Math-Net.Ru

Общероссийский математический портал

А. А. Увакин, О двумерных суммах и разностях, *Матем. заметки*, 2015, том 98, выпуск 4, 570–589

DOI: <https://doi.org/10.4213/mzm10597>

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: 54.198.64.247

26 апреля 2023 г., 13:35:04

О двумерных суммах и разностях

А. А. Увакин

В данной статье рассказывается о некотором обобщении хорошо известной теоремы для множества $A \subseteq G$, где G – любая абелева группа. Согласно этому классическому результату из $|A + A| < (3/2)|A|$ или $|A - A| < (3/2)|A|$ следует, что $A \subseteq H$, где H – смежный класс по некоторой подгруппе G и $|H| \leq (3/2)|A|$.

Рассмотрим множества $A^2 \pm \Delta(A) \subseteq G^2$ – двумерные сумму и разность. Здесь $A^2 = A \times A$ – множество пар элементов из A , а $\Delta(A)$ – диагональное множество $\Delta(A) = \{(a, a) \in G \times G \mid a \in A\}$. Основной результат работы касается приведенных множеств и заключается в следующем. Если $|A^2 \pm \Delta(A)| < 7/4|A|^2$, то $A \subseteq H + x$ для некоторого $x \in G$ и подгруппы $H \subseteq G$, причем $|H| < 3/2|A|$.

Библиография: 10 названий.

DOI: 10.4213/mzm10597

1. Введение. Пусть $G = (G, +)$ – абелева группа и $A \subseteq G$ – ее произвольное подмножество. Определим *сумму* и *разность* множества A как

$$A + A = \{x : x = a_1 + a_2, a_1, a_2 \in A\} \subseteq G, \quad (1)$$

$$A - A = \{x : x = a_1 - a_2, a_1, a_2 \in A\} \subseteq G \quad (2)$$

соответственно. Число $D[A] = |A + A|/|A|$ называется *константой удвоения* множества A , а число $K[A] = |A - A|/|A|$ – *константой разности* множества A ; здесь $|A|$ означает мощность конечного множества A .

Особый интерес представляет ситуация, когда число $D[A]$ (соответственно $K[A]$) мало по сравнению с $|A|$, см. [1]. Такие множества называются *множествами с малым удвоением* (соответственно *разностью*). Это семейство интенсивно изучалось в работах Фреймана [2], Тао и Ву [1], Грина и Ружи [3], Сандерса [4], Шкредова [5] и др.

Фрейман впервые начал систематически исследовать такие множества в общем групповом контексте [6]. Сформулируем один из первых результатов в этом направлении.

ТЕОРЕМА 1. Пусть $A \subseteq G$, где G – произвольная абелева группа. Если выполнено

$$|A - A| < \frac{3}{2}|A|, \quad \text{либо} \quad |A + A| < \frac{3}{2}|A|,$$

то A содержится в смежном классе по подгруппе $H < G$, $|H| < (3/2)|A|$.

Работа выполнена при поддержке Российского научного фонда (грант № 14-11-00433).

Разность $A - A$ из формулы (2) можно интерпретировать как множество тех s , что $A \cap (A - s) \neq \emptyset$. В работе [7] рассматривались многомерные обобщения разностей, а именно, множества

$$H = \{(s_1, \dots, s_k) \in G^k \mid A \cap (A - s_1) \cap \dots \cap (A - s_k) \neq \emptyset\}. \quad (3)$$

Если использовать обозначение

$$\Delta(A) = \Delta_k(A) = \{(a, a, \dots, a) \mid a \in A\} \subseteq G^k,$$

то множество (3) может быть представлено в виде обычной разности

$$H = A^k - \Delta(A) = \{(x_1 - z, x_2 - z, \dots, x_k - z)\} \subseteq G^k.$$

В этой работе мы докажем обобщение и уточнение теоремы 1, ограничиваясь случаем $k = 2$.

ТЕОРЕМА 2. Пусть $A \subseteq G$, где G – произвольная абелева группа. Если выполнено

$$|A^2 + \Delta(A)| < \left(\frac{3}{2} + c\right)|A|^2 \quad \text{или} \quad |A^2 - \Delta(A)| < \left(\frac{3}{2} + c\right)|A|^2,$$

то A содержится в смежном классе по подгруппе $H < G$, $|H| < (3/2)|A|$. Здесь c – абсолютная константа, которая может быть взята равной $1/4$.

Напомним, что множеством симметрий (стабилизатором) множества X называется объект

$$\text{Sym } X = \{g \in G \mid X + g = X\}. \quad (4)$$

Доказательства и теорем 1 и 2 опираются на известную теорему Кнезера [1], [8], [9].

ТЕОРЕМА 3 (Кнезер). Пусть G – произвольная абелева группа и $A, B \subseteq G$. Тогда

$$\begin{aligned} |A + B| &\geq |A + \text{Sym}(A + B)| + |B + \text{Sym}(A + B)| - |\text{Sym}(A + B)| \\ &\geq |A| + |B| - |\text{Sym}(A + B)|. \end{aligned}$$

Как легко видеть, непосредственное применение теоремы Кнезера к множествам A^2 и $\Delta(A)$ не дает теоремы 2. Наше доказательство базируется на формуле [10]

$$|A^2 \pm \Delta(A)| = \sum_{z \in A - A} |A \pm A_z|, \quad \text{где } A_z = A \cap (A - z), \quad (5)$$

а затем теорема Кнезера используется для оценки мощностей множеств $A \pm A_z$ для некоторых z . Таким образом, мы сводим многомерную задачу (3) к обычным одномерным суммам и разностям.

Как известно, константа $3/2$ в теореме 1 является точной. Примером является множество $A = \{0, 1\} \subset \mathbb{Z}$. В этом случае $A + A = \{0, 1, 2\}$ и верно равенство $|A + A| = (3/2)|A|$. Кроме того, множество A не лежит ни в каком смежном классе единственной подгруппы $\mathbb{Z} - \{0\}$. Найденное значение c в теореме 2 равно 0.25 . То же самое множество $A = \{0, 1\} \subseteq \mathbb{Z}$ и в этой двумерной ситуации является экстремальным. Легко видеть, что $|A^2 \pm \Delta(A)| = 7$ и, следовательно, $c = 1/4$. Таким образом, теорема 2 является точной и представляет собой первый нетривиальный структурный результат о многомерных суммах с малым значением $|A^2 \pm \Delta(A)|$.

2. Основной результат. Теорему 2 можем переписать в более удобном виде.

ТЕОРЕМА 4. Пусть $|A^2 \pm \Delta(A)| < (7/4)|A|^2$. Тогда существует H – подгруппа G такая, что $|H| < (3/2)|A|$ и A содержится в некотором смежном классе по H .

Обозначим декартово произведение множеств $A \times B$ как (A, B) . Кроме того для удобства изложения будем считать, что $0 \in A$. Этого можем добиться сдвигом A на любой его элемент. Учитывая сказанное, $A \cap H \neq \emptyset$ для любой подгруппы H и тогда утверждение теоремы 4 состоит в том, что $A \subseteq H$.

Заметим, что из

$$|A^2 + \Delta(A)| < \frac{7}{4}|A|^2 \quad \text{и} \quad |A^2 + \Delta(A)| = \sum_{z \in A-A} |A + A_z| \geq |A| |A - A|$$

следует, что $|A - A| < (7/4)|A|$.

