что $J(S) = E(S)$, поэтому существует целое число $j > 2$ такое, что $r_s(\varepsilon q), r_{2s}(\varepsilon q) \in R_j(u)$. Положим $r = r_{s-1}(\varepsilon q)$, если $s \neq 7$, и $r = r_5(\varepsilon q)$, если $s = 7$. По лемме 3.9 получаем, что $t(r, L) \geq 5$. По предложению 4.3 можно считать, что r взаимно просто с $|\overline{G}/S|$. Если $r \in \pi(K)$, то из леммы 4.1 следует, что $r = v$. Тогда $t(v, S) \geq 5$ по лемме 3.1; противоречие с леммой 3.5. Значит, можно считать, что r взаимно просто с $|\overline{G}/S| \cdot |K|$, в частности, $r \in \pi(S)$. По лемме 4.5(г) получаем, что $t(r, S) \geq t(r, L) \geq s - 1 > 2$, поэтому $r \notin \delta(S)$. Тогда r смежно с $r_s(\varepsilon q)$ и не смежно с $r_{2s}(\varepsilon q)$ в $GK(S)$; противоречие. \square

Лемма 5.3 Предположим, что $t(S) = t(L)$ и $S = L_m^\tau(u)$, где $\tau \in \{+, -\}$. Обозначим $s = \lfloor \frac{n-1}{2} \rfloor$. Если $t(L) \geq 10$ и $0 \leq i \leq 2$ или $t(L) = 9$ и $0 \leq i \leq 1$, то $R_{s-i}(\varepsilon q) \subseteq R_{s-i}(\tau u)$.

Доказательство. Согласно таблице 2 находим, что $t(L) = \lfloor \frac{n+1}{2} \rfloor$ и, следовательно, $s = t(L) - 1$. Если $t(L) = 9$, то $17 \leq n \leq 18$, поэтому $s \geq 8$ и $s - 1 > 6$, в частности, $s - 1 > \frac{n}{3}$. Аналогично, если $t(L) \geq 10$, то $s - 2 > \frac{n}{3} > 6$. С другой стороны, видим, что $s < n/2$. Следовательно, получаем, что $t(r_{s-i}(\varepsilon q), L) = s - i$ во всех случаях по лемме 3.9.

Пусть j – целое число такое, что $n \geq j \geq s - 2$, если $t(L) > 9$, и $n \geq j \geq s - 1$, если $t(L) = 9$. Мы утверждаем, что каждое число $r_j(\varepsilon q)$ взаимно просто с $|\overline{G}/S| \cdot |K|$. По предложению 4.3 получаем, что $r_j(\varepsilon q)$ не делит $|\overline{G}/S|$. Предположим, что $r_j(\varepsilon q) \in \pi(K)$. Из леммы 4.1 следует, что $r_j(\varepsilon q) = v$. Используя лемму 4.5, получаем, что $t(v, S) \geq t(v, L) \geq 6$; противоречие с леммой 3.5. Следовательно, $r_j(\varepsilon q)$ взаимно просто с $|\overline{G}/S| \cdot |K|$, в частности, $r_j(\varepsilon q) \in \pi(S)$. По лемме 4.5(в) получаем что $t(r_j(\varepsilon q), S) \geq t(r_j(\varepsilon q), L)$. Значит, если $r_j(\varepsilon q)$ большое относительно L , то $r_j(\varepsilon q)$ большое относительно S . Более того, если $t(L) \geq 10$ и $0 \leq i \leq 2$ или $t(L) = 9$ и $0 \leq i \leq 1$, то $t(r_{s-i}(\varepsilon q), S) \geq t(r_{s-i}(\varepsilon q), L) = s - i$.

Предположим, что $i = 0$. Если $t(r_s(\varepsilon q), S) \neq s$, то $t(r_s(\varepsilon q), S) \geq s + 1 = t(S)$, и, следовательно, $r_s(\varepsilon q)$ большое относительно S . Поскольку $2s + 1 \leq n$, лемма 3.2 влечет, что $r_s(\varepsilon q)$ смежно с $r_{s+1}(\varepsilon q)$ и $r_{2s}(\varepsilon q)$ в $GK(L)$. Согласно таблице 2 видим, что $r_{s+1}(\varepsilon q)$ и $r_{2s}(\varepsilon q)$ являются большими относительно L и не смежны в $GK(L)$. Следовательно, получаем, что числа $e(r_s(\varepsilon q), \tau u), e(r_{s+1}(\varepsilon q), \tau u), e(r_{2s}(\varepsilon q), \tau u)$ попарно различны и принадлежат $J(S) \setminus E(S)$; противоречие, поскольку $|J(S) \setminus E(S)| \leq 2$ по таблице 2. Значит, $t(r_s(\varepsilon q), S) = s$ и поэтому $r_s(\varepsilon q) \in R_s(\tau u)$ по лемме 3.9. Поскольку это верно для любого $r_s(\varepsilon q) \in R_s(\varepsilon q)$, получаем, что $R_s(\varepsilon q) \subseteq R_s(\tau u)$.

Предположим, что $i = 1$. Если $t(r_{s-1}(\varepsilon q), S) \neq s - 1$, то $t(r_{s-1}(\varepsilon q), S) \geq s$. Если $t(r_{s-1}(\varepsilon q), S) = s$, то $r_{s-1}(\varepsilon q) \in R_s(\tau u)$ по лемме 3.9. Однако мы знаем, что $r_s(\varepsilon q) \in R_s(\tau u)$. Поскольку $r_{2s}(\varepsilon q)$ смежно с $r_s(\varepsilon q)$ и не смежно с $r_{s-1}(\varepsilon q)$ в $GK(S)$,

приходим к противоречию. Если $t(r_{s-1}(\varepsilon q), S) \geq s + 1$, то $r_{s-1}(\varepsilon q)$ большое относительно S . Рассматривая простые числа $r_{s+2}(\varepsilon q)$ и $r_{2s-2}(\varepsilon q)$, и рассуждая, как в предыдущем случае, получаем противоречие с $|J(S) \setminus E(S)| \leq 2$. Следовательно, для любого $r_{s-1}(\varepsilon q) \in R_{s-1}(\varepsilon q)$ верно, что $t(r_{s-1}(\varepsilon q), S) = s - 1$. Тогда $R_{s-1}(\varepsilon q) \subseteq R_{s-1}(\tau u)$ по лемме 3.9.

