Math-Net.Ru

Общероссийский математический портал

Т. Г. Петросян, О числе множеств, свободных от произведений, в группах четного порядка, *Дискрет. матем.*, 2005, том 17, выпуск 1, 89–101

DOI: <https://doi.org/10.4213/dm90>

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: 34.229.45.116

26 апреля 2023 г., 07:34:39

УДК 519.1

О числе множеств, свободных от произведений, в группах четного порядка

© 2005 г. Т. Г. Петросян

Получена асимптотика числа множеств, свободных от произведений, в конечных группах четного порядка.

Работа выполнена при поддержке Российского фонда фундаментальных исследований, проект 04-01-00359.

1. Введение и основные понятия

Множество A элементов группы G называется свободным от произведений, если 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 [1] показал, что верна оценка

$$\log_2 P(n) \leq n(1/2 + \varepsilon(n)),$$

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

В. Ф. Лев, Т. Лучак и Т. Шон в [2] и независимо А. А. Сапоженко в [3] получили асимптотику числа множеств свободных от произведений в абелевых группах четного порядка. Более точно, ими было установлено, что 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, $\varepsilon(n) \rightarrow 0$ при $n \rightarrow \infty$ и второе неравенство справедливо, начиная с некоторого n .

В данной работе неравенства (1) обобщаются на случай произвольных конечных групп четного порядка, имеющих хотя бы одну подгруппу индекса 2.

Теорема 1. Для любой группы G четного 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 .

Доказательство верхней оценки в (2) сводится к оценке числа независимых множеств в так называемых графах Кэли подобно тому, как это делалось в работах [1] и [3].

Пусть G — группа, $A \subset G$, $e \notin A$, $A^{-1} = \{a^{-1} : a \in A\}$. Графом Кэли $\mathcal{C}_A(G)$ на множестве G относительно множества A будем называть граф с множеством вершин G , в котором ребрами являются пары $\{u, v\}$ такие, что $u^{-1}v \in (A \cup A^{-1})$. Из этого 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 $\mathcal{F}(\Gamma)$. 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 $A \subseteq B$.

Если $\Gamma = (V, E)$ и $A \subset V$, то 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 $A \subset V$. Введем обозначение $AB = \{ab : a \in A, b \in B\}$.

Везде в дальнейшем предполагается, что n достаточно велико.

2. Вспомогательные утверждения

В работе используются следующие результаты, полученные в [4].

Теорема 2. Пусть Γ — n -вершинный регулярный граф степени k . Тогда

$$|\mathcal{F}(\Gamma)| \leq 2^{(n/2)(1+O(\sqrt{(\log k)/k}))}. \quad (3)$$

Здесь и далее $\log n$ означает $\log_2 n$.

Теорема 3. Для любого n -вершинного регулярного графа Γ степени k и любого 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

$$I_\beta(\Gamma) \leq 2^{(n/2)(1-\beta^2/(2\ln 2)+O(\sqrt{(\log k)/k}))}. \quad (4)$$

Теорема 4. Пусть $\Gamma = (V, E)$ — n -вершинный регулярный граф степени k , являющийся δ -расширителем для некоторого δ , $0 \leq \delta < 1$. Тогда

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

Мы также используем следующие две теоремы Олсона [5].

Теорема 5. Пусть A и B являются конечными подмножествами группы G , тогда существует подмножество S множества AB и подгруппа H группы G такие, что $|AB| \geq |A| + |B| - |H|$ и либо $SH = S$, либо $HS = S$.

Теорема 6. Пусть A и B являются конечными подмножествами группы G , тогда либо $ABV^{-1}B = AB$, либо $|AB| \geq |A| + |B|/2$.

Лемма 1. Пусть H — некоторая собственная подгруппа порядка $m > 1$ группы G , $v \in H \setminus \{e\}$, H' — смежный класс группы G по подгруппе H . Тогда число $\mu(H', v)$ множеств $B \subseteq H'$ таких, что $B \cup \{v\} \in \mathcal{P}(G)$, удовлетворяет неравенству

$$\mu(H', v) \leq 3^{m/2}. \quad (5)$$

Доказательство аналогично доказательству леммы 6 в [3].

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 K является подгруппой группы G . Подгруппа K' называется сопряженной к K , если существует такой элемент x группы G , что $xKx^{-1} = K'$.

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

Доказательство. Пусть T является левым смежным классом по H . Легко видеть, что для любых $x, y \in (L \cap T)$ справедливы включения $x^{-1}y \in (L \cap H)$ и $x(L \cap H) \subset (L \cap T)$. Следовательно, множество $L \cap T$ является левым смежным классом группы G по подгруппе $L \cap H$. В случае, когда T является правым смежным классом доказательство проводится аналогично.

