Math-Net.Ru

Общероссийский математический портал

Т. Г. Петросян, Верхняя оценка числа множеств, свободных от произведений, в одном классе групп, *Дискрет. матем.*, 2007, том 19, выпуск 1, 76–88

DOI: <https://doi.org/10.4213/dm10>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением

<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 54.92.164.108

26 апреля 2023 г., 16:58:53

Верхняя оценка числа множеств, свободных от произведений, в одном классе групп

© 2007 г. Т. Г. Петросян

В работе получена оценка числа множеств, свободных от произведений, в конечных группах, содержащих нормальную подгруппу простого индекса.

1. Введение

Введем обозначение

$$AB = \{ab: a \in A, b \in B\}.$$

Множество A элементов группы G называется свободным от произведений, если $AA \cap A = \emptyset$ или, что эквивалентно, уравнение $xy = z$ не имеет решений в множестве A . Семейство всех подмножеств группы G , свободных от произведений, обозначим через $\mathcal{P}(G)$. Пусть

$$P(G) = |\mathcal{P}(G)|, \quad P(n) = \max_{|G|=n} P(G).$$

Н. Алон в [5] показал, что верна следующая теорема. Здесь и далее логарифмы берутся по основанию два.

Теорема 1. *Справедлива оценка*

$$\log P(n) \leq n(1/2 + \varepsilon(n)),$$

где $\varepsilon(n) \rightarrow 0$ при $n \rightarrow \infty$.

В. Ф. Лев, Т. Лучак и Т. Шон в [7] и независимо А. А. Сапоженко в [2] получили асимптотику числа множеств, свободных от произведений в абелевых группах четного порядка.

Теорема 2. *Для любой абелевой группы G четного порядка n с числом подгрупп индекса 2, равным t , выполняются неравенства*

$$t2^{n/2} - 2^{(n/4)(1+\varepsilon(n))} \leq P(G) \leq t2^{n/2} + 2^{n(1/2-c)}, \quad (1)$$

где c — положительная постоянная и $\varepsilon(n) \rightarrow 0$ при $n \rightarrow \infty$.

Для константы c в [7] указано значение 10^{-8} , а в [2] значение 0,017.

Недавно Б. Грин и И. З. Ружа получили асимптотику логарифма числа множеств, свободных от произведений, в классе абелевых групп. Пусть $\mu(G) = 1/3 + 1/(3p)$, если p является наименьшим простым делителем n вида $p \equiv 2 \pmod{3}$, если такого делителя нет, но $3 \mid n$, то $\mu(G) = 1/3$, в противном случае, $\mu(G) = 1/3 - 1/(3m)$, где m — экспонента группы G .

Теорема 3. Для любой конечной абелевой группы G порядка n

$$\log |\mathcal{P}(G)| = \mu(G)n(1 + o(1))$$

при $n \rightarrow \infty$.

Теорема 2 была обобщена автором (см. [1]) на случай конечных групп, содержащих подгруппу индекса 2.

Теорема 4. Для любой группы G порядка n с числом подгрупп индекса 2, равным t , $t \geq 1$,

$$t2^{n/2} - 2^{n(1+\varphi(n))/4} \leq P(G) \leq t2^{n/2} + 2^{n(1/2-\varepsilon)}, \quad (2)$$

где $\varepsilon > 0$, $\varphi(n) \rightarrow 0$ при $n \rightarrow \infty$ и второе неравенство справедливо, начиная с некоторого n .

В настоящей работе доказывается следующая теорема.

Теорема 5. Пусть G — конечная группа порядка n , а K — ее нормальная подгруппа наименьшего простого индекса. Пусть $|G : K| = p$, $p \geq 3$, где p — простое число. Тогда

$$2^{\lceil (p-1)/3 \rceil n/p} \leq P(G) \leq 2^{(n/2)(1-0,004/p)}. \quad (3)$$

2. Основные понятия

Пусть G — группа, $A \subset G$, $e \notin A$, $A^{-1} = \{a^{-1}, a \in A\}$. Граф с множеством вершин G , в котором ребрами являются пары $\{u, v\}$ такие, что $u^{-1}v \in (A \cup A^{-1})$, будем называть графом Кэли $\mathcal{C}_A(G)$ на множестве G относительно множества A . Из определения следует, что $\mathcal{C}_A(G)$ — регулярный граф степени $|A \cup A^{-1}|$. Множество U вершин графа Γ называется независимым, если подграф, порожденный множеством U , является пустым. Семейство всех независимых множеств графа Γ обозначим через $\mathcal{I}(\Gamma)$. Пусть $A \subset G$ и $B \subseteq G$. Через $\mathcal{C}_A(B)$ обозначим подграф графа $\mathcal{C}_A(G)$, порожденный множеством B . Ясно, что каждое множество $B \in \mathcal{P}(G)$ является независимым в графе $\mathcal{C}_A(G)$ при любом непустом $A \subseteq B$.

Пусть $\Gamma = (V, E)$ и $A \subset V$. Множество

$$\partial(A) = \{v \in V \setminus A : \exists u \in A \text{ такое, что } (u, v) \in E\}$$

называется границей A в графе Γ . Граф $\Gamma = (V, E)$ называется δ -расширителем, если $|A| \leq (1 - \delta)|\partial(A)|$ для любого независимого $A \subset V$.

Множество D , свободное от произведений, называется максимальным, если не существует другого множества S , свободного от произведений, такого, что $|S| > |D|$.

3. Вспомогательные утверждения

В работе используются следующие результаты.