Предположим, что $i = 2$. Тогда $t(L) \geq 10$, поэтому $n \geq 19$ и $s \geq 9$. Если $t(r_{s-2}(\varepsilon q), S) \neq s - 2$, то $t(r_{s-2}(\varepsilon q), S) \geq s - 1$. Если $t(r_{s-2}(\varepsilon q), S) = s$ или $t(r_{s-2}(\varepsilon q), S) = s - 1$, то из леммы 3.9 следует, что $r_{s-2}(\varepsilon q) \in R_s(\tau u)$ или $r_{s-2}(\varepsilon q) \in R_{s-1}(\tau u)$ соответственно. Мы уже знаем, что $R_s(\varepsilon q) \subseteq R_s(\tau u)$, при этом $r_s(\varepsilon q)$ смежно с $r_{2s}(\varepsilon q)$ в $GK(S)$, кроме того, $R_{s-1}(\varepsilon q) \subseteq R_{s-1}(\tau u)$ и $r_{s-1}(\varepsilon q)$ смежно с $r_{2s-2}(\varepsilon q)$ в $GK(S)$. Поскольку $r_{s-2}(\varepsilon q)$ не смежно с $r_{2s}(\varepsilon q)$ и $r_{2s-2}(\varepsilon q)$ в $GK(S)$, получаем противоречие. Предположим, что $t(r_{s-2}(\varepsilon q), S) \geq s + 1$. Тогда $r_{s-2}(\varepsilon q)$ является большим относительно S . Рассматривая простые числа $r_{s+3}(\varepsilon q)$ и $r_{2s-4}(\varepsilon q)$, которые являются большими относительно L и смежными с $r_{s-2}(\varepsilon q)$ в $GK(L)$, получаем противоречие с $|J(S) \setminus E(S)| \leq 2$, как и выше. Следовательно, для любого $r_{s-2}(\varepsilon q) \in R_{s-2}(\varepsilon q)$ верно, что $t(r_{s-2}(\varepsilon q), S) = s - 2$. Тогда $R_{s-2}(\varepsilon q) \subseteq R_{s-2}(\tau u)$ по лемме 3.9. \square

Лемма 5.4. Если $S = L_m^\tau(u)$, где $\tau \in \{+, -\}$, то $u^{m-1} < \frac{q}{q-1} \cdot \frac{u}{u-1} \cdot (m, u - \tau 1)q^{n-1}$, в частности, $u^{m-1} < 3mq^{n-1}$.

Доказательство. По [29, следствие 3] находим, что $\frac{u^m - \tau 1}{(u - \tau 1, m)(u - \tau 1)} \in \omega(S)$. Заметим, что $\frac{u^m - \tau 1}{(u - \tau 1, m)(u - \tau 1)} \geq \frac{u^{m+1}}{(u - \tau 1, m)(u + 1)}$. Легко видеть, что $\frac{u^{m+1}}{u+1} > \frac{u-1}{u}u^{m-1}$. По лемме 3.7 каждый элемент $\omega(L)$ не превосходит $\frac{q}{q-1}q^{n-1}$. Следовательно, $\frac{u-1}{(u - \tau 1, m)u}u^{m-1} < \frac{u^{m+1}}{(u - \tau 1, m)(u + 1)} \leq \frac{q}{q-1}q^{n-1}$ и поэтому $u^{m-1} < \frac{q}{q-1} \frac{u}{u-1} (u - \tau 1, m)q^{n-1}$. Поскольку $q \geq 3$ и $u \geq 2$, получаем, что $\frac{q}{q-1} \leq \frac{3}{2}$ и $\frac{u}{u-1} \leq 2$, следовательно, $\frac{q}{q-1} \frac{u}{u-1} mq^{n-1} \leq 3mq^{n-1}$. \square

Теперь докажем теорему 2, рассматривая несколько случаев в следующих леммах.

Лемма 5.5. Теорема 2 верна, если $17 \leq n \leq 26$.

Доказательство. Согласно таблице 2 находим, что $9 \leq t(L) \leq 13$. Из теоремы 3 следует, что $t(S) = t(L)$. Обозначим $m = \text{prk } S$. Разобьем доказательство на несколько случаев в зависимости от значения $t(L)$.

Случай $t(L) = 13$. Тогда $n = 25$ или $n = 26$. Предположим, что S – симплектическая или ортогональная группа. Поскольку $t(S) = t(L) = 13$, получаем, что $S \in \{O_{33}(u), S_{32}(u), O_{34}^\pm(u), O_{36}^+(u), O_{32}^-(u)\}$ согласно таблице 2.