Следствие 1. Пусть v — тип подгруппы L относительно подгруппы H . Тогда

$$|T \cap L| = |L|/v,$$

где T — произвольный (левый или правый) смежный класс по подгруппе H , имеющий непустое пересечение с подгруппой L .

Пусть T и R — левый и правый, соответственно, смежные классы группы G по подгруппе H . Введем

$$TT^{-1} = H_T, \quad R^{-1}R = H_R.$$

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 $H_T \cap H$.

Доказательство. Пусть $x \in (T \cap R)$. Тогда из того, что $H_R = (Hx)^{-1}R$ следует равенство

$$x^{-1}R \cap H = H_R \cap H,$$

откуда следует, что

$$R \cap xH = x(H_R \cap H).$$

Последнее равенство эквивалентно равенству

$$R \cap T = R \cap xH = x(H_R \cap H).$$

Аналогично доказывается, что $R \cap T$ — правый смежный класс по подгруппе H_T .

Лемма 4. Пусть H является подгруппой группы G . Тогда произвольный левый (правый) смежный класс T группы G по H имеет непустое пересечение ровно с ν правыми (левыми) смежными классами группы G по H , где ν 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 $|H|/\nu$.

Доказательство. Рассмотрим случай, когда T — левый смежный класс по H . Из леммы 3 следует, что пересечение T с любым правым смежным классом по H , имеющим непустое пересечение с T , является правым смежным классом по подгруппе $H_T \cap H$. Отсюда согласно следствию 1 вытекает, что T имеет непустое пересечение ровно с ν правыми смежными классами группы G по H , где ν является типом подгруппы H_T относительно H . Ясно, что мощности пересечения $T \cap R$, где R — произвольный правый смежный класс по H такой, что $T \cap R \neq \emptyset$, равны $|H|/\nu$. Случай, когда T — правый смежный класс, рассматривается аналогично.

Условимся через $t_k(G)$ обозначать число подгрупп индекса k группы G . Определим функцию $t_k(x)$, полагая

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

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

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

Доказательство. Пусть H — подгруппа группы G индекса k . Семейство всех подгрупп индекса k группы G разобьем на k непересекающихся подсемейств $\mathcal{T}_1, \dots, \mathcal{T}_k$, где $\mathcal{T}_l$ — подсемейство всех подгрупп группы G индекса k и типа l относительно H . Оценим мощность класса $\mathcal{T}_l$. Из следствия 1 вытекает, что пересечение любой группы из $\mathcal{T}_l$ с группой H является подгруппой индекса l группы H . Число подгрупп индекса l группы H не превосходит $t_l(n/k)$. Зафиксируем некоторую подгруппу N индекса l группы H . Покажем, что число подгрупп из подсемейства $\mathcal{T}_l$, пересечение которых с группой H есть N , не превосходит $\binom{k-1}{l-1} l^{l-1}$. Действительно, каждая такая подгруппа пересекает ровно $l-1$ левых смежных классов группы G по H помимо самой H . Из леммы 2 следует, что пересечение подгруппы из подсемейства $\mathcal{T}_l$, пересечение которой с H равно N , с любым левым смежным классом по H есть левый смежный класс по подгруппе N . Ясно, что левых смежных классов по подгруппе N ровно l в каждом левом смежном классе по H .

Следствие 2. Существуют положительные постоянные c_1 и c_2 такие, что $t_2(n) \leq n-1$, $t_3(n) \leq c_1 n^2$, $t_4(n) \leq c_2 n^5$.

Пусть G — группа порядка n . Обозначим через $\mathcal{T}(G)$ семейство подмножеств $C \in \mathcal{P}(G)$ таких, что выполняются следующие условия:

- (1) существуют подгруппа K индекса 2 группы G , подгруппа H индекса 2 подгруппы K и два левых смежных класса L_1 и L_2 группы G по подгруппе H , удовлетворяющих условиям

$$L_1 \subset K, \quad L_1 \neq H, \quad L_2 \subset (G \setminus K), \quad C \subseteq (L_1 \cup L_2), \quad (7)$$

- (2) если H является нормальной подгруппой группы G , то факторгруппа G/H изоморфна $\mathbb{Z}_4$.

Лемма 6. Пусть порядок группы G равен n . Тогда

$$|T(G)| \leq 2^{0,45n}. \quad (8)$$

Доказательство. Рассмотрим два случая.