Теорема 6 (Коши–Дэвенпорт, [6]). Пусть A и B — непустые подмножества группы G простого порядка. Тогда либо $A + B = G$, либо $|A + B| \geq |A| + |B| - 1$.

Теорема 7 (Сапоженко, [3]). Пусть Γ — n -вершинный регулярный граф степени k . Тогда

$$|\mathcal{F}(\Gamma)| \leq 2^{(n/2)(1+O(\sqrt{(\log k)/k}))}. \quad (4)$$

Теорема 8 (Сапоженко, [3]). Для любого n -вершинного регулярного графа Γ степени k и числа β такого, что $0 < \beta < 1$, пусть $I_\beta(\Gamma)$ — число независимых множеств A графа Γ таких, что $|A| - n/4 \geq \beta n/4$. Тогда

$$I_\beta(\Gamma) \leq 2^{(n/2)(1-\beta^2/(2\ln 2)+O(\sqrt{(\log k)/k}))}. \quad (5)$$

Теорема 9 (Сапоженко, [3]). Пусть $\Gamma = (V; E)$ — n -вершинный регулярный граф степени k , являющийся δ -расширителем для некоторого $0 \leq \delta < 1$. Тогда

$$|\mathcal{F}(\Gamma)| \leq 2^{(n/2)(1-\delta/7+O(\sqrt{(\log k)/k}))}.$$

Теорема 10 (Олсон, [9]). Пусть A и B являются конечными непустыми подмножествами группы G , тогда существует подмножество S множества AB и подгруппа H группы G такие, что $|S| \geq |A| + |B| - |H|$, и либо $SH = S$, либо $HS = S$.

Следствие 1. Пусть A и B являются конечными непустыми подмножествами группы G , тогда существует подмножество T множества AB и подгруппа S группы G такие, что $|T| \geq |A| + |B| - |S|$, и T содержит хотя бы один левый смежный класс по подгруппе S .

Доказательство. Из теоремы 10 следует, что существует подгруппа H такая, что $|T| \geq |A| + |B| - |H|$, и либо $TH = T$, либо $HT = T$. Если $TH = T$, то следствие доказано. Пусть $HT = T$. Следовательно, T содержит некоторый правый смежный класс R по подгруппе H . Рассмотрим сопряженную к H подгруппу $S = R^{-1}R$. Очевидно, что R является левым смежным классом по подгруппе S и $|S| = |H|$.

Теорема 11 (Олсон, [9]). Пусть A и B являются конечными подмножествами группы G , тогда либо $ABV^{-1}B = AB$, либо $|AB| \geq |A| + (1/2)|B|$.

Доказательство следующей леммы содержится, например, в [4] (лемма 6.8).

Лемма 1. Справедливо неравенство

$$\sum_{i=0}^{\lfloor \lambda m \rfloor} \binom{m}{i} \leq 2^{m\lambda \log(e/\lambda)}.$$

Леммы 2–4 доказаны в [1].

Лемма 2. Пусть L и H являются подгруппами группы G , а множество T — произвольный левый (правый) смежный класс группы G по H такой, что $L \cap T \neq \emptyset$. Тогда множество $L \cap T$ является левым (правым) смежным классом по подгруппе $L \cap H$.

Пусть даны две подгруппы X и H некоторой группы G . Число левых (или правых) смежных классов группы G по подгруппе H , с которыми подгруппа X имеет непустое пересечение, назовем типом подгруппы X относительно подгруппы H .

Пусть T и R — левый и правый, соответственно, смежные классы группы G по подгруппе H . Введем обозначения $TT^{-1} = H_T$ и $R^{-1}R = H_R$. Очевидно, что множества H_T и H_R являются подгруппами группы G , сопряженными с подгруппой H .

Лемма 3. Пусть $T \cap R \neq \emptyset$. Тогда $T \cap R$ является левым смежным классом по подгруппе $H_R \cap H$ и правым смежным классом по подгруппе $H_T \cap H$.

Лемма 4. Пусть H является подгруппой группы G . Тогда произвольный левый (правый) смежный класс T группы G по H имеет непустое пересечение ровно с v правыми (левыми) смежными классами группы G по H , где v является типом подгруппы TT^{-1} ($T^{-1}T$) относительно H . При этом мощность пересечения смежного класса T с каждым правым (левым) смежным классом, имеющим непустое пересечение с T , равна $|H|/v$.

Условимся через $a_k(G)$ обозначать число подгрупп индекса k группы G . Определим функцию $t_k(x)$ следующим образом:

$$t_k(x) = \begin{cases} \max_{|G|=x} a_k(G), & x \in \mathbf{N}, \\ 0 & \text{в противном случае.} \end{cases}$$

Лемма 5. Для любых натуральных чисел k и n верно соотношение

$$t_k(n) \leq \sum_{l=1}^k t_l(n/k) \binom{k-1}{l-1} l^{l-1}. \quad (6)$$

Следствие 2. Существуют такие положительные константы c_1 и c_2 , что

$$t_2(n) \leq n - 1, \quad t_3(n) \leq c_1 n^2, \quad t_4(n) \leq c_2 n^5.$$

4. Доказательство теоремы 5

Пусть K — нормальная подгруппа простого индекса p , $p \geq 3$, группы G порядка n , причем в G не существует нормальной подгруппы простого индекса, меньшего чем p . Обозначим смежные классы группы G по нормальной подгруппе K через $K_0 = K, \dots, K_{p-1}$, таким образом, что при изоморфизме $G/K \rightarrow \mathbf{Z}_p$ класс K_i соответствует $i \in \mathbf{Z}_p$. Пусть $D \in \mathcal{P}(G)$. Введем обозначения

$$\begin{aligned} A &= D \cap K, & D_i &= D \cap K_i, \\ D_i(A) &= \{D \in \mathcal{P}_i(G) : D \cap K = A\}, \end{aligned}$$

где семейства $\mathcal{P}_i(G)$ будут определены позднее и $m = n/p$.