Предположим, что $S \in \{O_{33}(u), S_{32}(u), O_{32}^-(u)\}$. Согласно таблице 2 видим, что $J(S) = E(S)$. Теперь покажем, что $q^{17} < u^{12}$. Поскольку $r_{23}(\varepsilon q)$ и $r_{19}(\varepsilon q)$ являются большими относительно L и не смежны в $GK(L)$, из леммы 5.1 следует, что существуют различные натуральные числа i_1 и i_2 такие, что $k_{23}(\varepsilon q)$ делит $k_{i_1}(u)$ и $k_{19}(\varepsilon q)$ делит $k_{i_2}(u)$. Поскольку $m = 16$, получаем, что $\eta(i_1), \eta(i_2) \leq 16$. Ясно, что хотя бы одно из чисел i_1 или i_2 не равно 32. Обозначим это число через i . Тогда $\varphi(i) \leq 12$. Из лемм 2.4(г) и 2.6 следует, что $\frac{u}{u-1}u^{12} > \Phi_i(u) \geq k_i(u) > \frac{5}{3}q^{17}$, в частности, $u \geq 3$. Следовательно, получаем, что $\frac{3}{2}u^{12} > \frac{5}{3}q^{17}$ и поэтому $q^{17} < u^{12}$.

Применяя предложение 2.15 для S и L , находим, что $\frac{2}{21}u^{160} \leq \exp(S) \leq \exp(L) \leq 8990q^{213}$. Поскольку $q^{17} < u^{12}$, получаем, что $q^{226} < u^{160} < 21 \cdot 8990q^{213} < 3^{13}q^{213}$. Это неравенство влечет, что $q < 3$; противоречие.

Предположим, что $S \in \{O_{34}^\pm(u), O_{36}^+(u)\}$. Согласно таблице 2 видим, что $J(S) \setminus E(S)$ равно $\{9, 16\}$, $\{16, 18\}$, или $\{9, 18\}$. Поскольку $r_{23}(\varepsilon q)$ является большим относительно

L , из леммы 5.1 следует, что $k_{23}(\varepsilon q)$ делит $k_i(u)$, где i – целое число, $k_9(u)k_{18}(u)$ или $k_9(\tau u)k_{16}(u)$, где $\tau \in \{+, -\}$. Заметим, что $\eta(i) \leq 18$ и поэтому $\varphi(i) \leq 16$. По лемме 2.6 получаем, что $k_{23}(\varepsilon q) > \frac{5}{3}q^{21}$. Из леммы 2.4(г) следует, что $k_i(u) \leq \Phi_i(u) < \frac{u}{u-1}u^{\varphi(i)}$, $k_9(u)k_{18}(u) \leq \Phi_9(u)\Phi_{18}(u) < 4u^{12}$, и $k_9(\tau u)k_{16}(u) \leq \Phi_9(\tau u)\Phi_{16}(u) < 4u^{14}$. Следовательно, верно, что $\frac{5}{3}q^{21} < k_{23}(\varepsilon q) < \frac{3}{2}u^{16} < \frac{5}{3}u^{16}$ и поэтому $q^{21} < u^{16}$. Применяя предложение 2.15, находим, что $\frac{2}{21}u^{176} \leq \exp(S) \leq \exp(L) \leq 8990q^{213}$. Поскольку $q^{21} < u^{16}$, получаем, что $q^{231} < u^{176} < 21 \cdot 8990q^{213}$. Это неравенство влечет, что $q < 3$; противоречие.

Предположим, что $S \simeq L_m^\tau(u)$, где $\tau \in \{+, -\}$. Поскольку $t(S) = 13$, находим, что $25 \leq m \leq 26$. По лемме 5.2 получаем, что $m \geq n$. Из леммы 5.3 следует, что $R_{12}(\varepsilon q) \subseteq R_{12}(\tau u)$. Значит, $k_{12}(\varepsilon q)$ делит $k_{12}(\tau u)$. Из равенства (1) следует, что $k_{12}(\varepsilon q) = q^4 - q^2 + 1$ и $k_{12}(\tau u) = u^4 - u^2 + 1$. Поскольку $q \neq u$, то $k_{12}(\varepsilon q) \neq k_{12}(\tau u)$. Каждый простой делитель числа $k_{12}(\tau u)$ не меньше 13, поэтому $13k_{12}(\varepsilon q) \leq k_{12}(\tau u)$. Откуда следует, что $\frac{13}{2}q^4 < 13k_{12}(\varepsilon q) \leq k_{12}(\tau u) < u^4$. По лемме 5.4 получаем, что $78q^{n-1} > u^{m-1} \geq u^{n-1}$; противоречие с неравенством $u^4 > 6q^4$.

Случай $t(L) = 12$. Тогда $n = 23$ или $n = 24$. Предположим, что S – симплектическая или ортогональная группа. Поскольку $t(S) = 12$, то $S \in \{O_{31}(u), S_{30}(u), O_{30}^\pm(u), O_{32}^+(u)\}$.

Предположим, что $S \in \{O_{31}(u), S_{30}(u)\}$. Согласно таблице 2 видим, что $|J(S) \setminus E(S)| = 3$; противоречие с леммой 5.1.

Предположим, что $S \in \{O_{30}^+(u), O_{30}^-(u), O_{32}^+(u)\}$. Согласно таблице 2 верно, что $J(S) = E(S)$. Из леммы 5.1 следует, что существует целое число i такое, что $k_{23}(\varepsilon q)$ делит $k_i(u)$. Поскольку $\eta(i) \leq 15$, то $\varphi(i) \leq 12$. Используя лемму 2.4, получаем, что $k_i(u) \leq \Phi_i(u) \leq \frac{u}{u-1}u^{12}$. Лемма 2.6 влечет, что $k_{23}(\varepsilon q) > \frac{5}{3}q^{21}$. Следовательно, $u \geq 3$ и $\frac{5}{3}q^{21} < \frac{5}{3}u^{12}$. По предложению 2.15 находим, что $\frac{2}{16}u^{136} \leq \exp(S) \leq \exp(L) \leq 6203q^{181}$. Следовательно, получаем, что $q^{238} < u^{136} \leq 8 \cdot 6203q^{181}$. Значит, $q < 3$; противоречие.