1. Пусть $T_1(G)$ — подсемейство семейства $T(G)$, состоящее из тех и только тех множеств $C \in T(G)$, для которых H является нормальной подгруппой G . Тогда по условию факторгруппа G/H изоморфна $\mathbb{Z}_4$. Из следствия 2 вытекает, что число подгрупп индекса 4 группы порядка n не превосходит cn^5 , где c — некоторая положительная постоянная. Пусть $A = C \cap L_1$, $B = C \cap L_2$. Выберем некоторое множество B мощности k . Это можно сделать не более чем $\binom{n/4}{k}$ способами. Поскольку $L_2 L_2 = L_1$ и $B B \cap A = \emptyset$, множество A можно выбрать не более чем $2^{n/4-k}$ способами, где $k = |B|$. Таким образом,

$$|T_1(G)| \leq cn^5 \sum_{0 \leq k \leq n/4} 2^{n/4-k} \leq cn^5 3^{n/4} \leq 2^{(n \log 3)/4(1+o(1))}. \quad (9)$$

2. Пусть $T_2(G)$ — подсемейство семейства $T(G)$, состоящее из тех и только тех множеств $C \in T(G)$, для которых H не является нормальной подгруппой G . Пусть L_1, L_2 и L_3 — левые смежные классы, не равные H , группы G по подгруппе H , причем $L_1 \subset K$. Ясно, что подгруппа $L_2 H L_2^{-1}$ имеет тип 2 относительно H . Пусть $R_2 = L_2^{-1}$ и $R_3 = L_3^{-1}$. Из леммы 4 следует, что $|R_i \cap L_j| = n/8$ для всех $i, j \in \{2, 3\}$. Пусть $A = C \cap L_1$ и $B' = C \cap L_2 \cap R_3$.

Легко видеть, что число множеств $C \in T_2(G)$ таких, что $C \cap (R_2 \cap L_2) = \emptyset$, не превосходит

$$cn^5 2^{n/4} 2^{n/8} \leq 2^{3n/8(1+o(1))}. \quad (10)$$

Пусть существует $x \in (C \cap (R_2 \cap L_2))$. Выберем некоторое множество B' мощности k . Заметим, что $(R_3 \cap L_2)x^{-1} \subset L_1$. Из того, что $B'x^{-1} \cap A = \emptyset$, следует, что число способов выбора множества A не превышает $2^{n/4-k}$. Существуют две пары смежных классов, удовлетворяющих условиям (7). Учитывая (10), получаем, что

$$|T_2(G)| \leq 2cn^5 2^{n/8} \sum_{0 \leq k \leq n/8} \binom{n/8}{k} 2^{n/4-k} \leq 2^{1+n/4+(n \log 3)/8+o(n)} \leq 2^{0,45n}. \quad (11)$$

Из оценок (9) и (11) следует (8).

3. Доказательство теоремы 1

Пусть G — группа порядка $n = 2m$. Назовем множество $C \in \mathcal{P}(G)$ правильным, если существует подгруппа L индекса 2 группы G такая, что $C \cap L = \emptyset$, и неправильным в противном случае.

1. Пусть $\mathcal{P}_1(G)$ — подсемейство правильных множеств в $\mathcal{P}(G)$, а t — число подгрупп индекса 2 группы G . Тогда

$$t 2^{n/2} - t^2 2^{n/4} \leq |\mathcal{P}_1(G)| \leq t 2^{n/2}. \quad (12)$$

Верхняя оценка следует из того, что всякое подмножество смежного класса по фиксированной подгруппе индекса 2, отличного от группы, является свободным от произведений. Нижняя оценка вытекает из того, что мощность пересечения смежных классов двух разных подгрупп индекса 2 равна $n/4$, и из формулы включения–исключения. Из следствия 2 вытекает, что $\log t \leq \log n = o(n)$. Таким образом, нижняя оценка в (2) доказана.

Теперь оценим сверху число неправильных множеств. Пусть K — произвольная подгруппа индекса 2 группы G и $K' = G \setminus K$. Если $C \in \mathcal{P}(G)$, то везде далее $A = C \cap K$, $B = C \cap K'$. Семейство неправильных множеств обозначим через $\tilde{\mathcal{P}}(G)$.

2. Пусть $0 < \gamma < 1$ и $0 < \Delta_1 < 1$ таковы, что

$$\gamma \log(e/\gamma) + (1/2) \log 3 \leq 1 - \Delta_1.$$

Положим

$$\mathcal{P}_2(G) = \{C \in \tilde{\mathcal{P}}(G) : |A| \leq \gamma m\}.$$

При заданном A для любого $v \in A$ число способов выбора $B \subset K'$ не больше $\mu(K', v)$. Используя лемму 1, получаем, что

$$|\mathcal{P}_2(G)| \leq \sum_{i \leq \gamma m} \binom{m}{i} 3^{m/2} \leq 2^{m(\gamma \log(e/\gamma) + (\log 3)/2)} \leq 2^{m(1-\Delta_1)}. \quad (13)$$

Здесь и далее используется оценка

$$\sum_{i \leq \lambda n} \binom{n}{i} \leq 2^{n\lambda \log(e/\lambda)}$$

(см., например, задачу 5.8 на с. 280 в [6]).