Оценка снизу тривиальна. Действительно, из теоремы 6 следует, что размер максимального множества, свободного от произведений, в циклической группе простого порядка p равен $\lceil (p-1)/3 \rceil$. Рассмотрим произвольное максимальное множество, свободное от произведений, в факторгруппе $G/K \simeq \mathbf{Z}_p$. Полный прообраз этого множества при естественном гомоморфизме $G \rightarrow G/K$ является множеством, свободным от произведений, размера $\lceil (p-1)/3 \rceil m$. Поскольку любое подмножество множества, свободного от

произведений, само является множеством, свободным от произведений, получаем оценку снизу в теореме 5.

Выберем α и β такими, что

$$1 - 6\alpha \log \frac{e}{\alpha} \geq 0,9, \quad (7)$$

$$2\alpha \log \frac{e}{\alpha} - \frac{\beta^2}{2 \ln 2} < -0,004. \quad (8)$$

Рассмотрим следующие семейства множеств, свободных от произведений.

1. Пусть

$$\mathcal{P}_1(G) = \{D \in \mathcal{P}(G) : |A| < \alpha m\}.$$

1.1. Введем обозначение

$$\mathcal{P}_1^1(G) = \{D \in \mathcal{P}_1(G) : |D_i| < \alpha m, i = 1, \dots, p-1\}.$$

Используя лемму 1, получаем, что

$$|\mathcal{P}_1^1(G)| \leq \left(\sum_{i=0}^{\lfloor \alpha m \rfloor} \binom{m}{i} \right)^p \leq 2^{\alpha n \log(e/\alpha)}. \quad (9)$$

1.2. Рассмотрим семейство

$$\mathcal{P}_1^2(G) = \{D \in \mathcal{P}_1(G) : \exists s \in \{1, \dots, p-1\} \text{ такое, что } |D_s| \geq \alpha m\}.$$

Построим графы Кэли на парах смежных классов. Рассмотрим разбиение множества $\{K_1, \dots, K_{p-1}\}$ на пары (K_i, K_j) . Пусть $K_t K_t = K_s$, то есть $t = s/2 \pmod{p}$. Тем самым образована первая пара (K_t, K_s) . Далее пары строятся следующим образом: $K_{j_v} = K_{i_v}^{-1} K_s$, где $i_v \leq p-1$, — это наименьшее натуральное число, не принадлежащее $\{t, s, i_1, \dots, i_{v-1}, j_1, \dots, j_{v-1}\}$. Ясно, что пары (K_{i_v}, K_{j_v}) , $v = 1, \dots, p-3$, не имеют общих элементов друг с другом и с парой (K_t, K_s) .

Пусть $Q \subset K_s$, $|Q| = \lfloor \alpha m \rfloor$. Рассмотрим граф $\mathcal{F}_Q^m(K_{i_v}, K_{j_v})$, множеством вершин которого является $K_{i_v} \cup K_{j_v}$, а две вершины u и v соединяются ребром, только если $uv \in Q$, $u \in K_{i_v}$, $v \in K_{j_v}$. Легко видеть, что граф $\mathcal{F}_Q^m(K_{i_v}, K_{j_v})$ является двудольным регулярным графом степени $|Q|$. Согласно теореме 7

$$I(\mathcal{F}_Q^m(K_{i_v}, K_{j_v})) \leq 2^{m(1+o(1))}.$$

Используя лемму 1, получаем, что число способов выбора множества A не превосходит

$$\sum_{i=0}^{\lfloor \alpha m \rfloor} \binom{m}{i} \leq 2^{\alpha m \log(e/\alpha)}.$$

Пусть $|D_t| < \alpha m$. Тогда число множеств D_t по лемме 1 не превосходит

$$\sum_{i=0}^{\lfloor \alpha m \rfloor} \binom{m}{i} \leq 2^{\alpha m \log(e/\alpha)}.$$

Учитывая неравенство (7), получаем, что число множеств $D \in \mathcal{P}_1^2(G)$ таких, что $|D_t| < \alpha m$, не превосходит

$$\binom{m}{\lfloor \alpha m \rfloor} 2^{\alpha m \log(e/\alpha)} 2^{\alpha m \log(e/\alpha)} 2^{m(p-3)/2(1+o(1))} 2^m \leq 2^{(n/2)(1-(1-6\alpha \log(e/\alpha))/p)} \leq 2^{(n/2)(1-0,9/p)}. \quad (10)$$

Пусть теперь $|D \cap K_t| \geq \alpha m$, а $R \subset K_t$, $|R| = \lfloor \alpha m \rfloor$. Рассмотрим граф $\mathcal{F}_R^d(K_s, K_t)$, множеством вершин которого является $K_s \cup K_t$, а две вершины u и v соединены ребром, только если $u^{-1}v \in R$, $u \in K_t$, $v \in K_s$. Легко видеть, что этот граф является регулярным двудольным графом степени $|R|$. Из теоремы 7 следует, что

$$I(\mathcal{F}_R^d(K_s, K_t)) \leq 2^{m(1+o(1))}.$$

С учетом (7), получаем, что число множеств $D \in \mathcal{P}_1^2(G)$ таких, что $|D_t| \geq \alpha m$, не превосходит

$$\binom{m}{\lfloor \alpha m \rfloor} 2^{\alpha m \log(e/\alpha)} 2^{(m/2)(p-1+o(1))} \leq 2^{(n/2)(1-(1-4\alpha \log(e/\alpha))/p)} \leq 2^{(n/2)(1-0,9/p)}. \quad (11)$$