Предположим, что $S = L_m^\tau(u)$, $\tau \in \{+, -\}$. Поскольку $t(S) = 12$, находим, что $23 \leq m \leq 24$. По лемме 5.2 получаем, что $m \geq n$. Из леммы 5.3 следует, что $R_9(\varepsilon q) \subseteq R_9(\tau u)$. Тогда $3q^6 < u^6$ по [8, лемма 2.5(в)]. Значит, $u \geq 4$. Используя лемму 5.4, получаем, что $u^{n-1} \leq u^{m-1} < \frac{3 \cdot 4}{2 \cdot 3} \cdot 24q^{n-1}$, поэтому $u^{n-1} < 48q^{n-1}$. С другой стороны, неравенство $u^6 > 3q^6$ влечет, что $u^{n-1} > 3^{22/6}q^{n-1} > 56q^{n-1}$; противоречие.

Случай $t(L) = 11$. Тогда $n = 21$ или $n = 22$. Предположим, что S – симплектическая или ортогональная группа. Поскольку $t(S) = 11$, находим, что $S \in \{O_{27}(u), S_{26}(u), O_{29}(u), S_{28}(u), O_{28}^-(u)\}$ согласно таблице 2. Если $S = O_{28}^-(u)$, то $|J(S) \setminus E(S)| = 3$, значит случай невозможен по лемме 5.1(б). В других случаях видим, что $J(S) = E(S)$ или $J(S) \setminus E(S) = \{7, 14\}$. Из леммы 5.1(а) следует, что $k_{19}(\varepsilon q)$ делит $k_7(u)k_{14}(u)$ или $k_i(u)$, где i – целое число, такое что $\eta(i) \leq 14$. Тогда $\varphi(i) \leq 12$. Лемма 2.4(г) влечет, что $k_i(u) \leq \frac{u}{u-1}u^{12}$ и $k_7(u)k_{14}(u) \leq \Phi_7(u)\Phi_{14}(u) = \Phi_7(u^2) < \frac{4}{3}u^{12}$. Используя лемму 2.6, получаем, что $\frac{5}{3}q^{17} < k_{19}(\varepsilon q) < \frac{u}{u-1}u^{12}$ и, следовательно, $q^{17} < u^{12}$. Применяя предложение 2.15 для S и L , получаем, что $\frac{2}{12}u^{116} \leq \exp(S) \leq \exp(L) \leq 2832q^{151}$. Значит, $q^{164} < 6 \cdot 2832q^{151}$ и поэтому $q^{13} < 17000$. Это неравенство влечет, что $q < 3$; противоречие.

Предположим, что $S = L_m^\tau(u)$, где $\tau \in \{+, -\}$. Поскольку $t(S) = 11$, находим, что $21 \leq m \leq 22$. По лемме 5.2 получаем, что $m \geq n$. Из леммы 5.3 следует, что $R_8(\varepsilon q) \subseteq R_8(\tau u)$. Тогда $k_8(\varepsilon q)$ делит $k_8(\tau u)$. Используя равенство (1), получаем, что $k_8(\varepsilon q) = (q^4 + 1)/2$ и $k_8(\tau u) = (u^4 + 1)/(u - 1, 2)$. Предположим, что $k_8(\varepsilon q) = k_8(\tau u)$. Поскольку $q \neq u$, имеем равенство $q^4 - 1 = 2u^4$. Очевидно, что $q^4 - 1$ делится на 8 и $r_4(q)$, поэтому $q^4 - 1 \neq 2u^4$. Значит, $k_8(\varepsilon q)$ – собственный делитель $k_8(\tau u)$, и, следовательно,

$17 \cdot (q^4 + 1)/2 \leq (u^4 + 1)$. Поскольку $u^4 + 1 < \frac{16}{15}u^4$, получаем, что $\frac{17}{2}q^4 < \frac{16}{15}u^4$, поэтому $7q^4 < u^4$. С другой стороны, из леммы 5.4 следует, что $u^{n-1} \leq 66q^{n-1}$, что противоречит неравенству $7q^4 < u^4$.

Случай $t(L) = 10$. Тогда $n = 19$ или $n = 20$. Предположим, что S – симплектическая или ортогональная группа. Поскольку $t(S) = 10$, находим, что $S \in \{O_{25}(u), S_{24}(u), O_{26}^\pm(u), O_{24}^-(u), O_{28}^+(u)\}$ согласно таблице 2.

Предположим, что $S \in \{O_{25}(u), S_{24}(u), O_{24}^-(u)\}$. Согласно таблице 2 видим, что $J(S) = E(S)$. Из леммы 5.1 следует, что существует целое число i такое, что $k_{19}(\varepsilon q)$ делит $k_i(u)$. Поскольку $\eta(i) \leq 12$, имеем $\varphi(i) \leq 10$ и поэтому $k_i(u) \leq 2u^{10}$ по лемме 2.4. Используя лемму 2.6, получаем, что $q^{17} < k_{19}(\varepsilon q) \leq k_i(u) \leq 2u^{10}$. В силу предложения 2.15, находим, что $\frac{2}{8}u^{92} \leq \exp(S) \leq \exp(L) \leq 1922q^{129}$. Следовательно, $q^{156} < 2^{92/10} \cdot 4 \cdot 1922q^{129}$ и, поэтому $q < 3$; противоречие.