3. Положим

$$\mathcal{P}_3(G) = \{C \in \tilde{\mathcal{P}}(G) : \gamma m \leq |A| \leq m(1 - \beta)/4\}.$$

Пусть $0 < \beta < 1$, $0 < \alpha < 1$ и $0 < \Delta_2 < 1$ таковы, что

$$\frac{\beta^2}{4 \ln 2} - \alpha \log \frac{e}{\alpha} > \Delta_2.$$

Множества C из $\mathcal{P}_3(G)$ будем строить следующим образом. Зафиксируем достаточно малое $0 < \alpha \leq \gamma$ и выберем подмножество $D \subset K$ такое, что $|D| = \lfloor \alpha m \rfloor$. Затем выберем $A \subset K$, независимое в графе $\mathcal{C}_D(K)$. Наконец, выберем множество $B \subset K'$, независимое в графе $\mathcal{C}_A(K')$. С использованием (3) и (4) получаем, что

$$\begin{aligned} |\mathcal{P}_3(G)| &\leq \binom{m}{\lfloor \alpha m \rfloor} 2^{(m/2)(2-\beta^2/(2 \ln 2) + O(\sqrt{(\log m)/m}))} \\ &\leq 2^{m(1-\beta^2/(4 \ln 2) + \alpha \log(e/\alpha) + O(\sqrt{(\log n)/n}))}. \end{aligned}$$

Таким образом,

$$|\mathcal{P}_3(G)| \leq 2^{m(1-\Delta_2)}. \quad (14)$$

4. Пусть $\mathcal{P}_4(G)$ — семейство множеств $C \in \tilde{\mathcal{P}}(G)$ таких, что $|A| > m(1 - \beta)/4$ и существует подгруппа H индекса 2 группы K такая, что $A \cap H = \emptyset$. Пусть H_1, H_2 и H_3 являются различными левыми смежными классами группы G по H , причем $H_1 \subset K$. Возможны три случая.

4.1. Обозначим через $\mathcal{P}_4^1(G)$ семейство множеств $C \in \mathcal{P}_4(G)$, удовлетворяющих условию: пересечение множества B с каким-то из смежных классов H_2 и H_3 пусто. Заметим, что если H является нормальной подгруппой G , то факторгруппа G/H изоморфна $\mathbb{Z}_4$, поскольку в противном случае (то есть, когда $G/H \simeq \mathbb{Z}_2^2$) $A \cup B$ было бы правильным множеством. Воспользовавшись леммой 6, получаем оценку

$$|\mathcal{P}_4^1(G)| \leq 2^{0,45n} \leq 2^{m(1-0,1)}. \quad (15)$$

Пусть $B_2 = B \cap H_2$ и $B_3 = B \cap H_3$.

4.2. Обозначим через $\mathcal{P}_4^2(G)$ семейство множеств $C \in \mathcal{P}_4(G)$ таких, что множества B_2 и B_3 не пусты и одно из них по мощности не превосходит γm , где γ — некоторая положительная постоянная. Без ограничения общности можно считать, что $|B_2| \leq \gamma m$. Пусть $0 < \gamma < 1$ таково, что

$$\gamma \log(e/(2\gamma)) + (1/2) \log 3 \leq 0,9.$$

Построим граф Γ_b на множестве $H_1 \cup H_3$ такой, что пара $\{u, v\}$ является ребром, тогда и только тогда, когда один из элементов u и v , скажем u , лежит в H_3 и верно равенство $uv = b$. Ясно, что граф Γ_b является парасочетанием. Легко видеть, что

$$|\mathcal{F}(\Gamma_b)| = 3^{m/2}.$$

Выберем множество B_2 в смежном классе H_2 . Это можно сделать $\sum_{1 \leq i \leq \gamma m} \binom{m/2}{i}$ способами. Пусть $b \in B_2$. Выберем множество $F \subset H_1 \cup H_3$, независимое в графе Γ_b . Таким образом,

$$|\mathcal{P}_4^2(G)| \leq \sum_{1 \leq i \leq \gamma m} \binom{m/2}{i} 3^{m/2} \leq 2^{m(\gamma \log(e/(2\gamma)) + (\log 3)/2)} \leq 2^{m(1-0,1)}. \quad (16)$$

4.3. Оценим мощность

$$\mathcal{P}_4^3(G) = \{C \in \mathcal{P}_4(G) : |B_2| > \gamma m, |B_3| > \gamma m\}.$$

Пусть

$$F_i \subset H_i, \quad |F_i| = \lfloor \alpha m \rfloor, \quad i = 1, 2, 3, \quad \tilde{F} = (F_1, F_2, F_3).$$