Из неравенств (10) и (11) следует, что

$$|\mathcal{P}_1^2(G)| \leq 2^{(n/2)(1-0,9/p)}. \quad (12)$$

Итак, из неравенств (9) и (12) получаем оценку

$$|\mathcal{P}_1(G)| \leq 2^{(n/2)(1-0,9/p)}. \quad (13)$$

2. Оценим число элементов семейства

$$\mathcal{P}_2(G) = \{D \in \mathcal{P}(G) : \alpha m \leq |A| \leq (1-\beta)m/4\}.$$

Пусть $F \subset K$ и $|F| = \lfloor \alpha m \rfloor$. Рассмотрим граф Кэли $\mathcal{C}_F(K)$. Используя теорему 8, получаем, что

$$\mathcal{J}(\mathcal{C}_F(K)) \leq 2^{(m/2)(1-\beta^2/(2 \ln 2)+o(1))}.$$

Из теоремы 7 следует, что

$$\mathcal{J}(\mathcal{C}_F(K_i)) \leq 2^{(m/2)(1+o(1))}, \quad i = 1, \dots, p-1.$$

Таким образом,

$$\begin{aligned} |\mathcal{P}_2(G)| &\leq \binom{m}{\lfloor \alpha m \rfloor} 2^{(m/2)(1-\beta^2/(2 \ln 2)+o(1))} 2^{(m/2)(p-1+o(1))} \\ &= 2^{(m/2)(p+2\alpha \log(e/\alpha)-\beta^2/(2 \ln 2)+o(1))}. \end{aligned}$$

Отсюда с учетом (8) получаем, что

$$|\mathcal{P}_2(G)| \leq 2^{(n/2)(1-0,004/p)}. \quad (14)$$

3. Пусть семейство $\mathcal{P}_3(G)$ состоит из множеств $D \in \mathcal{P}(G)$, для которых выполнено условие $|A| > (1 - \beta)m/4$ и существует подгруппа H индекса 2 группы K такая, что $A \subseteq H'$, где $H' = K \setminus H$.

По условию группа G не имеет подгруппы индекса 2, поэтому подгруппа H не является нормальной подгруппой группы G . Действительно, допустим, что $H \triangleleft G$. Тогда, поскольку $|G/H| = 2p$, в G/H должна была бы существовать подгруппа индекса 2, а из этого следовало бы существование подгруппы индекса 2 в G . Итак, существует некоторый элемент $x \in G$ такой, что

$$xHx^{-1} \neq H. \quad (15)$$

Очевидно, что $x \notin K$. Без ограничения общности можно считать, что $x \in K_1$. Пусть K_{1j} — левые смежные классы по подгруппе H группы G , содержащиеся в K_1 , здесь и далее $j = 1, 2$. Заметим, что $K_{11}K_{11}^{-1} = K_{12}K_{12}^{-1}$. Введем обозначения

$$H_1 = K_{1j}K_{1j}^{-1}, \quad A_0 = A \cap H_1, \quad A_1 = A \setminus A_0, \quad D_{1j} = D \cap K_{1j}.$$

3.1. Пусть

$$\mathcal{P}_{31}(G) = \{D \in \mathcal{P}_3(G) : |A_0| < \alpha m\}.$$

Пусть $0 < \alpha < 1/2$, $0 < \beta < 1$ и $0 < \eta < 1$ удовлетворяют неравенству

$$2\alpha \log \frac{e}{\alpha} + \frac{\beta + \alpha}{2} < 0,1.$$

Поскольку для всех $A \in D_A$, $D_A \in \mathcal{P}_{31}(G)$,

$$|A \setminus A_0| > \frac{1 - \beta - 4\alpha}{4}m,$$

число способов выбора множеств A , $D_A \in \mathcal{P}_{31}(G)$, не превосходит

$$\sum_{i=0}^{\lfloor \alpha m \rfloor} \binom{m/4}{i} \sum_{i=0}^{\lceil (\beta + \alpha)m/4 \rceil} \binom{m/4}{i} \leq 2^{m(\alpha \log(e/\alpha) + (\beta + \alpha)/4)}. \quad (16)$$

Рассмотрим граф Кэли $\mathcal{C}_A(K_i)$, $i = 1, \dots, p-1$. Используя (16) и теорему 7, получаем оценку

$$|\mathcal{P}_{31}(G)| \leq 2^{(m/2)(2\alpha \log(e/\alpha) + (\beta + \alpha)/2)} 2^{(m/2)(p-1+o(1))} \leq 2^{(n/2)(1-0,9/p)}. \quad (17)$$

3.2. Обозначим $\mathcal{P}_{32}(G)$ семейство множеств $D \in \mathcal{P}_3(G)$ таких, что $|A_0| \geq \alpha m$ и одно из множеств D_{11} и D_{12} пусто. Для определенности будем считать, что $D_{12} = \emptyset$. Рассмотрим граф Кэли $\mathcal{C}_{A_0}^r(K_{11})$. Используя теорему 7 получаем, что

$$\mathcal{F}(\mathcal{C}_{A_0}^r(K_{12})) \leq 2^{(m/4)(1+o(1))}. \quad (18)$$

Рассмотрим графы Кэли $\mathcal{C}_A(K_s)$, $s = 2, \dots, p-1$. Согласно теореме 7

$$\mathcal{F}(\mathcal{C}_A(K_s)) \leq 2^{(m/2)(1+o(1))}. \quad (19)$$

Так как число выборов множества A не превосходит $2^{m/2}$, из (18) и (19) получаем, что

$$|\mathcal{P}_{32}(G)| \leq 2^{m/2} 2^{(m/4)(1+o(1))} 2^{(m/2)(p-2+o(1))} \leq 2^{(n/2)(1-1/(2p)+o(1))}. \quad (20)$$