Предположим, что $S \in \{O_{26}^+(u), O_{26}^-(u), O_{28}^+(u)\}$. Согласно таблице 2 видим, что $J(S) \setminus E(S)$ равно $R_{12}(u) \cup R_{14}(u)$, $R_{12}(u) \cup R_7(u)$ или $R_7(u) \cup R_{14}(u)$. Лемма 5.1 влечет, что $k_{19}(\varepsilon q) \leq k_i(u)$, где i – целое число, или $k_{19}(\varepsilon q)$ делит одно из чисел $k_{12}(u)k_{14}(u)$, $k_{12}(u)k_7(u)$ или $k_7(u)k_{14}(u)$. Заметим, что $\varphi(i) \leq 12$, $\varphi(12) = 4$, $\varphi(7) = \varphi(14) = 6$. Используя лемму 2.4 и равенство $\Phi_7(u)\Phi_{14}(u) = \Phi_7(u^2)$, получаем, что $q^{17} < k_{19}(\varepsilon q) \leq 2u^{12}$ во всех случаях. Из предложения 2.15 следует, что $\frac{2}{16}u^{104} < \exp(S) \leq \exp(L) < 1922q^{129}$. Значит, $q^{147} < 2^{(104/12)} \cdot 8 \cdot 1922q^{129}$ и поэтому $q^{18} < 7 \cdot 10^6$. Это неравенство влечет, что $q < 3$; противоречие.

Предположим, что $S = L_m^\tau(u)$, где $\tau \in \{+, -\}$. Поскольку $t(S) = 10$, получаем, что $19 \leq m \leq 20$. По лемме 5.2 верно, что $m \geq n$. Применяя лемму 5.3, находим, что $R_8(\varepsilon q) \subseteq R_8(\tau u)$. Аналогично предыдущему случаю, имеем $7q^4 < u^4$. С другой стороны, лемма 5.4 влечет, что $u^{n-1} \leq u^{m-1} < 60q^{n-1}$, что невозможно, поскольку $u^{n-1} > 7^3q^{n-1}$.

Случай $t(L) = 9$. Тогда $n = 17$ или $n = 18$. Предположим, что S – симплектическая или ортогональная группа. Поскольку $t(S) = 9$, получаем, что $S \in \{O_{23}(u), S_{22}(u), O_{22}^\pm(u), O_{24}^+(u)\}$.

Если $S \in \{O_{23}(u), S_{22}(u)\}$, то $|J(S) \setminus E(S)| = 3$, поэтому этот случай невозможен по лемме 5.1(б). Предположим, что $S \in \{O_{24}^+(u), O_{22}^+(u), O_{22}^-(u)\}$. Согласно таблице 2 видим, что $J(S) = E(S)$. По лемме 5.1(а) существует целое число i такое, что $k_{17}(\varepsilon q)$ делит $k_i(u)$. Поскольку $\eta(i) \leq 12$, заключаем, что $\varphi(i) \leq 10$. Из лемм 2.6 и 2.4 следует, что $\frac{5}{3}q^{15} < k_{17}(\varepsilon q) \leq k_i(u) \leq \frac{u}{u-1}u^{10}$, поэтому $u \geq 3$ и $q^{15} < u^{10}$. Используя предложение 2.15, находим, что $\frac{2}{10}u^{74} \leq \exp(S) \leq \exp(L) < 860q^{103}$. Следовательно, $q^{111} < u^{74} \leq 5 \cdot 860q^{103}$ и поэтому $q^8 < 4390$. Это неравенство влечет, что $q < 3$; противоречие.

Предположим, что $S = L_m^\tau(u)$, где $\tau \in \{+, -\}$. Поскольку $t(S) = 9$, находим, что $17 \leq m \leq 18$. По лемме 5.2 имеем неравенство $m \geq n$. Применяя лемму 5.3, получаем, что $R_8(\varepsilon q) \subseteq R_8(\tau u)$. Следовательно, $7q^4 < u^4$. С другой стороны, лемма 5.4 влечет, что $u^{n-1} \leq u^{m-1} < 54q^{n-1}$, что невозможно, поскольку $u^{n-1} > 7^3q^{n-1}$. \square

Лемма 5.6. Теорема 2 верна, если $15 \leq n \leq 16$.

Доказательство. В этом случае получаем, что $t(L) = 8$. По теореме 3 верно, что $t(S) = 8$.

Предположим, что S – симплектическая или ортогональная группа. Согласно таблице 2 получаем, что $S \in \{O_{19}(u), S_{18}(u), O_{21}(u), S_{20}(u), O_{20}^-(u)\}$.

Предположим, что $S \in \{O_{19}(u), S_{18}(u)\}$. Согласно таблице 2, видим, что $J(S) = E(S)$. Если $n = 16$, то $r_8(\varepsilon q)$ и $r_{16}(\varepsilon q)$ являются большими относительно L и смежными в $GK(L)$. По лемме 3.9 получаем, что $r_8(\varepsilon q)$ и $r_{16}(\varepsilon q)$ большие относительно S и смежны

в $GK(S)$. Поскольку $J(S) = E(S)$, получаем равенство $\varphi(r_8(\varepsilon q), S) = \varphi(r_{16}(\varepsilon q), S)$. С другой стороны, $r_7(\varepsilon q)$ взаимно просто с $|K| \cdot |\overline{G}/S|$ по лемме 4.1 и предложению 4.3. Следовательно, $r_7(\varepsilon q)$ смежно с $r_8(\varepsilon q)$ и не смежно с $r_{16}(\varepsilon q)$ в $GK(S)$; противоречие с леммой 3.10. Следовательно, можно считать, что $n = 15$. Из леммы 5.1 следует, что существует целое число i такое, что $k_{13}(\varepsilon q)$ делит $k_i(u)$. Поскольку $\eta(i) \leq 9$, имеем $\varphi(i) \leq 8$, поэтому $k_i(u) \leq \frac{u}{u-1}u^8$ по лемме 2.4. Поскольку $k_i(u) \geq k_{13}(\varepsilon q) > q^{11}$, находим, что $u \geq 5$. По лемме 2.6 получаем, что $\frac{5}{3}q^{11} < k_{13}(\varepsilon q) \leq k_i(u) \leq \frac{5}{4}u^8$ и, следовательно, $q^{11} < \frac{3}{4}u^8$. Используя предложение 2.15, находим, что $\frac{2}{8}u^{56} \leq \exp(S) \leq \exp(L) \leq 531q^{73}$. Следовательно, $q^{77} < (\frac{3}{4})^7 u^{56} < (\frac{3}{4})^7 \cdot 4 \cdot 531q^{73}$ и поэтому $q < 5$. Значит, $q = 3$. Используя неравенство $u^{56} \leq 4 \cdot 531q^{73}$, находим, что $u < 5$; противоречие с $u \geq 5$.

