Владикавказский математический журнал
2012, Том 14, Выпуск 2, С. 50–56

УДК **512.542.52**

ОЦЕНКА ФУНКЦИЙ Ф. ХОЛЛА НА ГРУППАХ ЛИЕВА ТИПА РАНГА 1[1]

Ю. Ю. Ушаков

В 1936 г. Ф. Холл ввел на конечных группах обобщенную n-ю функцию Эйлера и взаимосвязанную функцию, называемую n-й функцией Холла. Значения последней оцениваются в статье на трех из четырех серий простых групп лиева типа ранга 1. При $n = 2$ найденные оценки подтверждают для указанных групп гипотезу Уайголда.

Ключевые слова: n-базы группы, обобщенная функция Эйлера, функция Холла, группа лиева типа.

Введение

Ф. Холл [1] в 1936 г. ввел понятие n-й функции Эйлера φ_n на конечных группах G. По определению, $\varphi_n(G)$ есть число всех n-баз группы G, т. е. число упорядоченных наборов из n ее элементов, порождающих G. Когда G — циклическая группа, $\varphi_1(G)$ совпадает со значением на $|G|$ обычной теоретико-числовой функции Эйлера.

Как показал Ф. Холл [1], для любой конечной простой неабелевой группы G и натурального числа n существует наибольшее число $d = d_n(G)$ такое, что прямая степень G^d порождается n элементами. Согласно [1, п. 1.3],

$$\varphi_n(G) = d_n(G)\,|\mathrm{Aut}\,G|. \tag{1}$$

Вопрос вычисления значений $d_2(G)$ для конечных простых групп G записан в Коуровской тетради [2, вопрос 12.86]. Значения функции φ_2 вычислены в [1] явно для групп $PSL_2(p)$ (p — простое число) и некоторых групп подстановок малых степеней. Рекуррентное описание чисел $d_2(G)$ для групп Сузуки $Sz(2^m)$ и $PSL_2(2^m)$ получили Н. М. Сучков и Д. М. Приходько [3].

Уайголд высказал следующую гипотезу (см. [2, вопрос 17.116] и [4]):

Если G — конечная простая неабелева группа, то

$$d_2(G) \geqslant \sqrt{|G|}. \tag{2}$$

Гипотеза исследовалась для знакопеременных групп [5] и групп $PSL_n(q)$ [6]. См. также [7–9]. В [4] она подтверждена для симплектических групп $PSp_{2m}(q)$ при $2 \leqslant m \leqslant 5$, $m \geqslant 10$ и $q \geqslant 2$.

[1] Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований, проект № 12-01-00968-а.

В настоящей работе оценивается n-я функция Холла d_n на трех из четырех серий групп лиева типа ранга 1. Основным результатом является

Теорема 1. *Пусть G есть одна из простых групп $PSL_2(q)$, групп Сузуки $Sz(2^{2k+1})$ или групп Ри $\mathrm{Re}\,(3^{2k+1})$. Тогда*

$$d_n(G) \geqslant |G|^{n-\frac{3}{2}} \quad (n \geqslant 2). \tag{3}$$

Гипотеза Уайголда для групп из теоремы 1 вытекает из (3) при $n = 2$.

1. Схема доказательства теоремы 1

Следующая лемма редуцирует доказательство теоремы 1 к доказательству гипотезы Уайголда для тех же групп.

Лемма 1.1. *Если G — конечная простая неабелева группа, то*

$$d_k(G) \geqslant |G|^{k-2} d_2(G) \quad (k \geqslant 2). \tag{4}$$

$\lhd$ Если группа G порождается упорядоченной последовательностью $(a_1, a_2, \ldots, a_k)$ ее элементов, то G порождается также любой последовательностью $(a_1, a_2, \ldots, a_k, x)$, $x \in G$. Поэтому $\varphi_{k+1}(G) \geqslant |G|\varphi_k(G)$ и, следовательно, $\varphi_k(G) \geqslant |G|^{k-2}\varphi_2(G)$. Отсюда для d_k имеем оценку:

$$d_k(G) = \frac{\varphi_k(G)}{|\mathrm{Aut}\, G|} \geqslant \frac{|G|^{k-2}\varphi_2(G)}{|\mathrm{Aut}\, G|} = |G|^{k-2} d_2(G). \rhd$$

Заметим, что число упорядоченных пар элементов конечной группы G равно $|G|^2$, причем каждая пара либо порождает G, либо лежит в одной из максимальных подгрупп в G. Поэтому справедлива

Лемма 1.2. *Для любой конечной группы G выполняется неравенство*

$$\varphi_2(G) \geqslant |G|^2 - \sum_M |M|^2, \tag{5}$$

где суммирование ведется по всем максимальным подгруппам группы G.