3.3. Обозначим через $\mathcal{P}_3^3(G)$ семейство множеств $D \in \mathcal{P}_3(G)$ таких, что множества D_{11} и D_{12} не пусты и одно из них по мощности не превосходит γm , где γ — некоторая положительная константа. Без ограничения общности можно считать, что $|D_{12}| \leq \gamma m$.

Пусть $0 < \gamma < 1$ таково, что

$$\gamma \log \frac{e}{2\gamma} + \frac{1}{2} \log 3 - 2 \leq -1.$$

Построим граф $\Gamma_b(H' \cup K_{11})$, $b \in K_{12}$, на множестве $H' \cup K_{11}$, в котором пара $\{u, v\}$ является ребром тогда и только тогда, когда один из элементов u и v , скажем u , лежит в K_{11} и выполняется равенство $uv = b$. Ясно, что граф $\Gamma_b(H' \cup K_{11})$ является паросочетанием. Легко видеть, что

$$|\mathcal{F}(\Gamma_b(H' \cup K_{11}))| = 3^{m/2}.$$

Выберем множество D_{12} в смежном классе K_{12} . Это можно сделать $\sum_{1 \leq i \leq \gamma m} \binom{m/2}{i}$ способами. Пусть $b \in D_{12}$. Выберем множество $F \subset H' \cup K_{11}$, независимое в графе $\Gamma_b(H' \cup K_{11})$. Рассмотрим графы Кэли $\mathcal{C}_A(K_s)$, $s = 2, \dots, p-1$. В силу теоремы 7

$$\mathcal{F}(\mathcal{C}_A(K_s)) \leq 2^{(m/2)(1+o(1))}.$$

Таким образом,

$$\begin{aligned} |\mathcal{P}_3^3(G)| &\leq \sum_{1 \leq i \leq \gamma m} \binom{m/2}{i} 3^{m/2} 2^{(m/2)(p-2+o(1))} \\ &\leq 2^{m(\gamma \log(e/(2\gamma)) + (1/2) \log 3 + p - 2 + o(1))} \leq 2^{n(1-1/p)}. \end{aligned} \quad (21)$$

3.4. Оценим мощность семейства

$$\mathcal{P}_3^4(G) = \{D \in \mathcal{P}_3(G) : |D_{11}| > \gamma m, |D_{12}| > \gamma m\}.$$

Пусть $F \subset H'$, $F_j \subset K_{1j}$ и $|F| = |F_j| = \lfloor \alpha m \rfloor$, а $\tilde{F} = (F, F_1, F_2)$. Пусть $0 < \alpha < 1$ таково, что

$$\alpha \leq \gamma, \quad \frac{3}{4} + 3\alpha \log \frac{e}{2\alpha} < 1.$$

Рассмотрим граф $\mathcal{L}_{\tilde{F}}(H' \cup K_{11} \cup K_{12})$ на множестве $H' \cup K_{11} \cup K_{12}$, в котором пара $\{u, v\}$ является ребром в том и только том случае, когда выполняется одно из следующих условий:

- (i) $u \in H'$, $v \in K_{11}$ и $vu \in F_2$,
- (ii) $u \in H'$, $v \in K_{12}$ и $vu \in F_1$,
- (iii) $u \in K_{11}$, $v \in K_{12}$ и $u^{-1}v \in F$.

Нетрудно проверить, что граф $\mathcal{L}_F(H' \cup K_{11} \cup K_{12})$ является $2\lfloor \alpha m \rfloor$ -регулярным.

Воспользовавшись теоремой 7, получим оценку

$$|\mathcal{F}(\mathcal{L}_F(H' \cup K_{11} \cup K_{12}))| \leq 2^{(3/4)m(1+o(1))}.$$

Выберем тройку $\tilde{F}$, затем множества, независимые в графе $\mathcal{L}_{\tilde{F}}(H' \cup K_{11} \cup K_{12})$. Затем, как и в п. 2 и 3, выберем множества, независимые в графах $\mathcal{C}_A(K_s)$, $s = 2, \dots, p-1$. Таким образом, получаем оценку

$$\begin{aligned} |\mathcal{P}_3^4(G)| &\leq \binom{m/2}{\lfloor \alpha m \rfloor}^3 2^{(3/4)m(1+o(1))} 2^{(m/2)(p-2+o(1))} \\ &\leq 2^{m(3/4+3\alpha \log(e/(2\alpha)+o(1)))} 2^{(m/2)(p-2+o(1))} \leq 2^{(n/2)(1-1/p)}. \end{aligned} \quad (22)$$

Из неравенств (17), (20)–(22) следует оценка

$$|\mathcal{P}_3(G)| \leq 2^{(n/2)(1-1/(2p))}. \quad (23)$$

4. Введем следующие обозначения. Пусть

$\mathcal{P}_4^1(G)$ — семейство множеств $D \in (\mathcal{P}(G) \setminus \mathcal{P}_1(G))$ таких, что множество A содержится в смежном классе по некоторой подгруппе индекса 4 группы K ;