Пусть $0 < \alpha < 1$ таково, что

$$\alpha \leq \gamma, \quad 3/4 + 3\alpha \log(e/(2\alpha)) < 0,8.$$

Рассмотрим граф $\mathcal{L}_{\tilde{F}}(G \setminus H)$ на множестве $G \setminus H$ такой, что пара $\{u, v\}$ является ребром в том и только том случае, когда

$$\begin{aligned} u \in H_1, \quad v \in H_2, \quad vu \in F_3, \\ u \in H_1, \quad v \in H_3, \quad vu \in F_2, \\ u \in H_2, \quad v \in H_3, \quad u^{-1}v \in F_1. \end{aligned}$$

Нетрудно проверить, что граф $\mathcal{L}_F(G \setminus H)$ является $2[\alpha m]$ -регулярным.

Воспользовавшись теоремой 2, получим оценку

$$|\mathcal{F}(\mathcal{L}_F(G \setminus H))| \leq 2^{(3/4)m(1+o(1))}.$$

Множества $C \in \mathcal{P}_4^3(G)$ будем покрывать следующим образом: сначала выберем тройку $\tilde{F}$, затем множества, независимые в графе $\mathcal{L}_{\tilde{F}}(G \setminus H)$. Таким образом, получаем оценку

$$|\mathcal{P}_4^3(G)| \leq \left(\frac{m/2}{[\alpha m]}\right)^3 2^{(3/4)m(1+o(1))} \leq 2^{m(3/4+3\alpha \log(e/(2\alpha))+o(1))} \leq 2^{m(1-0.2)}. \quad (17)$$

Из неравенств (15)–(17) следует, что

$$|\mathcal{P}_4(G)| \leq 2^{m(1-0.1)}. \quad (18)$$

5. Пусть $\mathcal{P}_5^1(G)$ — семейство множеств $C \in \tilde{\mathcal{P}}(G) \setminus \mathcal{P}_2(G)$ таких, что множество A содержится в смежном классе по некоторой подгруппе индекса 4 группы K ; $\mathcal{P}_5^2(G)$ — семейство множеств $C \in \tilde{\mathcal{P}}(G) \setminus \mathcal{P}_2(G)$ таких, что A содержится в смежном классе по некоторой подгруппе индекса 3 группы K ; $\mathcal{P}_5^3(G)$ — семейство множеств $C \in \tilde{\mathcal{P}}(G) \setminus \mathcal{P}_2(G)$ таких, что множество A содержится в объединении трех смежных классов по некоторой подгруппе порядка $m/8$, содержащейся в подгруппе порядка $m/4$ группы K , и

$$\mathcal{P}_5(G) = \mathcal{P}_5^1(G) \cup \mathcal{P}_5^2(G) \cup \mathcal{P}_5^3(G).$$

Оценим мощность семейства $\mathcal{P}_5^3(G)$. Из следствия 2 вытекает, что число подгрупп порядка $m/8$, содержащихся в некоторой подгруппе порядка $m/4$, не больше чем cm^6 , где c — некоторая положительная постоянная. Выбрать множество A можно не более чем $2^{3m/8}$ способами. Множество B выберем независимым в графе $\mathcal{C}_A(K')$. Применив теорему 2 к графу $\mathcal{C}_A(K')$, получаем, что

$$|\mathcal{P}_5^3(G)| \leq cm^6 \binom{8}{3} 2^{3m/8(m/2)(1+o(1))} \leq 2^{(7m/8)(1+o(1))}.$$

Нетрудно проверить, что

$$|\mathcal{P}_5^1(G)| = o(2^{7m/8}), \quad |\mathcal{P}_5^2(G)| = o(2^{7m/8}).$$

Таким образом,

$$|\mathcal{P}_5(G)| \leq 2^{(7m/8)(1+o(1))}. \quad (19)$$

6. Положим

$$\mathcal{P}_6(G) = \{C \in \tilde{\mathcal{P}}(G) \setminus (\mathcal{P}_4(G) \cup \mathcal{P}_5(G)) : |A| > (1 - \beta)m/4\}.$$

Далее будет показано, что для множеств $C \in \mathcal{P}_6(G)$ граф $\mathcal{C}_A(K')$ является δ -расширителем при

$$\delta = \frac{1 - 5\beta}{11 - 5\beta}.$$

Заметим, что в графе $\mathcal{C}_A(K')$ граница $\partial(N)$ множества $N \subset K'$ равна $N(A \cup A^{-1})$.
Рассмотрим подсемейства семейства независимых множеств $\mathcal{F}_A = \mathcal{F}(\mathcal{C}_A(K'))$.