Утверждение ниже показывает структуру множества симметрий.

ЛЕММА 1. Множество $T = \text{Sym}(X) \subseteq G$ является подгруппой. Кроме того, выполнено $T \subseteq X - X$.

Следующая лемма показывает структуру одномерного множества с удвоением меньшим, чем $7/4$.

ЛЕММА 2. Пусть $A \subseteq G$ и выполнено $|A \pm A| < (7/4)|A|$. Пусть также $H = \text{Sym}(A \pm A)$ соответственно. Тогда выполнено одно из следующих трех утверждений:

- 1) $|H| < (7/4)|A|$ такая, что A содержится в H , причем $A \pm A = H$;
- 2) $|H| < (7/12)|A|$ такая, что A содержится в объединении двух смежных классов по H и $A \pm A$ равно объединению ровно трех смежных классов по A ; при этом для некоторого $x \notin H$ выполнено

$$A \subseteq H \sqcup (H + x), \\ A + A = H \sqcup (H + x) \sqcup (H + 2x), \quad A - A = (H - x) \sqcup H \sqcup (H + x);$$

- 3) $|H| < (7/20)|A|$ такая, что A содержится в объединении трех смежных классов по H и $A \pm A$ равно объединению ровно пяти смежных классов по A , причем выполнено одно из следующих четырех условий:

а) $A \subseteq H \sqcup (H + x) \sqcup (H + y)$, $2x \in H$, и тогда

$$A + A = H \sqcup (H + x) \sqcup (H + y) \sqcup (H + 2y) \sqcup (H + x + y); \quad (6)$$

б) $A \subseteq H \sqcup (H + x) \sqcup (H + y)$, $2x \in (H + 2y)$, и тогда

$$A + A = H \sqcup (H + x) \sqcup (H + y) \sqcup (H + 2x) \sqcup (H + x + y); \quad (7)$$

в) $A \subseteq H \sqcup (H + x) \sqcup (H + 2x)$, и тогда

$$A + A = H \sqcup (H + x) \sqcup (H + 2x) \sqcup (H + 3x) \sqcup (H + 4x), \\ A - A = H \sqcup (H - x) \sqcup (H + x) \sqcup (H - 2x) \sqcup (H + 2x); \quad (8)$$

г) $A \subseteq H \sqcup (H - x) \sqcup (H + x)$, и тогда

$$\begin{aligned} A + A &= H \sqcup (H + x) \sqcup (H + 2x) \sqcup (H - x) \sqcup (H - 2x), \\ A - A &= H \sqcup (H - x) \sqcup (H + x) \sqcup (H - 2x) \sqcup (H + 2x). \end{aligned} \quad (9)$$

Во введении мы дали определение множества симметрий (4), а в лемме 1 показали его структуру. По определению H верно $A \pm A + H = A \pm A$. Поэтому $A \pm A$ есть объединение некоторого числа смежных классов по H . Обозначим через R количество смежных классов по H в $A \pm A$. Тогда из сказанного выше следует, что $R = |A \pm A|/|H|$. Также нам понадобится k – количество смежных классов по H , имеющих непустое пересечение с A . Из определения k следует, что $|A| \leq k|H|$ и, более того, для некоторых $x_1, \dots, x_k \in G$ выполнено

$$A \subseteq \bigsqcup_{j=1}^k (H + x_j).$$

Числа R и k нам понадобятся в дальнейшем изложении.

Докажем теперь лемму 2.

ДОКАЗАТЕЛЬСТВО ЛЕММЫ 2. Из леммы 1 следует, что выполнено $\text{Sym}(A \pm A) = -\text{Sym}(A \pm A)$. Тогда по теореме Кнезера, примененной для множеств $A = A$ и $B = A$, в случае $A + A$ и для $A = A$ и $B = -A$ в случае $A - A$, имеем

$$\frac{7}{4}|A| > |A \pm A| \geq 2|A + \text{Sym}(A \pm A)| - |\text{Sym}(A \pm A)| \geq 2|A| - |\text{Sym}(A \pm A)|.$$

Отсюда следует, что $|H| > (1/4)|A|$.

Имеем

$$\frac{7}{4}|A| > |A \pm A| = |A \pm A + H| = R|H| > \frac{1}{4}R|A|,$$

а значит, $R < 7$. Так как $0 \in A$, то $A \subseteq A \pm A$. Таким образом, A содержится в объединении не более чем шести смежных классов по H .

Из наших рассуждений, а также из определений чисел k и R имеем

$$R|H| = |A \pm A| \geq 2|A + H| - |H| = (2k - 1)|H|.$$

Тогда $k \leq (R + 1)/2$. Кроме того, ясно, что

$$|A + A| \leq \frac{|A|(|A| + 1)}{2},$$

и тогда $R \leq k(k + 1)/2$, а также

$$|A - A| \leq |A|^2 - |A| + 1 \quad \text{и} \quad R \leq k(k - 1) + 1$$

в случае разностей.

Имеем следующие случаи в зависимости от R :

- если $R = 6$, то $k \leq 3.5$ и $k > 2$, а значит, $k = 3$;
- если $R = 5$, то $k \leq 3$ и $k > 2$, а значит, $k = 3$;
- если $R = 4$, то $k \leq 2.5$ и $k > 2$, т.е. этот случай невозможен;
- если $R = 3$, то $k \leq 2$ и $k > 1$, а значит, $k = 2$;

- если $R = 2$, то $k \leq 1.5$ и $k > 1$, т.е. этот случай невозможен;
- если $R = 1$, то $k = 1$.

Пусть $R = 6$, $k = 3$. Тогда $|A| \leq 3|H|$ и $6|H| = |A \pm A| < (7/4)|A|$, откуда $6|H| < (21/4)|H|$, противоречие. Значит, этот случай невозможен.

Пусть $R = 5$, $k = 3$. Тогда

$$A \subseteq H \sqcup (H + x) \sqcup (H + y) \quad (10)$$

для некоторых $x, y \in G$. Тогда $5|H| = |A \pm A| < (7/4)|A|$ и $|H| < (7/20)|A|$. В этом случае выполняется условие 3) леммы. Имеем

$$A + A = H \sqcup (H + x) \sqcup (H + y) \cup (H + 2x) \cup (H + 2y) \cup (H + x + y), \quad (11)$$

но так как $R = 5$, то один из смежных классов в определении $A + A$ совпадает с другим. В равенстве выше первые 2 объединения дизъюнкты по (10). Также очевидно, что не совпадают друг с другом смежные классы $H + 2x \neq H + x$, $H + 2x \neq H + x + y$. Тогда остальными возможными совпадениями с точностью до замены x на y будут следующие:

- $H + 2x = H$;
- $H + 2x = H + y$;
- $H + 2x = H + 2y$;
- $H + x + y = H$, тогда $H + y = H - x$.

Они и дают пункт 3) в условии леммы в случае суммы.

Рассмотрим теперь множество $A - A$:

$$A - A = H \sqcup (H + x) \sqcup (H + y) \cup (H - x) \cup (H - y) \cup (H + x - y) \cup (H + y - x); \quad (12)$$

так как $R = 5$, то среди смежных классов выше есть две пары совпадающих. Как и ранее, очевидно, что не совпадают

$$\begin{aligned} H - x \neq H, \quad H - y \neq H, \quad H - y \neq H - x - y, \quad H + x + y \neq H + x, \\ H + x + y \neq H + y, \quad H - x \neq H - y, \quad H - x \neq H - y - x, \quad H - x \neq H + y - x. \end{aligned}$$

Рассмотрим возможности других совпадений.