$\mathcal{P}_4^2(G)$ — семейство множеств $D \in (\mathcal{P}(G) \setminus \mathcal{P}_1(G))$ таких, что A содержится в смежном классе по некоторой подгруппе индекса 3 группы K ;

$\mathcal{P}_4^3(G)$ — семейство множеств $D \in (\mathcal{P}(G) \setminus \mathcal{P}_1(G))$ таких, что множество A содержится в объединении трех смежных классов по некоторой подгруппе индекса 8, содержащейся в некоторой подгруппе индекса 4 группы K ;

$$\mathcal{P}_4(G) = \mathcal{P}_4^1(G) \cup \mathcal{P}_4^2(G) \cup \mathcal{P}_4^3(G).$$

Оценим мощность семейства $\mathcal{P}_4^3(G)$. Из следствия 2 вытекает, что число подгрупп индекса 8, содержащихся в некоторой подгруппе индекса 4, не больше чем cm^6 , где c — некоторая положительная константа. Выбрать множество A можно не более чем $\binom{8}{3} 2^{3m/8}$ способами. Множество D_i выберем независимым в графе $\mathcal{C}_A(D_i)$. Применив теорему 7 к графам $\mathcal{C}_A(K_i)$, $i = 1, \dots, p-1$, получаем, что

$$|\mathcal{P}_4^3(G)| \leq cm^6 \binom{8}{3} 2^{3m/8} 2^{(m/2)(p-1+o(1))} \leq 2^{(n/2)(1-1/(4p)+o(1))}.$$

Нетрудно проверить, что

$$|\mathcal{P}_4^1(G)| = o(|\mathcal{P}_4^3(G)|), \quad |\mathcal{P}_4^2(G)| = o(|\mathcal{P}_4^3(G)|).$$

Таким образом,

$$|\mathcal{P}_4(G)| \leq 2^{(n/2)(1-1/(4p)+o(1))}. \quad (24)$$

5. Рассмотрим теперь семейство $\mathcal{P}_5(G)$ множеств $D \in \mathcal{P}(G) \setminus \mathcal{P}_4(G)$ таких, что $|A| > (1-\beta)m/4$ и для любой подгруппы H индекса 2 группы K

$$A \cap H \neq \emptyset. \quad (25)$$

Пусть $i \in \mathbb{N}$ и $i \leq p - 1$. Далее будет показано, что для любого подмножества $A \in D_5(A)$ граф $\mathcal{C}_A(K_i)$ является δ -расширителем при $\delta = (1 - 5\beta)/(11 - 5\beta)$. Заметим, что в графе $\mathcal{C}_A(K_i)$ выполняется равенство

$$\partial(N) = N(A \cup A^{-1}), \quad (26)$$

для любого непустого множества $N \subset K_i$. Рассмотрим следующие подсемейства семейства независимых множеств $\mathcal{F}_A = \mathcal{F}(\mathcal{C}_A(K_i))$. Без ограничения общности можно считать, что пустое множество не принадлежит $\mathcal{F}_A$.

5.1. Пусть

$$\mathcal{F}_1 = \{N \in \mathcal{F}_A : NAA^{-1}A \neq NA\}.$$

Пользуясь теоремой 11, получаем неравенство $|NA| \geq |N| + |A|/2$. Из (26) следует, что $NA \cap N = \emptyset$. Поскольку NA и N являются подмножествами K_i , справедливо неравенство $|N| \leq m/2$. Ясно, что

$$\begin{aligned} |\partial(N)| &= |N(A \cup A^{-1})| \geq |NA| \geq |N| + \frac{1}{2}|A| \\ &> |N| + \frac{1-\beta}{8}m \geq |N| \left(1 + \frac{1-\beta}{4}\right) \geq |N| / \left(1 - \frac{1-\beta}{5-\beta}\right). \end{aligned}$$

Таким образом, для всех множеств $N \in \mathcal{F}_1$ выполняется неравенство

$$|N| \leq \left(1 - \frac{1-\beta}{5-\beta}\right) |\partial(N)|. \quad (27)$$

Из следствия 1, примененного к множествам $N \subset K'$ и $A \subset K$, следует, что существует подгруппа M группы G такая, что верно неравенство

$$|NA| \geq |N| + |A| - |M| \quad (28)$$

и NA содержит по крайней мере один левый смежный класс по подгруппе M . Из включения $NA \subset K_i$ следует, что $M \leq K$, а поскольку $N \neq \emptyset$, то $M \neq K$. Итак, $M < K$. Отсюда $|M| \leq m/2$.

5.2. Пусть $\mathcal{F}_2$ — семейство множеств $N \in \mathcal{F}_A$, удовлетворяющих неравенствам (28) и $|M| \leq m/5$. Пользуясь неравенством (28), получаем, что

$$\begin{aligned} |\partial(N)| &\geq |N| + |A| - |M| \geq |N| + \frac{1-\beta}{4}m - \frac{m}{5} \\ &\geq |N| \left(1 + \frac{1-5\beta}{20} \frac{m}{|N|}\right) \geq |N| \left(1 + \frac{1-5\beta}{10}\right) = |N| / \left(1 - \frac{1-5\beta}{11-5\beta}\right). \end{aligned}$$

Таким образом, для всех $N \in \mathcal{F}_2$ выполняется неравенство

$$|N| \leq \left(1 - \frac{1-5\beta}{11-5\beta}\right) |\partial(N)|. \quad (29)$$

Теперь рассмотрим те множества N , для которых подгруппа M удовлетворяет неравенствам $m/4 \leq |M| \leq m/2$.