6.1. Пусть

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

Пользуясь теоремой 6, получаем неравенство

$$|NA| \geq |N| + (1/2)|A|.$$

Из независимости N следует, что $NA \cap N = \emptyset$. Отсюда, $|N| \leq m/2$. Справедливы оценки

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

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

$$|N| \leq \left(1 - \frac{1 - \beta}{5 - \beta}\right) |\partial(N)|. \quad (20)$$

Из теоремы 5, примененной к множествам $N \subset K'$ и $A \subset K$, следует, что существуют подгруппа H и подмножество S множества NA такие, что верно неравенство

$$|NA| \geq |N| + |A| - |H| \quad (21)$$

и либо $SH = S$, либо $HS = S$. Так как $NA \subset K'$, то $H \subset K$. Легко видеть, что $|H| \leq m/2$.

6.2. Пусть $\mathcal{F}_2$ — подсемейство множеств $N \in \mathcal{F}_A$, удовлетворяющих неравенствам (21), и $|H| < m/4$. Из последнего неравенства следует, что $|H| \leq m/5$. Пользуясь неравенством (21), получаем, что

$$\begin{aligned} |\partial(N)| &\geq |NA| \geq |N| + |A| - |H| \geq |N| + \frac{1 - \beta}{8}n - \frac{n}{10} \\ &\geq |N| \left(1 + \frac{1 - 5\beta}{40} \frac{n}{|N|}\right) \geq |N| \left(1 + \frac{1 - 5\beta}{10}\right) \geq |N| \left(1 - \frac{1 - 5\beta}{11 - 5\beta}\right). \end{aligned}$$

Таким образом, для всех $C \in \mathcal{P}_6^2(G)$ выполняется неравенство

$$|N| \leq \left(1 - \frac{1 - 5\beta}{11 - 5\beta}\right) |\partial(N)|. \quad (22)$$

Теперь рассмотрим те множества N , для которых существуют подгруппа H , порядка, не меньшего $n/8$, и подмножество S множества NA такие, что выполняется неравенство (21) и условие $SH = S$ (откуда следует, что в NA содержится по крайней мере один левый смежный класс по подгруппе H). Случай $HS = S$ легко сводится к случаю, когда S содержит некоторый левый смежный класс. Действительно, пусть S содержит некоторый правый смежный класс R по подгруппе H . Тогда вместо H рассмотрим сопряженную к ней подгруппу $R^{-1}HR$. Множество R является левым смежным классом по подгруппе $R^{-1}HR$.

6.3. Обозначим через $\mathcal{F}_3$ подсемейство множеств $N \in \mathcal{F}_A$, для которых $|H| \geq n/8$ и $H \cap A \neq \emptyset$.

Пусть $a \in A \cap H$. По условию NA содержит некоторый левый смежный класс по H . Обозначим его через T . Ясно, что $N \cap T = \emptyset$. Отсюда следует, что $Na \cap Ta = Na \cap T = \emptyset$. Используя неравенства $|N|/2 \leq m/4 \leq |H|$, получаем, что

$$|\partial(N)| \geq |NA| \geq |N| + |H| \geq 3|N|/2,$$

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

$$|N| \leq (1 - 1/3)|\partial(N)|. \quad (23)$$

6.4. Пусть

$$\mathcal{F}_4 = \{N \in (\mathcal{F}_A \setminus \mathcal{F}_1) : |H| \geq n/8, H \cap A = \emptyset\}.$$

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

$$NAA^{-1}A = NA. \quad (24)$$

6.4.1. Обозначим через $\mathcal{F}_4^1$ семейство множеств $N \in \mathcal{F}_4$, для которых $|H| = n/4$.

Для всех $C \in \mathcal{P}_6(G)$ множество $A = C \cap K$ имеет непустое пересечение с любой подгруппой индекса 2 группы K , поэтому $\mathcal{F}_4^1 = \emptyset$.

6.4.2. Обозначим через $\mathcal{F}_4^2$ подсемейство множеств $N \in \mathcal{F}_4$ таких, что $|H| = n/6$.

Множество A не содержится ни в одном из левых смежных классов по подгруппе H , поэтому

$$\hat{A} = (A^{-1}A) \setminus H \neq \emptyset.$$

По условию множество NA содержит хотя бы один левый смежный класс по подгруппе H . Обозначим его через T . Из (24) следует, что $T\hat{A} \subset NA$. Так как $|T\hat{A}| \geq n/6$ и $T\hat{A} \cap T = \emptyset$, то

$$|NA| \geq |T| + |T\hat{A}| \geq n/3.$$

Отсюда

$$|NA| \geq 2|N|.$$

Таким образом, для всех множеств $N \in \mathcal{F}_4^2$ выполняется неравенство

$$|N| \leq (1 - 1/2)|\partial(N)|. \quad (25)$$

6.4.3. Пусть $\mathcal{F}_4^3$ — семейство множеств $N \in \mathcal{F}_4$ таких, что $|H| = n/8$ и хотя бы три правых смежных класса по H имеют непустые пересечения с $\tilde{A} = A^{-1}A$.