Если $S = O_{20}^-(u)$, то $J(S) \setminus E(S) = \{5, 10, 8\}$; противоречие с леммой 5.1.

Предположим, что $S \in \{O_{21}(u), S_{20}(u)\}$. Согласно таблице 2 получаем, что $J(S) \setminus E(S) = \{5, 10\}$. Из леммы 5.1 следует, что $R_{13}(\varepsilon q) \subseteq R_5(u) \cup R_{10}(u)$, или существует целое число i такое, что $R_{13}(\varepsilon q) \subseteq R_i(u)$. Поскольку $\eta(i) \leq 10$, заключаем, что $\varphi(i) \leq 8$ и поэтому $k_i(u) \leq 2u^8$ по лемме 2.4(г). С другой стороны, $k_5(u)k_{10}(u) \leq \Phi_5(u^2) = u^8 + u^6 + u^4 + u^2 + 1 < \frac{3}{2}u^8$. По лемме 2.6 получаем, что $k_{13}(\varepsilon q) > \frac{5}{3}q^{11}$ и, следовательно, $u > 2$. Из леммы 2.4(г) следует, что $\frac{5}{3}q^{11} < k_{13}(\varepsilon q) \leq \frac{5}{3}u^8$ и, следовательно, $q^{11} < u^8$. По предложению 2.15 получаем, что $\frac{5}{5}u^{64} \leq \exp(S) \leq \exp(L) \leq 569q^{81}$. Следовательно, $q^{88} < u^{64} < 3 \cdot 569q^{81}$ и поэтому $q < 3$; противоречие.

Предположим, что $S = L_m^\tau(u)$, где $15 \leq m \leq 16$ и $\tau \in \{+, -\}$. По лемме 5.2 получаем, что $m \geq n$. Из леммы 4.1 и предложения 4.3 следует, что простые числа $r_7(\varepsilon q)$, $r_8(\varepsilon q)$ и $r_{14}(\varepsilon q)$ взаимно просты с $|K| \cdot |\overline{G}/S|$. Следовательно, по леммам 3.9 и 4.5 получаем, что $t(r_7(\varepsilon q), S) \geq 7$. Если $t(r_7(\varepsilon q), S) = 8$, то $r_7(\varepsilon q)$ большое относительно S и смежно с $r_{14}(\varepsilon q)$ и $r_8(\varepsilon q)$ в $GK(S)$. Следовательно, числа $e(r_7(\varepsilon q), \tau u)$, $e(r_{14}(\varepsilon q), \tau u)$, и $e(r_8(\varepsilon q), \tau u)$ различны; противоречие с $|J(S) \setminus E(S)| \leq 2$. Значит, $t(r_7(\varepsilon q), S) = 7$ для любого $r_7(\varepsilon q) \in R_7(\varepsilon q)$ и поэтому $R_7(\varepsilon q) \subseteq R_7(\tau u)$ по лемме 3.9.

Предположим, что $n = 16$. Поскольку $r_8(\varepsilon q)$ и $r_{16}(\varepsilon q)$ смежны в $GK(S)$ и большие относительно S , а число $r_7(\varepsilon q)$ смежно с $r_8(\varepsilon q)$ и не смежно с $r_{16}(\varepsilon q)$ в $GK(S)$, получаем, что $m = 16$, $R_8(\varepsilon q) \subseteq R_8(\tau u)$ и $R_{16}(\varepsilon q) \subseteq R_{16}(\tau u)$. Следовательно, $k_8(\varepsilon q)$ делит $k_8(\tau u)$, и поэтому $7q^4 < u^4$. По лемме 5.4 получаем, что $u^{15} < 48q^{15}$; противоречие с $7q^4 < u^4$.

Предположим, что $n = m = 15$. Поскольку $r_8(\varepsilon q)$ и $r_{14}(\varepsilon q)$ смежны с $r_7(\varepsilon q)$, заключаем, что либо $R_8(\varepsilon q) \subseteq R_8(\tau u)$, либо $R_8(\varepsilon q) \subseteq R_{14}(\tau u)$. В первом случае находим, что $k_8(\varepsilon q)$ делит $k_8(\tau u)$, и получаем противоречие, как и в предыдущем случае. Поэтому можно считать, что $R_8(\varepsilon q) \subseteq R_{14}(\tau u)$. Тогда $R_{14}(\varepsilon q) \subseteq R_8(\tau u)$, и, следовательно, $k_{14}(\varepsilon q)$ делит $k_8(\tau u)$. По лемме 2.6 находим, что $q^5 < k_7(-\varepsilon q) = k_{14}(\varepsilon q) \leq k_8(\tau u) = u^4 + 1 < \frac{16}{15}u^4$. По предложению 2.15 получаем, что $\frac{v}{29}u^{72} < \exp(S) \leq \exp(L) < 531q^{73}$. Следовательно, $q^{90} < (\frac{16}{15})^{18}u^{72} < 4 \cdot 15 \cdot 531q^{73}$ и поэтому $q < 3$; противоречие.