5.3. Обозначим через $\mathcal{F}_3$ семейство множеств $N \in \mathcal{F}_A$, для которых $|M| \geq m/4$ и $M \cap A \neq \emptyset$.

Пусть $a \in M \cap A$. По условию NA содержит некоторый левый смежный класс по M . Обозначим его через L . Ясно, что $N \cap L = \emptyset$. Отсюда следует, что

$$Na \cap La = Na \cap L = \emptyset.$$

Используя неравенства $|N|/2 \leq m/4 \leq |M|$, получаем, что

$$|\partial(N)| \geq |NA| \geq |N| + |M| \geq 3|N|/2.$$

Отсюда следует, что для всех $N \in \mathcal{F}_3$

$$|N| \leq \left(1 - \frac{1}{3}\right) |\partial(N)|. \quad (30)$$

5.4. Пусть

$$\mathcal{F}_4 = \{N \in (\mathcal{F}_A \setminus \mathcal{F}_1) : |M| \geq m/4, M \cap A = \emptyset\}.$$

Заметим, что для любого $N \in \mathcal{F}_4$ выполняется равенство

$$NAA^{-1}A = NA. \quad (31)$$

5.4.1. Обозначим $\mathcal{F}_4^1$ семейство множеств $N \in \mathcal{F}_4$, для которых $|M| = m/2$. Из определения семейства $\mathcal{P}_5$ вытекает, что $A \cap M \neq \emptyset$. Следовательно, $\mathcal{F}_4^1 = \emptyset$.

5.4.2. Обозначим $\mathcal{F}_4^2$ подсемейство множеств $N \in \mathcal{F}_4$, для которых $|M| = m/3$.

Множество A не содержится ни в одном из левых смежных классов по подгруппе M , поэтому $\hat{A} = (A^{-1}A) \setminus M \neq \emptyset$. По условию множество NA содержит хотя бы один левый смежный класс по подгруппе M . Обозначим его через L . Из (31) следует, что $L\hat{A} \subset NA$. Так как $|L\hat{A}| \geq m/3$ и $L\hat{A} \cap L = \emptyset$, справедливо неравенство

$$|NA| \geq |L| + |L\hat{A}| \geq 2m/3.$$

Отсюда $|NA| \geq 2|N|$. Таким образом, для всех множеств $N \in \mathcal{F}_4^2$ выполняется неравенство

$$|N| \leq \left(1 - \frac{1}{2}\right) |\partial(N)|. \quad (32)$$

5.4.3. Пусть $\mathcal{F}_4^3$ — семейство множеств $N \in \mathcal{F}_4$ таких, что $|M| = m/4$ и хотя бы два правых смежных класса по M имеют непустое пересечение с $\hat{A}$.

Обозначим левые смежные классы (не равные M) группы G по подгруппе M , $|M| = m/4$, содержащиеся в K , через L_i , $i = 1, 2, 3$, и содержащиеся в K_i , через L_i , $i = 4, 5, 6, 7$. Без ограничения общности можно считать, что $NA \supseteq L_7$. Введем обозначения $R_i = (L_i)^{-1}$, $i = 1, 2, 3$. Пусть R_k и R_l , $k, l \in \{1, 2, 3\}$, являются различными правыми смежными классами группы K по подгруппе M , с которыми $\hat{A}$ имеет непустое пересечение. Множества L_7R_k , L_7R_l и L_7 попарно не пересекаются, потому что они являются правыми смежными классами группы G по подгруппе $L_7L_7^{-1}$. Из (31) и включения $L_7 \subseteq NA$ следует, что L_7R_k и L_7R_l содержатся в NA . Отсюда получаем, что

$$|\partial(N)| \geq |NA| \geq \frac{3m}{4} \geq 3|N|.$$

Таким образом, для всех множеств $N \in \mathcal{F}_4^3$

$$|N| \leq (1 - 2/3)|\partial(N)|. \quad (33)$$

Заметим, что $\hat{A}$ не пусто. Действительно, из определения семейства $\mathcal{P}_5(G)$ следует, что множество A не содержится ни в каком левом смежном классе по подгруппе M . Далее будем считать, что $\hat{A}$ содержится в некотором правом смежном классе по M (случай, когда $\hat{A}$ имеет непустое пересечение хотя бы с двумя правыми смежными классами по M , уже рассмотрен в п. 4.3). Без ограничения общности можно считать, что

$$\hat{A} \subset R_1. \quad (34)$$

Условимся обозначать подгруппу $L_i L_i^{-1}$ через M_i , $i = 1, 2, 3$.

Допустим, что существует элемент $a \in (A \cap R_1)$. Тогда, очевидно, что $a^{-1}A \subset \hat{A}$ имеет непустое пересечение с одним из правых смежных классов R_2 и R_3 , а это противоречит условию (34). Следовательно, $A \cap R_1 = \emptyset$. Так как

$$\hat{A} = (\hat{A})^{-1}, \quad (35)$$

аналогичным образом доказывается, что и $A \cap L_1 = \emptyset$. Итак,

$$A \cap (L_1 \cup R_1) = \emptyset.$$

5.4.4. Обозначим через $\mathcal{F}_4^4$ семейство множеств $N \in \mathcal{F}_4$ таких, что $|M| = m/4$, $\hat{A} \neq \emptyset$, $\hat{A} \subset R_1$, $A \cap (L_1 \cup R_1) = \emptyset$ и $M_1 \neq M$.