Далее через $G(q)$ будет обозначаться группа $PSL_2(q)$ над конечным полем $GF(q)$ порядка q характеристики p, группа Ри $\mathrm{Re}\,(q)$, $q = 3^{2l+1}$ (тип ${}^2G_2$), или группа Сузуки $Sz(q)$, $q = 2^{2l+1}$ (тип ${}^2B_2$).

Группа $G(q)$ для любого подполя $GF(m) \subseteq GF(q)$ имеет подгруппу $G(m)$. Обозначим через $\mathscr{M}$ множество максимальных подгрупп группы $G(q)$, не изоморфных нормализатору $N(G(m))$ подгруппы $G(m)$ в $G(q)$ для любого подполя $GF(m) \subset GF(q)$. Также положим

$$d = 1,\ 1,\ \text{НОД}\,(2, q-1) \tag{6}$$

для групп $Sz(q)$, $\mathrm{Re}(q)$, $PSL_2(q)$ соответственно.

В § 2 доказывается

Лемма 1.3. *Для функции Эйлера φ_2 на группах $G(q)$ верно неравенство:*

$$\varphi_2(G(q)) \geqslant \big|G(q)\big|\Big(|G(q)| - 3d^2\sqrt{|G(q)|}\Big) - \sum_{M \in \mathscr{M}} |M|^2. \tag{7}$$

Далее, оценка последнего слагаемого в (7) опирается на известные описания максимальных подгрупп для групп лиева типа ранга 1.

Как и в [14], в группе $G(q)$ определяем подгруппу Бореля B с унипотентным радикалом U и мономиальную подгруппу $H \leftthreetimes \langle\tau\rangle$, где H — диагональная подгруппа, а τ — подходящая инволюция. Группа $G(q)$ допускает разложение Брюа

$$G(q) = B\langle\tau\rangle B, \quad B = U \leftthreetimes H, \quad \tau^2 = 1, \quad \tau H\tau = H.$$

Разложение Брюа и каноническая форма элементов [14, теорема 8.4.3] приводят к следующей формуле порядка группы $G(q)$:

$$|G(q)| = |U||H|(1 + |U|). \tag{8}$$

Известно, что

$$|H| = (q-1)/d, \quad |\mathrm{Aut}\, G(q)| = d\, n\, |G(q)| \quad (q = p^n), \tag{9}$$

$|U|$ определяется для группы $G(q) = \mathrm{Re}\,(q)$, $Sz(q)$ или $PSL_2(q)$ равенством:

$$|U| = q^3,\ q^2 \text{ или } q \tag{10}$$

соответственно.

В группах $PSL_2(q)$ и $\mathrm{Re}\,(q)$ существует подгруппа A_1 порядка, соответственно, $(q+1)/d$ и $(q+1)/4$. В группах $Sz(q)$ и $\mathrm{Re}\,(q)$ выделяют еще циклические холловские подгруппы A_2 и A_3, причем $|A_2| = q + 1 + r$, $|A_3| = q + 1 - r$, где $r^2 = q$. Отметим, что

$$|U| + 1 = d|A_1| \quad \text{при} \quad G(q) = PSL_2(q),$$
$$|U| + 1 = |A_2||A_3| \quad \text{при} \quad G(q) = Sz(q),$$
$$|U| + 1 = 4|A_1||A_2||A_3| \quad \text{при} \quad G(q) = \mathrm{Re}\,(q).$$

В § 3 доказательство теоремы 1 распадается на три случая в зависимости от особенностей подгруппового описания группы $G(q)$ каждого типа.

2. Доказательство леммы 1.3

Если q — простое число, то группа $G(q)$ не имеет собственных подгрупп $G(m)$, поэтому утверждение леммы сразу следует из неравенства (5). Далее в этом параграфе считаем $q = p^n$, p — простое число, $n > 1$.