Предположим, что $n = 15$ и $m = 16$. По предложению 2.15 находим, что $\frac{v}{57}u^{80} < \exp(S) \leq \exp(L) < 531q^{72}$. Если $(q - \varepsilon 1, 7) = 1$, то из леммы 2.8 следует, что $5q^6 < u^6$ и поэтому $5^{13}q^{80} < u^{80}$, что противоречит неравенству $\exp(S) \leq \exp(L)$. Значит, можно считать, что $(q - \varepsilon 1, 7) = 7$, в частности, $q \geq 13$. По лемме 5.1 получаем, что $k_{13}(\varepsilon q)$ делит $k_{16}(\tau u)k_8(\tau u)$ или $k_i(\tau u)$, где i – целое число такое, что $i \leq 16$. Используя равенство (1), получаем, что $k_{13}(\varepsilon q) > \frac{12}{13d}q^{12}$, где $d = (q - \varepsilon 1, 13)$. С другой стороны, $k_{16}(\tau u)k_8(\tau u) \leq (u^8 + 1)(u^4 + 1) < \frac{u}{u-1}u^{12}$ и $k_i(\tau u) \leq \frac{u}{u-1}u^{12}$ по лемме 2.4(г). Следовательно, $u \geq 7$ и поэтому $q^{12} < \frac{13}{12} \cdot \frac{7}{6}du^{12} < \frac{3}{2}du^{12}$. Тогда $q^{80} < (\frac{3}{2}d)^7 u^{80} < (\frac{3}{2}d)^7 \cdot 29 \cdot 531q^{73}$. Значит, $q^7 < 300000d^7$. Если $d = 1$, то получаем, что $q < 7$; противоречие с $q \geq 13$. Если $d = 13$, то $q - \varepsilon 1$ делится на 7 и 13, поэтому $q \geq 183$. Тогда $q^7 > (13^2)^7 > d^7 13^7 > 300000d^7$;

противоречие. □

Лемма 5.7. Теорема 2 верна, если $13 \leq n \leq 14$.

Доказательство. Поскольку n не является простым числом, получаем, что $n = 14$.

По теореме 3 верно, что $t(S) = 7$. Предположим, что S – симплектическая или ортогональная группа. Согласно таблице 2 получаем, что $S \in \{O_{17}(u), S_{16}(u), O_{18}^\pm(u), O_{20}^+(u), O_{16}^-(u)\}$. Из леммы 4.1 и предложения 4.3 следует, что $r_5(\varepsilon q)$, $r_7(\varepsilon q)$ и $r_{14}(\varepsilon q)$ взаимно просты с $|K| \cdot |\overline{G}/S|$. Тогда $r_7(\varepsilon q)$ и $r_{14}(\varepsilon q)$ являются большими относительно L и смежными в $GK(S)$. Поскольку $r_5(\varepsilon q)$ смежно с $r_7(\varepsilon q)$ и не смежно с $r_{14}(\varepsilon q)$ в $GK(S)$, получаем, что $J(S) \neq E(S)$. Следовательно, $S \notin \{O_{17}(u), S_{16}(u), O_{16}^-(u)\}$ согласно таблице 2. Таким образом, можно считать, что $S = O_{18}^\pm(u)$ или $S = O_{20}^+(u)$. В этом случае имеем $|J(S) \setminus E(S)| = 2$. Значит, $R_7(\varepsilon q) \subseteq R_{j_1}(u)$ и $R_{14}(\varepsilon q) \subseteq R_{j_2}(u)$, где $J(S) \setminus E(S) = \{j_1, j_2\}$. Следовательно, $R_{13}(\varepsilon q) \cap (R_{j_1}(u) \cup R_{j_2}(u)) = \emptyset$. Из леммы 5.1 следует, что $k_{13}(\varepsilon q)$ делит $k_i(u)$ для некоторого целого числа i такого, что $\eta(i) \leq 10$. Тогда $\varphi(i) \leq 8$. Обозначим число $(q - \varepsilon 1, 13)$ через d . Используя равенство (1), находим, что $k_{13}(\varepsilon q) \geq \frac{2}{3d}q^{12}$. Из леммы 2.4(г) следует, что $\frac{u}{u-1}u^8 > k_i(u) \geq \frac{2}{3d}q^{12}$. Поскольку $q \geq 3$, получаем, что $u \geq 4$. Следовательно, $q^{12} < \frac{4}{3} \cdot \frac{3}{2}du^8 = 2du^8$. По предложению 2.15 находим, что $\frac{v}{10}u^{50} < \exp(S) \leq \exp(L) \leq 247q^{65}$. Это означает, что $q^{75} < (2d)^{6.25}u^{50} < (2d)^{6.25} \cdot 1235q^{65}$. Тогда $q^{10} < 93995d^{6.25}$. Если $d = 1$, то $q < 4$ и, следовательно, $q = 3$. В этом случае $R_7(3) = \{1093\}$ и $R_{14}(3) = \{547\}$. Согласно таблице 2 получаем, что $j_1 \in \{5, 10\}$ или $j_2 \in \{5, 10\}$, следовательно, $1093 - 1$ или $547 - 1$ должно делиться на 10; противоречие. Если $d = 13$, то получаем, что $q < 15$, но это невозможно, поскольку $q - \varepsilon 1$ делится на 13.