- Пусть $H - x = H + x$; тогда $H + 2x = H$ и

$$A - A = H \sqcup (H + x) \sqcup (H + y) \cup (H - y) \cup (H + x + y) \cup (H - x - y), \quad (13)$$

имеется 6 смежных классов, значит, еще один из них совпадает с каким-то другим.

- Пусть $H - y = H + x$; тогда $H - y = H - x$, получаем противоречие с (10).
- Пусть $H - y = H + y$; тогда $H + x + y = H - x - y$ и мы получим, что $A - A$ равно объединению всего четырех смежных классов, что невозможно.
- Пусть $H - y = H + x + y$; тогда $H + 2y = H + x$. В этом случае $H - x - y = H + y$, так же получаем, что $A - A$ равно объединению всего четырех смежных классов.

а4) Пусть $H + x + y = H$; тогда $H + x = H - y$ и $A - A$ равно объединению всего четырех смежных классов.

- Пусть $H + x + y = H - x - y$; тогда $H + y = H - y$, получаем случай а2).

Аналогично $H - x - y$ не совпадает ни с одним из рассматриваемых смежных классов по H .

Итак, ни один из подпунктов а) не реализуется.

б) Пусть $H - x = H + y$; тогда

$$A - A = H \sqcup (H + x) \sqcup (H - x) \cup (H - 2x) \cup (H + 2x), \quad (14)$$

здесь 4 смежных класса, если x имеет порядок не менее 6. В этом случае

$$A - A = H \sqcup (H + x) \sqcup (H - x) \sqcup (H - 2x) \sqcup (H + 2x), \quad A \subseteq H \sqcup (H + x) \sqcup (H - x),$$

что соответствует пункту (3г) леммы.

в) Пусть $H - x = H + x - y$; тогда $H + y = H + 2x$ и

$$A - A = H \sqcup (H + x) \sqcup (H + 2x) \sqcup (H - x) \sqcup (H - 2x); \quad (15)$$

тогда

$$A \subseteq H \sqcup (H + x) \sqcup (H + 2x),$$

что соответствует пункту (3в) леммы.

В пунктах а)–в) мы рассматривали все совпадения с участием смежного класса $H - x$.

г) Если с одним из смежных классов в выражении (12) совпадает смежный класс $H - y$, то имеем те же случаи с точностью до переименования переменных.

д) Пусть $H + y - x = H + x - y$; тогда

$$A - A = H \sqcup (H + x) \sqcup (H + y) \cup (H + x - y) \cup (H - x) \cup (H - y), \quad (16)$$

здесь 6 смежных классов. Чтобы R было равно 5, надо, чтобы в этом объединении было еще одно совпадение смежных классов. Но остальные совпадения уже были разобраны выше.

Итак, случай $R = 5$, $k = 3$ разобран нами полностью.

Пусть теперь $R = 3$, $k = 2$; тогда $A \subseteq H \sqcup (H + x)$ для некоторого элемента $x \notin H$. Значит,

$$A + A = H \sqcup (H + x) \sqcup (H + 2x), \quad A - A = H \sqcup (H - x) \sqcup (H + x),$$

$$|H| = \frac{1}{3}|A \pm A| < \frac{7}{12}|A|$$

и, значит, выполнен пункт 2) леммы.

Ясно, что при $R = 1$ выполнено $A \subseteq H$, и по определению $A \pm A = H$. Получили пункт 1) леммы. Лемма доказана.

Следующая лемма показывает связь между $|A - A|$ и $|A + A|$ в случае константы разности меньшей, чем $7/4$.

ЛЕММА 3. Пусть $|A - A| < (7/4)|A|$. Тогда $|A + A| < (7/4)|A|$.

ДОКАЗАТЕЛЬСТВО. По предыдущей лемме, примененной для разностей, из неравенства $|A - A| < (7/4)|A|$ следует одно из следующих условий:

- 1) $R = 1$, $k = 1$, $A - A = H$;
- 2) $R = 3$, $k = 2$, $A - A = H \sqcup (H + x) \sqcup (H - x)$;
- 3) $R = 5$, $k = 3$ и возможно 2 случая:

а) $A \subseteq H \sqcup (H + x) \sqcup (H + 2x)$ и

$$A - A = H \sqcup (H + x) \sqcup (H + 2x) \sqcup (H - x) \sqcup (H - 2x);$$

б) $A \subseteq H \sqcup (H + x) \sqcup (H - x)$ и

$$A - A = H \sqcup (H + x) \sqcup (H + 2x) \sqcup (H - x) \sqcup (H - 2x).$$

Рассмотрим первый случай:

$$|H| = |A - A| < \frac{7}{4}|A| \quad \text{и} \quad A \subseteq H.$$

Следовательно,

$$A + A \subseteq H \quad \text{и} \quad |A + A| \leq |H| = |A - A| < \frac{7}{4}|A|.$$

Далее, рассмотрим случай 2):

$$A \subseteq H \sqcup (H + x) \quad \text{для некоторого } x \notin H.$$

Тогда

$$A - A = (H - x) \sqcup H \sqcup (H + x);$$

при этом $A + A = H \sqcup (H + x) \sqcup (H + 2x)$ и, значит,

$$A + A - x = (H - x) \sqcup H \sqcup (H + x) = A - A.$$

Отсюда следует $|A + A| = |A - A| < (7/4)|A|$.

Последний случай. При $A \subseteq H \sqcup (H + x) \sqcup (H - x)$ выполнено

$$A + A \subseteq H \sqcup (H - x) \sqcup (H + x) \sqcup (H - 2x) \sqcup (H + 2x) = A - A, \quad (17)$$

отсюда $|A + A| \leq |A - A| < (7/4)|A|$.

При $A \subseteq H \sqcup (H + x) \sqcup (H + 2x)$ выполнено

$$A + A \subseteq H \sqcup (H + x) \sqcup (H + 2x) \sqcup (H + 3x) \sqcup (H + 4x) = A - A + 2x, \quad (18)$$

и ясно, что

$$|A + A| \leq |A - A + 2x| = |A - A| < \frac{7}{4}|A|.$$

Лемма доказана.

Учитывая предыдущую лемму, дальше будем доказывать все утверждения для множества $A + A$ с $|A + A| < (7/4)|A|$.

В лемме ниже мы подробно разберем пункт 2) структурной леммы 2.