Если $GF(m)$ в (12) есть собственное подполе поля $GF(q)$, то $q = m^v$ для натурального числа $v > 1$. Для доказательства леммы 1.3 нам потребуется следующее вспомогательное соотношение:

$$\left|G(\sqrt[v]{q})\right| < \sqrt[v]{|G(q)|}. \tag{11}$$

Будем использовать очевидные для произвольных натуральных чисел a, b неравенства:

$$\sqrt[v]{a} - 1 \leqslant \sqrt[v]{a-1}, \quad \sqrt[v]{a+b} < \sqrt[v]{a} + \sqrt[v]{b}.$$

Если $G(q) = \mathrm{Re}\,(q)$, то легко находим

$$|\mathrm{Re}\,(\sqrt[v]{q})| = \sqrt[v]{q^3}\,\frac{\sqrt[v]{q^6} - 1}{\sqrt[v]{q^2} + \sqrt[v]{q} + 1} < \sqrt[v]{q^3}\,\frac{\sqrt[v]{q^6 - 1}}{\sqrt[v]{q^2 + q + 1}} = \sqrt[v]{|\mathrm{Re}\,(q)|}.$$

Для групп Сузуки и $PSL_2(q)$ доказательство аналогично.

Перейдем к доказательству леммы 1.3. Из неравенства (5) вытекает

$$\varphi_2(G(q)) \geqslant |G(q)|^2 - \sum_{M \in \mathscr{M}} |M|^2 - \sum_{GF(m) \subset GF(q)} c_m \big|N(G(m))\big|^2 \big|G(q) : N(G(m))\big|,$$

где c_m — число различных попарно несопряженных подгрупп, изоморфных $G(m)$. Согласно [12, 13], все подгруппы, изоморфные $G(m)$, сопряжены в случае $G(q) = Sz(q)$ или $G(q) = \mathrm{Re}\,(q)$. В случае $G(q) = PSL_2(q)$, если v — четное, то существует две несопряженные подгруппы, изоморфные $N(G(m))$, а при нечетном v — только одна. Следовательно, $c_m \leqslant d$. В силу соотношений

$$\big|N(G(m))\big|\big|G(q) : N(G(m))\big| = |G(q)|, \quad |N(G(m))| \leqslant d|G(m)|$$

получаем:

$$\varphi_2(G(q)) \geqslant |G(q)|^2 - \sum_{M \in \mathscr{M}} |M|^2 - d^2|G(q)| \sum_{GF(m) \subset GF(q)} |G(m)|. \tag{12}$$

Выберем наименьший делитель $k_1 > 1$ числа n. Положим также $k_2 = k_1$ при $k_1 = n$, а если $k_1 < n$, то через k_2 обозначаем наименьший делитель числа n, больший k_1. Наконец, k_3 — наименьший делитель числа n, больший k_2, или $k_3 = k_2$ при $k_2 = n$. Положим $n' = n/k_3$, если $k_3 > k_2 > k_1$, и $n' = 0$ в противном случае. Тогда

$$\begin{aligned}\sum_{q=m^v} |G(m)| < \sum_{q=m^v} |G(q)|^{\frac{1}{v}} \leqslant |G(q)|^{\frac{1}{k_1}} + |G(q)|^{\frac{1}{k_2}} \\ + \sum_{i=0}^{n'} |G(q)|^{\frac{i}{n}} \leqslant |G(q)|^{\frac{1}{2}} + |G(q)|^{\frac{1}{3}} + \frac{n}{4}\,|G(q)|^{\frac{1}{4}}.\end{aligned}$$

Поскольку $\frac{n}{4} \leqslant 2^{\frac{n}{4}} \leqslant \sqrt{q} \leqslant |G(q)|^{\frac{1}{4}}$, то отсюда получаем

$$\sum_{q=m^v} |G(m)| < |G(q)|^{\frac{k-1}{2}} + |G(q)|^{\frac{k-1}{3}} + \frac{n}{4}\,|G(q)|^{\frac{k-1}{4}} \leqslant 3\,|G(q)|^{\frac{k-1}{2}}.$$

Подставляя в (12) последнюю оценку, приходим к неравенству (7). Это завершает доказательство леммы 1.3.