Предположим, что $S = L_m^\tau(u)$, где $13 \leq m \leq 14$. Из леммы 5.2 следует, что $m = 14$. Согласно таблице 2 видим, что $J(L) \setminus E(L) = J(S) \setminus E(S) = \{7, 14\}$. Применяя лемму 4.1 и предложение 4.3, получаем, что $r_5(\varepsilon q)$ взаимно просто с $|K| \cdot |\overline{G}/S|$. Следовательно, $r_5(\varepsilon q)$ смежно с $r_7(\varepsilon q)$ и не смежно с $r_{14}(\varepsilon q)$ в $GK(S)$. Это означает, что $R_7(\varepsilon q) \subseteq R_7(\varepsilon u)$ и $R_{14}(\varepsilon q) \subseteq R_{14}(\varepsilon u)$, где $\varepsilon \in \{+, -\}$. По лемме 2.8 получаем, что $5q^6 < u^6$ и, следовательно, $32q^{13} < u^{13}$. С другой стороны, лемма 5.4 влечет, что $u^{13} < \frac{q}{q-1} \cdot \frac{u}{u-1} \cdot (u - \tau 1, 14)q^{13}$. Если $u \geq 4$, то $\frac{q}{q-1} \cdot \frac{u}{u-1} \cdot (u - \tau 1, 14) < \frac{3}{2} \cdot 14 = 28$, а если $u \leq 3$, то $(u - \tau 1, 14) \leq 2$ и $\frac{q}{q-1} \cdot \frac{u}{u-1} \cdot (u - \tau 1, 14) \leq \frac{3}{2} \cdot 2 \cdot 2 = 6$; противоречие с $32q^{13} < u^{13}$. □

Лемма 5.8. Теорема 2 верна, если $n = 12$.

Доказательство. В этом случае $t(L) = 6$ и $t(S) = 6$ по теореме 3. Предположим, что S – симплектическая или ортогональная группа. Тогда получаем, что $S \in \{O_{15}(u), S_{14}(u), O_{14}^\pm(u), O_{16}^+(u)\}$, где $u \neq 2$, если $S = O_{14}^\pm(u)$. Согласно таблице 2 видим, что $|J(S) \setminus E(S)| = 3$, если $S \in \{O_{15}(u), S_{14}(u)\}$. Следовательно, эти случаи невозможны по лемме 5.1(б). Предположим, что $S \in \{O_{14}^\pm(u), O_{16}^+(u)\}$. Согласно таблице 2 видим, что $J(S) = E(S)$. В силу леммы 2.12 и предложения 4.3 существует $r_6(\varepsilon q) \neq 7$, взаимно простое с $|\overline{G}/S|$. Из леммы 4.1 следует, что $r_6(\varepsilon q) \notin \pi(K)$. Значит, числа $r_{12}(\varepsilon q)$ и $r_6(\varepsilon q)$ являются большими относительно S и смежными в $GK(S)$. Аналогично, мы получаем, что $r_5(\varepsilon q)$ взаимно просто с $|\overline{G}/S| \cdot |K|$. Это означает, что $r_5(\varepsilon q)$ смежно с $r_6(\varepsilon q)$ и не смежно с $r_{12}(\varepsilon q)$ в $GK(S)$. Получаем противоречие с $J(S) = E(S)$.

Предположим, что $S \simeq L_m(\tau u)$, где $\tau \in \{+, -\}$ и $11 \leq m \leq 12$. Из леммы 5.2 следует, что $m = 12$. Заметим, что $J(L) \setminus E(L) = J(S) \setminus E(S) = \{6, 12\}$. Рассматривая

простые числа $r_5(\varepsilon q)$, $r_6(\varepsilon q)$ и $r_{12}(\varepsilon q)$, находим, что для некоторого $r_6(\varepsilon q)$ верно, что $r_6(\varepsilon q) \in R_6(\tau u)$ и поэтому $R_{12}(\varepsilon q) \subseteq R_{12}(\tau u)$. Следовательно, получаем, что $k_{12}(\varepsilon q)$ делит $k_{12}(\tau u)$. Это означает, что $6q^4 < u^4$ и поэтому $138q^{11} < u^{11}$. С другой стороны, находим, что $u^{11} < 33q^{11}$ по лемме 5.4; противоречие. \square

6 Доказательство теоремы 1

Предположим, что группа L изоморфна $L_n(q)$ или $U_n(q)$, где $n \geq 11$, а q – степень простого числа p . Если q четно, то проблема распознаваемости для L решена в случае линейных групп в [30] и в случае унитарных групп в [31]. В частности, для любой группы G , изоспектральной L , верно, что $L \leq G \leq \text{Aut } L$. Поэтому можно считать, что q нечетно.

Предположим, что G – группа, изоспектральная L . Если $n \geq 27$, то из [8, теорема 1.2] следует, что $L \leq G \leq \text{Aut } L$. Аналогичное заключение верно, если n – простое число в силу основной теоремы статьи [32] и [5, следствие 1]. Основные результаты из [33] показывают, какие именно группы G подходят для L , поэтому проблема распознаваемости решена в этих случаях. Следовательно, можно считать, что n не является простым числом и $12 \leq n \leq 26$.

Используя [25, таблица 2] и [23, таблица 6], видим, что $t(L) \geq 6$ и $t(2, L) \geq 2$. Из леммы 3.1 следует, что существует неабелева простая группа S такая, что $S \leq G = G/K \leq \text{Aut } S$ для максимальной нормальной разрешимой подгруппы K группы G . По [4, следствие 1] группа S не изоморфна исключительной группе лиева типа. По [34, теоремы 1 и 2] и [24, теоремы 1 и 2] получаем, что S не изоморфна знакопеременной группе, спорадической группе или группе Титса ${}^2F_4(2)'$. Следовательно, можно считать, что S – простая классическая группа. По теореме 2 получаем, что S определена над полем характеристики p . Теперь из [24, теорема 3] следует, что $S \simeq L$, и, следовательно, $K = 1$ по [11, следствие 1]. Таким образом, $L \leq G \leq \text{Aut } L$ и группа L почти распознаваема. Чтобы определить, какие группы G подходят, можно воспользоваться основными результатами работы [33], поэтому проблема распознаваемости для L решена.