Обозначим левые смежные классы (не равные H) группы G по подгруппе H , $|H| = m/4$, через L_i , $i = 1, \dots, 7$, где $L_i \subset K$, $i = 1, 2, 3$, а $L_i \subset K'$, $i = 4, 5, 6, 7$. Без ограничения общности можно считать, что $NA \supseteq L_7$. Введем обозначения $R_i = (L_i)^{-1}$, $i = 1, \dots, 7$. Пусть R_k и R_l , $k, l \in \{1, 2, 3\}$, являются различными правыми смежными классами, не равными H , с которыми $\tilde{A}$ имеет непустое пересечение. Множества L_7R_k ,

$L_7 R_l$ и L_7 попарно не пересекаются, потому что они являются правыми смежными классами группы G по подгруппе $L_7 L_7^{-1}$. Из (24) и включения $L_7 \subseteq NA$ следует, что $L_7 R_k$ и $L_7 R_l$ содержатся в NA , откуда следует, что

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

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

$$|N| \leq (1 - 1/3)|\partial(N)|. \quad (26)$$

Из определения семейства $\mathcal{P}(G)$ следует, что множество A не содержится ни в каком левом смежном классе по подгруппе H . Это эквивалентно тому, что $\hat{A} = \tilde{A} \setminus H$ непусто. Далее будем считать, что $\hat{A}$ содержится в некотором правом смежном классе по H (случай, когда $\tilde{A}$ имеет непустое пересечение с двумя правыми смежными классами по H уже рассмотрен в пункте 6.4.3). Без ограничения общности можно считать, что $\hat{A} \subset R_1$. Условимся обозначать подгруппу $L_i H L_i^{-1}$ через H_i , $i = 1, 2, 3$.

6.4.4. Обозначим через $\mathcal{F}_4^4$ семейство множеств $N \in \mathcal{F}_4$ таких, что

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

Пусть существует элемент $a \in (A \cap R_1)$. Из того, что $N \cap NA = \emptyset$ и $L_7 \subseteq NA$, следует равенство $Na \cap L_7 R_1 = \emptyset$. Так как $\hat{A} \subset R_1$ и $L_7 \subset BA$, из (24) следует включение $L_7 R_1 \subset NA$. Используя неравенство $|N| \leq m/2$, получаем, что

$$|\partial(N)| \geq |NA| \geq |N| + |L_7 R_1| \geq \left(1 + \frac{m}{4|N|}\right) |N| \geq 3|N|/2,$$

откуда следует, что

$$|N| \leq (1 - 1/3)|\partial(N)|. \quad (27)$$

Пусть теперь $A \cap R_1 = \emptyset$ и $A \cap L_1 \neq \emptyset$. Тогда $A^{-1} \cap R_1 \neq \emptyset$. Пусть $a \in A^{-1} \cap R_1$. Поскольку $\partial(N) = N(A \cup A^{-1})$, то, как и при доказательстве (27), получаем, что $Ba^{-1} \cap L_7 R_1 = \emptyset$, откуда следует, что

$$|\partial(N)| = |N(A \cup A^{-1})| \geq |Na^{-1}| + |L_7 R_1| \geq |N| + m/4 \geq 3|N|/2.$$

Таким образом,

$$|N| \leq (1 - 1/3)|\partial(B)|. \quad (28)$$

Из неравенств (27) и (28) следует, что для всех множеств $N \in \mathcal{F}_4^4$ выполняется неравенство

$$|N| \leq (1 - 1/3)|\partial(B)|. \quad (29)$$

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

$$|H| = m/4, \quad \hat{A} \neq \emptyset, \quad \hat{A} \subset R_1, \quad A \cap (L_1 \cup R_1) = \emptyset, \quad H_1 \neq H.$$

Из условий следует, что не более чем два левых смежных класса по H имеют непустое пересечение с множеством A . Пользуясь неравенством