3. Завершение доказательства теоремы 1

Для завершения доказательства основной теоремы оценим сумму $\sum_{M \in \mathscr{M}} |M|^2$ в (7) отдельно для каждого типа групп $G(q)$.

Случай группы $PSL_2(q)$. Из известного подгруппового описания группы $PSL_2(q)$ (см. [11, гл. 12]) вытекает

Лемма 3.1. *Максимальная подгруппа группы $PSL_2(q)$ либо изоморфна нормализатору $N(PSL_2(m))$ подгруппы $PSL_2(m)$ в $PSL_2(q)$ ($GF(m)$ есть подполе $GF(q)$), либо сопряжена одной из следующих подгрупп:*

1. *подгруппа B, $N(H)$ или $N(A_1)$;*

2. *при $q = 8h \pm 1$ — одна из двух несопряженных подгрупп, изоморфных симметрической группе $\mathscr{S}_4$;*

3. *при* $q = 10h \pm 1$ — *одна из двух несопряженных подгрупп, изоморфных знакопеременной группе* $\mathscr{A}_5$;

4. *при* $q = 8h \pm 3$ — *подгруппа, изоморфная знакопеременной группе* $\mathscr{A}_4$.

Перейдем к оценке значений функции d_2 на группах $G(q) = PSL_2(q)$. Пусть S есть число всех пар элементов, лежащих в одной из максимальных подгрупп, изоморфных $\mathscr{S}_4$, $\mathscr{A}_4$ или $\mathscr{A}_5$, и не изоморфных $N(G(m))$ для $GF(m) \subset GF(q)$, B, $N(H)$ или $N(A_1)$. Тогда в силу леммы 3.1

$$S \leqslant 2\,|G(q)|\big(|\mathscr{S}_4| + |\mathscr{A}_5|\big) = 168\,|G(q)|.$$

Поэтому из лемм 1.3 и 3.1 вытекают неравенства:

$$\begin{aligned} d_2(G(q)) \geqslant{}& \frac{1}{|\mathrm{Aut}\,G(q)|}\Big(|G(q)|^2 - 6d^2|G(q)|^{\frac{3}{2}} - |B|^2|G(q):B| \\ &-|N(H)|^2|G(q):N(H)| - |N(A_1)|^2|G(q):N(A_1)| - S\Big) \\ ={}& \frac{1}{d\,n}\bigg(\frac{q^3-q}{d} - 3d^{\frac{3}{2}}\sqrt{q^3-q} - \frac{q^2-q}{d} - \frac{2(q-1)}{d} - \frac{2(q+1)}{d} - 168\bigg) \\ \geqslant{}& \frac{1}{nd^2}\Big(q^3 - q^2 - 24q^{\frac{3}{2}} - 4q - 168\Big). \end{aligned}$$

С другой стороны, $\sqrt{|G(q)|} = \sqrt{q^3-q} \leqslant q^{\frac{3}{2}}$. Введем функцию

$$f(q) = \frac{1}{24}\Big(q^3 - q^2 - 24q^{\frac{3}{2}} - 4q - 168\Big) - q^{\frac{8}{5}}.$$

Учитывая неравенства $\frac{1}{n} \geqslant \frac{1}{6}2^{-\frac{n}{10}} \geqslant \frac{1}{6}\,q^{-1/10}$, получаем

$$d_2(G(q)) - \sqrt{|G(q)|} \geqslant q^{-\frac{1}{10}} f(q).$$

Дифференцируя функцию $f(q)$ три раза по q, находим:

$$f'''(q) = \frac{1}{4} + \frac{3}{8\cdot q^{\frac{3}{2}}} + \frac{48}{125\cdot q^{\frac{7}{5}}} > 0 \quad (q > 0).$$

Поскольку значения $f(16) \approx 1.88$, $f'(16) \approx 16.1$ и $f''(16) \approx 3.41$ также положительны, то функции $f(q)$, $f'(q)$ и $f''(q)$ возрастают и положительны при $q \geqslant 16$. Поэтому неравенство (2) доказано для случая $q \geqslant 16$. В оставшихся случаях неравенство подтверждаем, вычислив значения $d_2(G(q))$ с помощью GAP [15]:

$$\begin{gathered} d_2(G(4)) = d_2(G(5)) = 19; \quad d_2(G(7)) = 57; \quad d_2(G(8)) = 213; \\ d_2(G(9)) = 53; \quad d_2(G(11)) = 660; \quad d_2(G(13)) = 495. \end{gathered}$$

Тем самым, доказательство неравенства (2) для групп $PSL_2(q)$ завершено.