ЛЕММА 4. Пусть для $A \subseteq G$ выполнено $|A \pm A| < (7/4)|A|$ и $A \pm A$ равно объединению ровно трех смежных классов по H . Тогда

$$|A^2 \pm \Delta(A)| \geq \frac{7}{4}|A|^2.$$

ДОКАЗАТЕЛЬСТВО. По лемме 2 $A \subseteq H \sqcup (H + x)$ для некоторого $x \notin H$ и

$$A + A = H \sqcup (H + x) \sqcup (H + 2x), \quad A - A \subseteq H \sqcup (H - x) \sqcup (H + x), \quad |H| < \frac{7}{12}|A|,$$

в случае знаков “+” в условии;

$$A + A \subseteq H \sqcup (H + x) \sqcup (H + 2x), \quad A - A = H \sqcup (H - x) \sqcup (H + x), \quad |H| < \frac{7}{12}|A|,$$

в случае знаков “−” в условии. Обозначим

$$A_1 = A \cap H, \quad A_2 = A \cap (H + x).$$

Имеем

$$\begin{aligned} A^2 \pm \Delta(A) &= (A_1 \sqcup A_2)^2 \pm \Delta(A_1 \sqcup A_2) \\ &= (A_1, A_1) \sqcup (A_1, A_2) \sqcup (A_2, A_1) \sqcup (A_2, A_2) \pm (\Delta(A_1) \sqcup \Delta(A_2)). \end{aligned} \quad (19)$$

Воспользуемся равенством $(B \sqcup C) \pm D = (B \pm D) \cup (C \pm D)$. Отсюда

$$\begin{aligned} A^2 \pm \Delta(A) &= [(A_1, A_1) \pm \Delta(A_1)] \cup [(A_1, A_2) \pm \Delta(A_1)] \cup [(A_2, A_1) \pm \Delta(A_1)] \\ &\quad \cup [(A_2, A_2) \pm \Delta(A_1)] \cup [(A_1, A_1) \pm \Delta(A_2)] \cup [(A_1, A_2) \pm \Delta(A_2)] \\ &\quad \cup [(A_2, A_1) \pm \Delta(A_2)] \cup [(A_2, A_2) \pm \Delta(A_2)]. \end{aligned} \quad (20)$$

Заметим, что

$$\begin{aligned} (A_1, A_1) \pm \Delta(A_1) &\subseteq (H, H), & (A_1, A_2) \pm \Delta(A_1) &\subseteq (H, H + x), \\ (A_2, A_1) \pm \Delta(A_1) &\subseteq (H + x, H), & (A_2, A_2) \pm \Delta(A_1) &\subseteq (H + x, H + x), \\ (A_1, A_1) \pm \Delta(A_2) &\subseteq (H \pm x, H \pm x), & (A_1, A_2) \pm \Delta(A_2) &\subseteq (H + x, H + 2x), \\ (A_1, A_2) - \Delta(A_2) &\subseteq (H - x, H), & (A_2, A_1) + \Delta(A_2) &\subseteq (H + 2x, H + x), \\ (A_2, A_1) - \Delta(A_2) &\subseteq (H, H - x), & (A_2, A_2) + \Delta(A_2) &\subseteq (H + 2x, H + 2x), \\ (A_2, A_2) - \Delta(A_2) &\subseteq (H, H), \end{aligned} \quad (21)$$

и можем переписать

$$\begin{aligned} A^2 + \Delta(A) &= [(A_1, A_1) + \Delta(A_1)] \sqcup [(A_1, A_2) + \Delta(A_1)] \sqcup [(A_2, A_1) + \Delta(A_1)] \\ &\quad \sqcup [((A_2, A_2) + \Delta(A_1)) \cup ((A_1, A_1) + \Delta(A_2))] \\ &\quad \sqcup [(A_1, A_2) + \Delta(A_2)] \sqcup [(A_2, A_1) + \Delta(A_2)] \sqcup [(A_2, A_2) + \Delta(A_2)], \\ A^2 - \Delta(A) &= [(A_1, A_1) - \Delta(A_1)] \sqcup [(A_2, A_2) - \Delta(A_2)] \sqcup [(A_1, A_2) - \Delta(A_1)] \\ &\quad \sqcup [(A_2, A_1) - \Delta(A_1)] \sqcup [((A_2, A_2) - \Delta(A_1)) \\ &\quad \sqcup ((A_1, A_1) - \Delta(A_2))] \sqcup [(A_1, A_2) - \Delta(A_2)] \sqcup [(A_2, A_1) - \Delta(A_2)]. \end{aligned} \quad (22)$$

В обоих равенствах имеется только по одному недизъюнктному объединению.

Для $i = 1, 2$ выполнено

$$|A_i| \geq |A| - |H| > \left(\frac{12}{7} - 1\right)|H| = \frac{5}{7}|H|.$$

Покажем, что $|A_1^2 \pm \Delta(A_1)| = |H|^2$. Для остальных множеств в (21) аналогичные равенства доказываются тем же способом. Имеем

$$|A_1^2 \pm \Delta(A_1)| = \sum_{z \in A_1 - A_1} |A_1 \pm A_{1z}|; \quad (23)$$

ясно, что $A_{1z} = A_1 \cap (A_1 - z) \subseteq H$, $A_1 \cup (A_1 - z) \subseteq H$ и

$$|A_{1z}| = |A_1| + |A_1 - z| - |A_1 \cup (A_1 - z)| \geq 2|A_1| - |H| > \frac{3}{7}|H|.$$

Значит, для любого $z \in A_1 - A_1$ выполнено $|A_1| + |A_{1z}| > |H|$; отсюда следует, что $|A_1 \pm A_{1z}| = |H|$, а также $|A_1 - A_1| = |H|$. И следовательно,

$$|A_1^2 \pm \Delta(A_1)| = \sum_{z \in A_1 - A_1} |A_1 \pm A_{1z}| = \sum_{z \in H} |H| = |H|^2. \quad (24)$$

Отсюда $|A^2 \pm \Delta(A)| = 7|H|^2$. Так как $A \subseteq H \sqcup (H + x)$, то $|A| \leq 2|H|$; значит, $|A^2 \pm \Delta(A)| \geq (7/4)|A|^2$. Лемма доказана.

Следующее утверждение описывает третий вариант в лемме 2. В некоторых подслучаях оценка получается даже лучше той, что указана в условии леммы 5, однако для наших целей достаточно и более слабых неравенств.

ЛЕММА 5. Пусть $A \subseteq G$, выполнено $|A \pm A| < (7/4)|A|$ и $A \pm A$ лежит в объединении ровно пяти смежных классов по H . Тогда

$$|A^2 \pm \Delta(A)| \geq \frac{19}{9}|A|^2.$$

ДОКАЗАТЕЛЬСТВО. По лемме 2 имеем $|H| < (7/20)|A|$, что A содержится в объединении трех смежных классов по H и $A + A$ равно объединению ровно пяти смежных классов по A , причем выполнено одно из условий а)-г).

Обозначим

$$A_1 = H \cap A, \quad A_2 = (H + x) \cap A, \quad A_3 = (H + y) \cap A.$$

В этих терминах имеем

$$\begin{aligned} A^2 + \Delta(A) &= (A_1, A_1) \sqcup (A_1, A_2) \sqcup (A_1, A_3) \sqcup (A_2, A_1) \sqcup (A_2, A_2) \sqcup (A_2, A_3) \sqcup (A_3, A_1) \\ &\sqcup (A_3, A_2) \sqcup (A_3, A_3) + \Delta(A_1) \sqcup \Delta(A_2) \sqcup \Delta(A_3) = [(A_1, A_1) + \Delta(A_1)] \\ &\sqcup [(A_1, A_1) + \Delta(A_2)] \sqcup [(A_1, A_1) + \Delta(A_3)] \sqcup [(A_1, A_2) + \Delta(A_1)] \\ &\sqcup [(A_1, A_2) + \Delta(A_2)] \sqcup [(A_1, A_2) + \Delta(A_3)] \sqcup [(A_1, A_3) + \Delta(A_1)] \\ &\sqcup [(A_1, A_3) + \Delta(A_2)] \sqcup [(A_1, A_3) + \Delta(A_3)] \sqcup [(A_2, A_1) + \Delta(A_1)] \\ &\sqcup [(A_2, A_1) + \Delta(A_2)] \sqcup [(A_2, A_1) + \Delta(A_3)] \sqcup [(A_2, A_2) + \Delta(A_1)] \\ &\sqcup [(A_2, A_2) + \Delta(A_2)] \sqcup [(A_2, A_2) + \Delta(A_3)] \sqcup [(A_2, A_3) + \Delta(A_1)] \\ &\sqcup [(A_2, A_3) + \Delta(A_2)] \sqcup [(A_2, A_3) + \Delta(A_3)] \sqcup [(A_3, A_1) + \Delta(A_1)] \\ &\sqcup [(A_3, A_1) + \Delta(A_2)] \sqcup [(A_3, A_1) + \Delta(A_3)] \sqcup [(A_3, A_2) + \Delta(A_1)] \\ &\sqcup [(A_3, A_2) + \Delta(A_2)] \sqcup [(A_3, A_2) + \Delta(A_3)] \sqcup [(A_3, A_3) + \Delta(A_1)] \end{aligned}$$