Из условий следует, что ровно два левых смежных класса по M имеют непустое пересечение с множеством A . Отсюда, пользуясь неравенством $|A| > (1 - \beta)m/4$, получаем, что

$$|R_1 \cap L_1| \geq |\hat{A}| \geq (1 - \beta)m/8. \quad (36)$$

Из (35) следует, что $\hat{A} \subset (R_1 \cap L_1)$. Из леммы 2 и условия $M_1 \neq M$ следует, что $|M_1 \cap M| = m/4k$, где $k = 2, 3, 4$. Отсюда при помощи леммы 4 и (36) получаем, что

$$|M_1 \cap M| = |M_1 \cap L_1| = m/8.$$

Также из леммы 4 следует, что R_1 имеет непустое пересечение ровно с двумя левыми смежными классами группы K по подгруппе M . Поэтому множество $R_1 \setminus L_1$ содержится либо в L_2 , либо в L_3 . Без ограничения общности можно считать, что $R_1 \setminus L_1$ содержится в L_2 . По условию $A \subset K \setminus (R_1 \cup L_1 \cup M)$. Покажем, что $K \setminus (R_1 \cup L_1 \cup M)$ является объединением трех правых смежных классов по подгруппе $\hat{M} = M_1 \cap M$. Действительно, из леммы 3 следует, что $L_1 \cap R_1$ и $L_2 \cap R_1$ являются левыми смежными классами по подгруппе $\hat{M}$. Отсюда следует, что $L_1 \setminus R_1$ и $L_2 \setminus R_1$ также являются левыми смежными классами по $\hat{M}$. Ясно, что L_3 — объединение двух левых смежных классов по $\hat{M}$.

Таким образом, A содержится в объединении трех левых смежных классов по подгруппе порядка $m/8$. Но это исключено, поскольку $D \in \mathcal{P}_5$.

Итак, доказано, что $\mathcal{F}_4^4 = \emptyset$.

5.4.5. Обозначим через $\mathcal{F}_4^5$ подсемейство множеств $N \in \mathcal{F}_4$ таких, что

$$|M| = m/4, \quad \hat{A} \neq \emptyset, \quad \hat{A} \subset R_1, \quad A \cap (L_1 \cup R_1) = \emptyset, \quad M_1 = M.$$

Из условия следует, что $R_1 = L_1$ и $A \cap (M \cup L_1) = \emptyset$. Легко видеть, что $M \cup L_1$ является подгруппой. По условию п. 5 множество A имеет непустое пересечение с любой подгруппой индекса 2 группы K , поэтому $\mathcal{P}_4^5 = \emptyset$.

Из (27), (32) и (33) следует, что если в качестве δ взять $(1 - 5\beta)/(11 - 5\beta)$, то для всех множеств $A = D \cap K$, $D \in \mathcal{P}_5(G)$, граф $\mathcal{C}_A(K_i)$ является δ -расширителем. Оценим мощность семейства $\mathcal{P}_5(G)$.

Выберем подмножество $S \subset K$ так, что $|S| = \lfloor \alpha m \rfloor$. Затем выберем $A \subset K$, независимое в графе $\mathcal{C}_S(K)$. При фиксированном множестве A множества D_i выберем независимыми в графах $\mathcal{C}_A(K_i)$, $i = 1, \dots, p-1$. Применяя теорему 7 к графу $\mathcal{C}_S(K)$ и теорему 9 к графам $\mathcal{C}_A(K_i)$, $i = 1, \dots, p-1$, получаем, что

$$\begin{aligned} |\mathcal{P}_5(G)| &\leq \binom{m}{\lfloor \alpha m \rfloor} 2^{(m/2)(1+o(1))} 2^{(m/2)(p-1-(p-1)(1-5\beta)/(7(11-5\beta))+o(1))} \\ &\leq 2^{(m/2)(p+2\alpha \log(e/\alpha)-(p-1)(1-5\beta)/(7(11-5\beta))+o(1))} < 2^{(n/2)(1-(0,006-0,009/p)+o(1))}. \end{aligned}$$

Таким образом,

$$|\mathcal{P}_5(G)| \leq 2^{(n/2)(1-0,003)}. \quad (37)$$

Положим $\alpha = 0,0001$, $\beta = 0,1$. Тогда из неравенств (13), (14), (23), (24) и (37) следует верхняя оценка в (3).

Автор благодарен своему научному руководителю А. А. Сапоженко за постановку задачи и внимание к работе.

Список литературы

1. Петросян Т. Г., О числе множеств, свободных от произведений, в группах четного порядка. *Дискретная математика* (2005) **17**, №1, 89–91.
2. Сапоженко А. А., О числе множеств, свободных от сумм, в абелевых группах. *Вестник Московского университета, сер. I* (2002) №4, 14–17.
3. Сапоженко А. А., О числе независимых множеств в расширителях. *Дискретная математика* (2001) **13**, №1, 56–62.
4. Сапоженко А. А., *Проблема Дедекинда и метод граничных функционалов*. Изд-во ф-та ВМиК МГУ, Москва, 2005.
5. Alon N., Independent sets in regular graphs and sum-free subsets of finite groups. *Israel J. Math.* (1991) **73**, №2, 247–256.
6. Davenport H., On the addition of residue classes. *J. London Math. Soc.* (1935) **10**, 30–32.
7. Lev V., Luczak T., Schoen T., Sum-free sets in abelian groups. *Israel J. Math.* (2001) **125**, 347–367.
8. Mann H. B., *Addition theorems*. Interscience, New York, 1965.
9. Olson J. E., On the sum of two sets in a group. *J. Number Theory* (1984) **18**, 110–120.

Статья поступила 15.06.2006.