Случай группы $Sz(q)$. Максимальные подгруппы группы Сузуки $Sz(q)$ описаны в статье М. Сузуки [13].

Лемма 3.2. *Максимальная подгруппа группы* $Sz(q)$, $q = 2^{2k+1}$, *сопряжена одной из подгрупп* B, $N(H)$, $N(A_2)$, $N(A_3)$, $Sz(m)$, *где* $GF(m) \subset GF(q)$.

Из лемм 1.3 и 3.2 следует оценка:

$$d_2(G(q)) \geqslant \frac{1}{|\mathrm{Aut}\, G(q)|}\Big(|G(q)|^2 - 3|G(q)|^{\frac{3}{2}} - |B|^2|G(q):B| - |N(H)|^2|G(q):N(H)|$$
$$-|N(A_2)|^2|G(q):N(A_2)| - |N(A_3)|^2|G(q):N(A_3)|\Big) = \frac{1}{n}\Big(|G(q)| - 3|G(q)|^{\frac{1}{2}}$$
$$-|B| - |N(H)| - |N(A_2)| - |N(A_3)|\Big) \geqslant \frac{1}{6}\, q^{\frac{-1}{10}}\Big(q^5 - q^4 - 3q^{\frac{5}{2}} - 10q - 6\Big).$$

Для функции

$$f(q) = \frac{1}{6}\Big(q^5 - q^4 - 3q^{\frac{5}{2}} - 10q - 6\Big) - q^{\frac{13}{5}}$$

выполняется неравенство $d_2(G(q)) - \sqrt{|G(q)|} \geqslant q^{-\frac{1}{10}} f(q)$. С другой стороны, дифференцируя функцию $f(q)$ шесть раз по q, находим

$$f^{VI}(q) = \frac{225}{128\, q^{\frac{7}{2}}} + \frac{52416}{15625\, q^{\frac{17}{5}}} > 0 \quad \text{при} \quad q > 0.$$

Отсюда, как и выше, функция $f(q)$ и ее производные порядка $\leqslant 5$ возрастают и положительны при $q \geqslant 8$. Таким образом, оценка (2) подтверждена для групп $Sz(q)$.

Случай группы $\mathrm{Re}\,(q)$**.** Известно, что в группе $\mathrm{Re}\,(q)$ все инволюции (даже все 2-подгруппы одного порядка) сопряжены. Ее максимальные подгруппы перечислены в [12, теорема 1].

Лемма 3.3. *Максимальная подгруппа группы* $\mathrm{Re}\,(q)$ *сопряжена одной из следующих подгрупп: централизатор* $C(\tau)$ *инволюции* τ*;* $G(m)$*, где* $q = m^v$*,* v *— простое число;* B*;* $N(A_1)$*;* $N(A_2)$*;* $N(A_3)$*.*

Отсюда для групп $G(q) = \mathrm{Re}\,(q)$ имеем оценку:

$$d_2(G(q)) \geqslant \frac{1}{|\mathrm{Aut}\, G(q)|}\Big(|G(q)|^2 - 3|G(q)|^{\frac{3}{2}} - |B|^2 \cdot |G(q):B| C(\tau)|^2\, |G(q):C(\eta)|$$
$$-|N(A_1)|^2\, |G(q):N(A_1)| - |N(A_2)|^2\, |G(q):N(A_2)| - |N(A_3)|^2\, |G(q):N(A_3)|\Big)$$
$$\geqslant \frac{1}{n}\Big(|G(q)| - 3|G(q)|^{\frac{1}{2}} - |B| - |N(A_1)| - |N(A_2)| - |N(A_3)| - |C(\tau)|\Big)$$
$$= \frac{1}{n}\Big(q^7 - q^6 - 2q^4 - 3q^{\frac{7}{2}} + q^3 - 17q - 18\Big).$$