$$\begin{aligned}
& \cup [(A_3, A_3) + \Delta(A_2)] \cup [(A_3, A_3) + \Delta(A_3)] \subseteq (H, H) \cup (H + x, H + x) \\
& \cup (H + y, H + y) \cup (H + x, H + x) \cup (H + x, H + 2x) \\
& \cup (H + y, H + x + y) \cup (H, H + y) \cup (H + x, H + x + y) \\
& \cup (H + y, H + 2y) \cup (H + x, H) \cup (H + 2x, H + x) \cup (H + x + y, H + y) \\
& \cup (H + x, H + x) \cup (H + 2x, H + 2x) \cup (H + x + y, H + x + y) \\
& \cup (H + x, H + y) \cup (H + 2x, H + x + y) \cup (H + x + y, H + 2y) \\
& \cup (H + y, H) \cup (H + x + y, H + x) \cup (H + 2y, H + y) \\
& \cup (H + y, H + x) \cup (H + x + y, H + 2x) \cup (H + 2y, H + x + y) \\
& \cup (H + y, H + y) \cup (H + x + y, H + x + y) \cup (H + 2y, H + 2y). \quad (25)
\end{aligned}$$

Включение показывается так же, как и в лемме 4, для каждого множества отдельно (см. равенства (21)).

Покажем, что на самом деле вместо включения в предыдущем выражении имеется равенство множеств. Для этого проверим, что $|(A_1, A_1) + \Delta(A_1)| = |(H, H)| = |H|^2$; для остальных множеств аналогичные равенства доказываются тем же способом. Так как $A = A_1 \sqcup A_2 \sqcup A_3$, то выполнено

$$|A_1| = |A| - |A_2| - |A_3| \geq |A| - 2|H| > \left(\frac{20}{7} - 2\right)|H| = \frac{6}{7}|H|.$$

Покажем, что $|A_1^2 + \Delta(A_1)| = |H|^2$. Имеем

$$|A_1^2 + \Delta(A_1)| = \sum_{z \in A_1 - A_1} |A_1 + A_{1z}|. \quad (26)$$

Ясно, что для всех $z \in A_1 - A_1 \subseteq H$ выполнено

$$\begin{aligned}
A_{1z} &= A_1 \cap (A_1 - z) \subseteq H, \quad A_1 \cup (A_1 - z) \subseteq H, \\
|A_{1z}| &= |A_1| + |A_1 - z| - |A_1 \cup (A_1 - z)| \geq 2|A_1| - |H| > \frac{5}{7}|H|.
\end{aligned}$$

Значит, для любого $z \in A_1 - A_1$ выполнено $|A_1| + |A_{1z}| > |H|$. Отсюда следует, что $|A_1 + A_{1z}| = |H|$, а также $|A_1 - A_1| = |H|$. Следовательно,

$$|A_1^2 + \Delta(A_1)| = \sum_{z \in A_1 - A_1} |A_1 + A_{1z}| = \sum_{z \in H} |H| = |H|^2, \quad (27)$$

и равенство множеств доказано. Таким образом, в (25) вместо включения имеет место равенство. Заметим, что (25) мы получили, не учитывая соотношения между x и y , но в данном случае такие соотношения имеются и задаются условиями а)–г) пункта 3) леммы 2.

Рассмотрим случай а), соответствующий условию (6). Имеем $2x \in H$ и, следовательно, перепишем (25) в виде

$$\begin{aligned}
A^2 + \Delta(A) &= (H, H) \sqcup (H + x, H + x) \sqcup (H + y, H + y) \sqcup (H + x, H) \\
&\sqcup (H + y, H + x + y) \sqcup (H, H + y) \sqcup (H + x, H + x + y) \\
&\sqcup (H + y, H + 2y) \sqcup (H, H + x) \sqcup (H + x + y, H + y)
\end{aligned}$$

$$\begin{aligned}
& \sqcup (H + x + y, H + x + y) \sqcup (H + x, H + y) \sqcup (H, H + x + y) \\
& \sqcup (H + x + y, H + 2y) \sqcup (H + y, H) \sqcup (H + x + y, H) \\
& \sqcup (H + x + y, H + x) \sqcup (H + 2y, H + y) \sqcup (H + y, H + x) \\
& \sqcup (H + 2y, H + x + y) \sqcup (H + 2y, H + 2y). \tag{28}
\end{aligned}$$

В последнем выражении объединение множеств дизъюнктивное, а их количество равно 21, причем у каждого из них по доказанному ранее мощность равна $|H|^2$. Значит, $|A^2 + \Delta(A)| = 21|H|^2$, а так как $A \subseteq H \sqcup (H + x) \sqcup (H + y)$, то

$$|A| \leq 3|H| \quad \text{и} \quad |A^2 + \Delta(A)| \geq \frac{21}{9}|A|^2.$$

Теперь рассмотрим случай б), соответствующий условию (7). Выполнено $2x \in (H + 2y)$ и

$$\begin{aligned}
A^2 + \Delta(A) = & (H, H) \sqcup (H + x, H + x) \sqcup (H + y, H + y) \sqcup (H + x, H + 2x) \\
& \sqcup (H + y, H + x + y) \sqcup (H, H + y) \sqcup (H + x, H + x + y) \\
& \sqcup (H + y, H + 2x) \sqcup (H + x, H) \sqcup (H + 2x, H + x) \\
& \sqcup (H + x + y, H + y) \sqcup (H + 2x, H + 2x) \sqcup (H + x + y, H + x + y) \\
& \sqcup (H + x, H + y) \sqcup (H + 2x, H + x + y) \sqcup (H + x + y, H + 2x) \\
& \sqcup (H + y, H) \sqcup (H + x + y, H + x) \sqcup (H + 2x, H + y) \\
& \sqcup (H + y, H + x) \sqcup (H + 2x, H + 2x). \tag{29}
\end{aligned}$$

Тогда аналогично предыдущему случаю $|A^2 + \Delta(A)| = 21|H|^2$. Учитывая, что $A \subseteq H \sqcup (H + x) \sqcup (H + y)$, $|A| \leq 3|H|$, получаем, что выполнено

$$|A^2 + \Delta(A)| \geq \frac{21}{9}|A|^2.$$

В случае в), соответствующем условию (8), имеем

$$A \subseteq H \sqcup (H + x) \sqcup (H + 2x), \quad A + A = H \sqcup (H + x) \sqcup (H + 2x) \sqcup (H + 3x) \sqcup (H + 4x).$$