$$|A| > (1 - \beta)m/4,$$

отсюда получаем, что

$$|R_1 \cap L_1| \geq |\hat{A}| \geq (1 - \beta)m/8. \quad (30)$$

Заметим, что

$$\hat{A}^{-1} = \hat{A}, \quad \hat{A} \subset (R_1 \cap L_1).$$

Из леммы 2 и условия $H_1 \neq H$ следует, что

$$|H_1 \cap H| = m/(4k), \quad k = 2, 3, 4.$$

Отсюда, при помощи леммы 4 и оценки (30), получаем, что

$$H_1 \cap H = |R_1 \cap L_1| = m/8.$$

Также из леммы 4 следует, что R_1 имеет непустое пересечение ровно с двумя левыми смежными классами группы K по подгруппе H . 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 $A \subset K \setminus (R_1 \cup L_1 \cup H)$. Покажем, что $K \setminus (R_1 \cup L_1 \cup H)$ является объединением трех правых классов смежности по подгруппе $\hat{H} = H_1 \cap H$. Действительно, из леммы 3 следует, что $L_1 \cap R_1$ и $L_2 \cap R_1$ являются левыми смежными классами по подгруппе $\hat{H}$, откуда следует, что $L_1 \setminus R_1$ и $L_2 \setminus R_1$ также являются левыми смежными классами по $\hat{H}$. Ясно, что L_3 — объединение двух левых смежных классов по $\hat{H}$.

Таким образом, A содержится в объединении трех левых смежных классов по подгруппе порядка $m/8$. Но это исключено, так как $C \in \mathcal{P}_6(G)$ и $\mathcal{P}_6(G) \cap \mathcal{P}_5(G) = \emptyset$.

Итак, доказано, что $\mathcal{F}_4^5 = \emptyset$.

6.4.6. Обозначим через $\mathcal{F}_4^6$ семейство множеств $N \in \mathcal{F}_4$ таких, что

$$|H| = n/8, \quad \hat{A} \neq \emptyset, \quad \hat{A} \subset R_1, \quad A \cap (L_1 \cup R_1), \quad H_1 = H.$$

Из условия следует, что $R_1 = L_1$ и $A \cap (H \cup L_1) = \emptyset$. Легко видеть, что $H \cup L_1$ является подгруппой. По условию множество A имеет непустое пересечение с любой подгруппой индекса 2 группы K , поэтому $\mathcal{F}_4^6 = \emptyset$.

Итак, для всех множеств $A = C \cap K$, $C \in \mathcal{P}_6(G)$, граф $\mathcal{C}_A(K')$ является δ -расширителем. Из неравенств (20), (22), (23), (25), (26) и (29) следует, что в качестве δ можно взять $(1 - 5\beta)/(11 - 5\beta)$. Оценим мощность семейства $\mathcal{P}_6(G)$.

Пусть α и β удовлетворяют неравенству

$$\frac{1 - 5\beta}{7(11 - 5\beta)} - \alpha \log \frac{e}{\alpha} \leq \Delta_3.$$

Зафиксируем достаточно малое α , $0 < \alpha \leq \gamma$, и выберем подмножество $D \subset K$ такое, что $|D| = \lfloor \alpha t \rfloor$. Затем выберем $A \subset K$, независимое в графе $\mathcal{C}_D(K)$. При фиксированном

множестве A множество B выберем независимым в графе $\mathcal{C}_A(K')$. Применяя теорему 2 к графу $\mathcal{C}_D(K)$ и теорему 4 к графу $\mathcal{C}_A(K')$, получаем, что

$$|\mathcal{P}_6(G)| \leq \binom{m}{\lfloor \alpha m \rfloor} 2^{(m/2)(1+o(1))} 2^{(m/2)(1-(1-5\beta)/(7(11-5\beta))+o(1))} \\ \leq 2^{m(1+\alpha \log(e/\alpha)-(1-5\beta)/(7(11-5\beta))+o(1))}.$$

Таким образом,

$$|\mathcal{P}_6(G)| \leq 2^{m(1-\Delta_3)}. \quad (31)$$

Положим

$$\alpha = 0,0001, \quad \beta = 0,1, \quad \gamma = 0,01, \\ \Delta_1 = 0,1, \quad \Delta_2 = 0,002, \quad \Delta_3 = 0,005.$$

Тогда из неравенств (12)–(14), (18), (19) и (31) следует верхняя оценка в (2).

Автор благодарен А. А. Сапоженко за ценные советы и внимание к работе.

Список литературы

1. Alon N., Independent sets in regular graphs and sum-free subsets of finite groups. *Israel J. Math.* (1991) **73**, 247–256.
2. Lev V., Luczak T., Schoen T., Sum-free sets in abelian groups. *Israel J. Math.* (2001) **125** (2001), 347–367.
3. Сапоженко А. А., О числе множеств, свободных от сумм, в абелевых группах. *Вестник Московского ун-ва, сер. 1* (2002) **4**, 14–17.
4. Сапоженко А. А., О числе независимых множеств в расширителях. *Дискретная математика* (2001) **13**, №1, 56–62.
5. Olson J. E., On the sum of two sets in a group. *J. Number Theory* (1984) **18**, 110–120.
6. Гаврилов Г. П., Сапоженко А. А., *Задачи и упражнения по дискретной математике*. Физматлит, Москва, 2004.

Статья поступила 01.07.2004.

Переработанный вариант поступил 15.12.2004.