Для функции

$$f(q) = \frac{1}{6}\Big(q^7 - q^6 - 2q^4 - 3q^{\frac{7}{2}} + q^3 - 17q - 18\Big) - q^{\frac{18}{5}}$$

имеем $d_2(G(q)) - \sqrt{|G(q)|} \geqslant q^{-\frac{1}{10}} f(q)$. С другой стороны, продифференцировав $f(q)$ шесть раз по q, имеем:

$$f^{VI}(v) = 840 + \frac{1575}{256\, q^{\frac{7}{2}}} + \frac{943488}{78125\, q^{\frac{17}{5}}} \geqslant 0 \quad \text{при всех} \quad q > 0.$$

Как и в предыдущих двух случаях, функция $f(q)$ и ее производные порядка $\leqslant 5$ возрастают и положительны при $q \geqslant 27$. Отсюда следует справедливость оценки (2) для групп $\mathrm{Re}\,(q)$.

Таким образом, доказательство теоремы 1 полностью завершено.

Литература

1. *Hall Ph.* The Eulerian functions of a group // Quart. J. Math.—1936.—Vol. 7.—P. 134–151.
2. Коуровская тетрадь. Нерешенные вопросы теории групп. Изд. 17-е, дополненное.—Новосибирск: ИМ СО РАН, 2010.—219 с.
3. *Сучков Н. М., Приходько Д. М.* О числе пар порождающих групп $L_2(2^m)$ и $Sz(2^{2k+1})$ // Сиб. мат. журн.—2001.—Т. 42, № 5.—С. 1162–1167.
4. *Erfanian A., Rezaei R.* On the growth sequence of PSp(2m,q) // Intern. J. Algebra.—2007.—Vol. 1, № 2.—P. 51–62.
5. *Erfanian A.* A note on growth sequences of alternating groups // Arch. Math.—2002.—Vol. 78, № 4.—P. 257–262.
6. *Erfanian A.* A note on growth sequences of $PSL(m, q)$ // Southeast Asian Bull. Math.—2005.—Vol. 29, № 4.—P. 697–713.
7. *Левчук Д. В.* Функции Ф. Холла на группах лиева типа ранга 1 // Владикавк. мат. журн.—2008.—Т. 10, № 1.—С. 37–39.
8. *Ушаков Ю. Ю.* Оценка второй функции Эйлера на группах лиева типа ранга 1 // Тр. конф. «Алгебра, логика и приложения».—Красноярск: СФУ, 2010.—С. 101–102.
9. *Приходько Д. М.* О числе пар порождающих элементов некоторых групп $L_2(q)$ // Материалы 34-ой науч. студ. конф.—Красноярск: КрасГУ, 2001.—С. 91–102.
10. *Erfanian A.* Growth Sequence of Free Product of Alternating Groups // Int. J. Contemp. Math. Sc.—2007.—Vol. 2, № 14.—P. 685–691.
11. *Dickson L. E.* Linear groups.—Leipzig, 1901.
12. *Левчук В. М., Нужин Я. Н.* О строении групп Ли // Алгебра и логика.—1985.—Т. 24, № 1.—С. 26–41.
13. *Suzuki M.* On a class of doubly transitive groups // Ann. Math.—1962.—Vol. 75, № 1.—P. 105–145.
14. *Carter R. W.* Simple Groups of Lie Type.—London: Wiley and sons, 1972.—346 p.
15. http: // www.gap-system.org.

Статья поступила 15 января 2011 г.

Ушаков Юрий Юрьевич
Сибирский федеральный университет,
аспирант каф. алгебры и мат. логики
РОССИЯ, 660041, Красноярск, пр. Свободный, 79
E-mail: yuron@akadem.ru

AN EVALUATION OF THE PH. HALL FUNCTION ON RANK 1 GROUPS OF LIE TYPE

Ushakov Yu. Yu.

In 1936 Ph. Hall introduced the generalized n-th Eulerian function on finite groups and the associated function that is called the n-th Hall function. The values of the latter are estimated in the article for three of the four series of Lie type groups of rank 1. When $n = 2$, these evaluations confirm the Wiegold conjecture for the groups.

Key words: n-base of a group, generalized Eulerian function, Hall function, Lie type group.