Тогда можем переписать (25) в виде

$$\begin{aligned}
A^2 + \Delta(A) = & (H, H) \sqcup (H + x, H + x) \sqcup (H + 2x, H + 2x) \sqcup (H + x, H + 2x) \\
& \sqcup (H + 2x, H + 3x) \sqcup (H, H + 2x) \sqcup (H + x, H + 3x) \\
& \sqcup (H + 2x, H + 4x) \sqcup (H + x, H) \sqcup (H, H + x) \sqcup (H + 2x, H + x) \\
& \sqcup (H + 3x, H + 2x) \sqcup (H + 3x, H + 3x) \sqcup (H + 3x, H + 4x) \\
& \sqcup (H + 2x, H) \sqcup (H + 3x, H + x) \sqcup (H + 4x, H + 2x) \\
& \sqcup (H + 4x, H + 3x) \sqcup (H + 4x, H + 4x); \tag{30}
\end{aligned}$$

значит,

$$|A^2 + \Delta(A)| = 19|H|^2 \geq \frac{19}{9}|A|^2.$$

В отличие от предыдущих случаев а), б) в данном случае $A - A$ равно объединению пяти смежных классов по H , поэтому необходимо рассмотреть и множество $A^2 - \Delta(A)$. Аналогично случаю с суммой, имеем

$$A^2 - \Delta(A) = (H, H) \sqcup (H, H + x) \sqcup (H, H + 2x) \sqcup (H + x, H) \sqcup (H + x, H + x)$$

$$\begin{aligned}
& \sqcup (H + x, H + 2x) \sqcup (H + 2x, H) \sqcup (H + 2x, H + x) \sqcup (H + 2x, H + 2x) \\
& \sqcup (H - x, H - x) \sqcup (H - x, H) \sqcup (H - x, H + x) \sqcup (H, H - x) \\
& \sqcup (H + x, H - x) \sqcup (H - 2x, H - 2x) \sqcup (H - 2x, H - x) \\
& \sqcup (H - 2x, H) \sqcup (H - x, H - 2x) \sqcup (H, H - 2x)
\end{aligned} \tag{31}$$

и, следовательно,

$$|A^2 - \Delta(A)| = 19|H|^2 \geq \frac{19}{9}|A|^2.$$

Случай г), соответствующий условию (9), можем свести к случаю в) следующим образом. Рассмотрим множество $A' = A + x$; тогда $A' \subseteq H \sqcup (H + x) \sqcup (H + 2x)$ и при этом

$$|A'^2 + \Delta(A')| = |A^2 + \Delta(A)| \quad \text{и} \quad |A'^2 - \Delta(A')| = |A^2 - \Delta(A)|.$$

По доказанному в предыдущем случае выполнено

$$|A'^2 \pm \Delta(A')| \geq \frac{19}{9}|A'|^2 = \frac{19}{9}|A|^2.$$

Лемма доказана.

Далее рассмотрим оставшийся случай множества A , удовлетворяющего условию (1) из леммы 2. Далее в этом пункте будем рассматривать множество A такое, что

$$|A^2 \pm \Delta(A)| < \frac{7}{4}|A|^2, \quad A \subseteq H = \text{Sym}(A \pm A), \quad R = 1.$$

Мы уже выяснили, что $|H| < (7/4)|A|$. Улучшим эту оценку.

Для начала покажем, что

$$A + A = A - A = \text{Sym}(A + A) = \text{Sym}(A - A).$$

По определению группы симметрий и так как $A \subseteq \text{Sym}(A \pm A)$, имеем $A \pm A \subseteq \text{Sym}(A \pm A)$. Понятно, что в таком случае из $A \pm A + \text{Sym}(A \pm A) = A \pm A$ следует $A \pm A = \text{Sym}(A \pm A)$. Докажем, что группы симметрий $\text{Sym}(A + A)$ и $\text{Sym}(A - A)$ равны. По лемме 3 из $|A - A| < (7/4)|A|$ вытекает, что $|A + A| < (7/4)|A|$. По лемме 2 имеем одновременно

$$A \subseteq \text{Sym}(A + A) \quad \text{и} \quad A \subseteq \text{Sym}(A - A).$$

Таким образом, $A \subseteq \text{Sym}(A + A) \cap \text{Sym}(A - A) = H'$, причем H' – подгруппа, как пересечение подгрупп. Но тогда

$$\text{Sym}(A \pm A) = A \pm A \subseteq \text{Sym}(A + A) \cap \text{Sym}(A - A);$$

получаем равенство групп симметрий.

ЗАМЕЧАНИЕ 1. В рассматриваемом случае, учитывая

$$\text{Sym}(A + A) = \text{Sym}(A - A) = A + A = A - A,$$

следующую лемму можно доказывать только для множества $A + A$ и подгруппы H равной $\text{Sym}(A + A)$.

В доказательстве далее нам понадобится несколько вспомогательных величин. Обозначим $H^z = \text{Sym}(A + A_z)$ группу симметрий множества $A + A_z$.

ЛЕММА 6. *Группа H^z является подгруппой H .*

ДОКАЗАТЕЛЬСТВО. Очевидно, что $A + A_z \subseteq A + A = H$. По лемме 1 выполнено

$$H^z \subseteq (A + A_z) - (A + A_z) \subseteq (A + A) - (A + A) = H - H = H;$$

кроме того, H^z является подгруппой G . Лемма доказана.

Обозначим через $k(z)$ индекс H^z в H . Тогда

$$k(z) = \frac{|H|}{|H^z|} \quad (32)$$

и является натуральным числом.

Доказательство основной теоремы 4 завершается следующей леммой.

ЛЕММА 7. *Пусть $|A^2 + \Delta(A)| < (7/4)|A|^2$ и при этом $A \subseteq H = \text{Sym}(A + A)$. Тогда*

$$|H| < \frac{3}{2}|A|.$$

ДОКАЗАТЕЛЬСТВО. Учитывая теорему 1 при $|A + A| < (3/2)|A|$ утверждение леммы верно, поэтому далее предполагаем, что

$$|A + A| \geq \frac{3}{2}|A|. \quad (33)$$

Доказательство разобьем на три части. Рассмотрим сначала случай

$$\frac{3}{2}|A| \leq |A + A| < \frac{8}{5}|A|.$$

Отсюда следует, что $(5/8)|H| < |A| \leq (2/3)|H|$.

Для любого $z \in H = A - A$ имеет место $A \subseteq H$ и $A - z \subseteq H$; значит, выполнена оценка

$$|A_z| = |A| + |A - z| - |A \cup (A - z)| \geq 2|A| - |H| > \frac{1}{4}|H|.$$

Будем пользоваться теоремой 3 Кнезера в виде

$$|A + A_z| \geq |A + H^z| + |A_z + H^z| - |H^z|. \quad (34)$$

Далее, рассмотрим некоторые возможные значения $k(z)$ и оценим для этих значений $|A + A_z|$.

Пусть для некоторого z выполнено $k(z) = 1$, т.е. $H^z = H$. Тогда по неравенству (34) получаем $|A + A_z| \geq |H^z| = |H|$, и тогда $A + A_z = H$.

Далее, для таких z , что $k(z) = 2$, выполнено $|A + H^z| \geq 2|H^z|$, поскольку

$$|A| > \frac{5}{8}|H| = \frac{5}{4}|H^z| > |H^z|$$

и A не принадлежит никакому одному смежному классу по H^z , т.е. $A + H^z$ равно объединению по крайней мере двух смежных классов по H^z и, значит, $|A + H^z| \geq 2|H^z|$. Но тогда $|A + A_z| \geq 2|H^z| = |H|$ и снова $A + A_z = H$.

Пусть для некоторого z выполнено $k(z) = 3$. Тогда

$$|A| > \frac{5}{8}|H| = \frac{15}{8}|H^z|$$

и A не лежит ни в каком одном смежном классе по H^z , т.е. $|A + H^z| \geq 2|H^z|$. В этом случае

$$|A + A_z| \geq 2|H^z| = \frac{2}{3}|H|, \quad (35)$$

причем равенство возможно только если A_z лежит ровно в одном смежном классе по H^z , а A – ровно в двух, так как должно быть выполнено $|A_z + H^z| = |H^z|$ и $|A + H^z| = 2|H^z|$. Вообще, $|A + A_z|$ может принимать только значения $(2/3)|H|$ или $|H|$. В случае равенства в (35) имеем для некоторого $x \in H$ вложение $A \subseteq H^z \sqcup (H^z + x)$. Обозначим

$$A_1 = A \cap H^z, \quad A_2 = A \cap (H^z + x).$$

Тогда

$$|A_1| = |A| - |A_2| \geq |A| - |H^z| > \left(\frac{15}{8} - 1\right)|H^z| = \frac{7}{8}|H^z|.$$

Действуя точно так же, как и в предыдущей лемме 4, получаем

$$|A^2 + \Delta(A)| = 7|H^z|^2 \geq \frac{7}{4}|A|^2,$$

что противоречит условию леммы. Получаем, что в условиях леммы случай $k(z) = 3$ и равенство в (35) невозможны одновременно, т.е. при $k(z) = 3$ имеем $|A + A_z| = |H|$.

Далее, если $k(z) = 4$, то

$$|A| > \frac{5}{2}|H^z| > 2|H^z|$$

и A не лежит в объединении никаких двух смежных классов по $|H^z|$. При этом $|A_z| > (1/4)|H| = |H^z|$ и A_z не лежит ни в каком смежном классе по H^z . Тогда

$$|A + A_z| \geq |H| \quad \text{и} \quad A + A_z = H.$$

При $k(z) = 5$ получаем

$$|A| > \frac{25}{8}|H^z| > 3|H^z|$$

и A не лежит в объединении никаких трех смежных классов по $|H^z|$. Кроме того, $|A_z| > (1/4)|H| > |H^z|$ и A_z не лежит ни в каком одном смежном классе по H^z . Значит, $|A + A_z| \geq |H|$ и, следовательно,

$$A + A_z = H.$$

При $k(z) = 6$ имеем

$$|A| > \frac{15}{4}|H| > 3|H^z| \quad \text{и} \quad |A_z| > \frac{1}{4}|H| > |H^z|,$$

т.е. $|A + H^z| \geq 4|H^z|$ и $|A_z + H^z| \geq 2|H^z|$. Тогда

$$|A + A_z| \geq \frac{5}{6}|H|.$$

При $k(z) = 7$ выполнено

$$|A| > \frac{35}{8} > 4|H^z| \quad \text{и} \quad |A_z| > \frac{1}{4}|H| = \frac{7}{4}|H^z| > |H^z|;$$

значит,

$$|A + A_z| \geq \frac{6}{7}|H|.$$

При $k(z) = 8$ получаем

$$|A| > 5|H^z|, \quad |A_z| > 2|H^z|$$

и, следовательно,

$$|A + A_z| \geq |H| \quad \text{и} \quad A + A_z = H.$$

При $k(z) = 9$ имеем

$$|A| > 5|H^z|, \quad |A_z| > 2|H^z|$$

и, следовательно,

$$|A + A_z| \geq \frac{8}{9}|H|.$$

При $k(z) = 10$ выполнено

$$|A| > 6|H^z|, \quad |A_z| > 2|H^z|$$

и, следовательно,

$$|A + A_z| > \frac{9}{10}|H| = \frac{4}{5}|H|.$$

Для z таких, что $k(z) \geq 11$, выполнено

$$|A + A_z| \geq |A| + |A_z| - \frac{|H|}{k(z)} > \left(\frac{5}{8} + \frac{1}{4} - \frac{1}{11}\right)|H| = \frac{69}{88}|H| > \frac{7}{9}|H|.$$

Из рассуждений выше следует, что для любого $z \in H$, какое бы значение не принимало $k(z)$, выполнено $|A + A_z| > (7/9)|H|$. Тогда

$$|A^2 + \Delta(A)| = \sum_{z \in H} |A + A_z| > \frac{7}{9}|H|^2. \quad (36)$$

По предположению (33) имеем $|H|^2 \geq (9/4)|A|^2$; значит,

$$|A^2 + \Delta(A)| > \frac{7}{9}|H|^2 \geq \frac{7}{4}|A|^2. \quad (37)$$

Получаем противоречие с условием леммы, а значит, допущение, что $(3/2)|A| \leq |H| < (8/5)|A|$, неверно, и тогда

$$|H| \geq \frac{8}{5}|A|. \quad (38)$$

Теперь рассмотрим случай

$$\frac{8}{5}|A| \leq |A + A| < \left(\frac{3}{2} + \frac{1}{6}\right)|A| = \frac{5}{3}|A|.$$

Отсюда следует, что

$$\frac{3}{5}|H| < |A| \leq \frac{5}{8}|H|. \quad (39)$$

Как и ранее, будем оценивать мощность множества $A + A_z$, исходя из значения $k(z)$. Для любого $z \in H = A - A$ выполнено

$$|A_z| = |A| + |A - z| - |A \cup (A - z)| \geq 2|A| - |H| > \frac{1}{5}|H|.$$

Пусть для некоторого z выполнено $k(z) = 1$, т.е. $H^z = H$. Тогда по неравенству (34) получаем $|A + A_z| \geq |H^z| = |H|$, и тогда $A + A_z = H$.

Далее, для таких z , что $k(z) = 2$, выполнено $|A + H^z| \geq 2|H^z|$, так как $|A| > (3/5)|H| = (6/5)|H^z| > |H^z|$ и A не лежит ни в каком одном смежном классе по H^z . Но тогда $|A + A_z| \geq 2|H^z| = |H|$ и снова $A + A_z = H$.

Пусть для некоторого z $k(z) = 3$. Тогда $|A| > (3/5)|H| = (9/5)|H^z|$ и A не лежит ни в каком одном смежном классе по H^z , т.е. $|A + H^z| \geq 2|H^z|$. В этом случае

$$|A + A_z| \geq 2|H^z| = \frac{2}{3}|H|,$$

причем равенство возможно только если A_z лежит ровно в одном смежном классе по H^z , а A ровно в двух, так как должно быть выполнено $|A_z + H^z| = |H^z|$ и $|A + H^z| = 2|H^z|$. В случае равенства, как и ранее, получаем противоречие с тем, что по условию $|A^2 + \Delta(A)| < (7/4)|A|^2$.

Далее, если $k(z) = 4$, то $|A| > (12/5)|H^z| > 2|H^z|$ и A не лежит в объединении никаких двух смежных классов по H^z . Тогда

$$|A + A_z| \geq \frac{3}{4}|H|.$$

При $k(z) = 5$ получаем $|A| > (15/5)|H^z| = 3|H^z|$ и A не лежит в объединении никаких трех смежных классов по H^z . Кроме того, $|A_z| > (1/5)|H| = |H^z|$ и A_z не лежит ни в каком одном смежном классе по H^z . Значит,

$$|A + A_z| \geq |H| \quad \text{и} \quad A + A_z = H.$$

При $k(z) = 6$ имеем

$$|A| > \frac{18}{5}|H| > 3|H^z| \quad \text{и} \quad |A_z| > \frac{1}{5}|H| > |H^z|,$$

т.е. $|A + H^z| \geq 4|H^z|$ и $|A_z + H^z| \geq 2|H^z|$. Тогда

$$|A + A_z| \geq \frac{5}{6}|H|.$$

При $k(z) = 7$ выполнено

$$|A| > \frac{21}{5} > 4|H^z| \quad \text{и} \quad |A_z| > \frac{1}{5}|H| = \frac{7}{5}|H^z| > |H^z|;$$

значит,

$$|A + A_z| \geq \frac{6}{7}|H|.$$

При $k(z) = 8$ получаем $|A| > 4|H^z|$, $|A_z| > |H^z|$ и

$$|A + A_z| \geq \frac{6}{8}|H| = \frac{3}{4}|H|.$$

При $k(z) = 9$ имеем $|A| > 5|H^z|$, $|A_z| > |H^z|$ и

$$|A + A_z| \geq \frac{7}{9}|H|.$$

При $k(z) = 10$ выполнено $|A| > 6|H^z|$, $|A_z| > 2|H^z|$ и

$$|A + A_z| > \frac{9}{10}|H| > \frac{4}{5}|H|.$$

Для z таких, что $k(z) > 10$, выполнено

$$|A + A_z| \geq |A| + |A_z| - \frac{|H|}{k(z)} > \left(\frac{3}{5} + \frac{1}{5} - \frac{1}{10}\right)|H| = \frac{7}{10}|H|.$$

Заметим, что в рассматриваемом случае для всех $z \in H$ выполнено $|A + A_z| > 0.7|H|$. Тогда

$$|A^2 + \Delta(A)| = \sum_{z \in H} |A + A_z| > 0.7|H|^2 \quad (40)$$

и, учитывая неравенство $|H| \geq (8/5)|A|$, получаем

$$|A^2 + \Delta(A)| > 0.7 \cdot \frac{64}{25}|A|^2 > \frac{7}{4}|A|^2. \quad (41)$$

Противоречие с условием леммы, а значит, неверно предположение (39), и тогда

$$|H| \geq \frac{5}{3}|A|.$$

Рассмотрим оставшийся случай. Имеем

$$\frac{4}{7}|H| < |A| \leq \frac{3}{5}|H|, \quad |A_z| = |A| + |A - z| - |A \cup (A - z)| \geq 2|A| - |H| > \frac{1}{7}|H|.$$

Предположим, что для всех $z \in H$ выполнено

$$|A + A_z| > |A| + |A_z| - \frac{|H|}{k_0} \quad \text{для некоторого } k_0 \in \mathbb{N}. \quad (42)$$

Тогда

$$|A^2 + \Delta(A)| > |H||A| + \sum_{z \in H} |A_z| - \sum_{z \in H} \frac{|H|}{k_0} = |A||H| + |A|^2 - \frac{|H|^2}{k_0}.$$

В последнем выражении выразим $|H|$ через $|A|$ для его оценки снизу. Предположим, что $|H| = \alpha|A|$. Тогда

$$|A||H| + |A|^2 - \frac{|H|^2}{k_0} = \left(-\frac{\alpha^2}{k_0} + \alpha + 1\right)|A|^2, \quad (43)$$

т.е. имеет место квадратичная зависимость по α . Ветви этой параболы направлены вниз, поэтому наименьшее значение при условии $\alpha \in [5/3; 7/4]$ выражение (43) может принимать только на концах отрезка. Если $\alpha = 5/3$, то

$$\left(-\frac{\alpha^2}{k_0} + \alpha + 1\right)|A|^2 = \left(-\frac{25}{9k_0} + \frac{5}{3} + 1\right)|A|^2 = \left(\frac{8}{3} - \frac{25}{9k_0}\right)|A|^2. \quad (44)$$

Если $\alpha = 7/4$, то

$$\left(-\frac{\alpha^2}{k_0} + \alpha + 1\right)|A|^2 = \left(-\frac{49}{16k_0} + \frac{7}{4} + 1\right)|A|^2 = \left(\frac{11}{4} - \frac{49}{16k_0}\right)|A|^2. \quad (45)$$

Предположим, что оба полученных значения в (44) и (45) не меньше, чем $(7/4)|A|^2$. Для этого необходимо в случае (44) выполнение оценки

$$\frac{25}{9k_0} \leq \frac{11}{12}, \quad k_0 \geq 4,$$

и в случае (45) – оценки

$$\frac{49}{16k_0} \leq 1, \quad k_0 \geq 4.$$

То есть при выборе параметра $k_0 = 4$ и выполненном предположении (42) получаем $|A^2 + \Delta(A)| \geq (7/4)|A|^2$, что противоречит условию леммы. И в этом случае лемма доказана. Итак, выберем $k_0 = 4$.

Покажем, что для данного k_0 предположение (42) верно. По теореме Кнезера для всех z выполнено

$$|A + A_z| \geq |A + H^z| + |A_z + H^z| - |H^z| \geq |A| + |A_z| - |H^z|.$$

Тогда при $k(z) \geq 4$ предположение доказано. Пусть $k(z) = 1$; тогда $H^z = H$ и можно написать оценку

$$|A + A_z| \geq |A + H^z| + |A_z + H^z| - |H^z| \geq |H^z| + |H^z| - |H^z| = |H^z| = |H|$$

и предположение окажется верным, если $|A| + |A_z| - |H|/4 \leq |H|$. Так как $|A_z| \leq |A|$, то

$$|A| + |A_z| - \frac{|H|}{4} \leq \frac{3}{5}|H| + \frac{3}{5}|H| - \frac{|H|}{4} = \frac{19}{20}|H| < |H|.$$

Пусть теперь $k(z) = 2$, $|H^z| = |H|/2$. Так как $|A| > (7/4)|H| > |H^z|$, то A не может лежать ни в каком одном смежном классе по H^z и

$$|A + A_z| \geq |A + H^z| + |A_z + H^z| - |H^z| \geq 2|H^z| + |H^z| - |H^z| = 2|H^z| = |H|,$$

т.е. предположение верно и для этого случая.

Далее, пусть $k(z) = 3$. Тогда

$$|A + A_z| \geq |A + H^z| + |A_z + H^z| - |H^z| \geq 2|H_z| + |H^z| - |H_z| = 2|H^z| = \frac{2}{3}|H|,$$

причем $|A + A_z|$ принимает значение $(2/3)|H|$ или $|H|$. Докажем, что $|A + A_z|$ не может принимать значение $(2/3)|H|$. Пусть $|A + A_z| = (2/3)|H|$, это возможно только

в том случае, если A лежит ровно в двух смежных классах по H^z . Тогда для некоторого $x \in H$ выполнено

$$A \subseteq H^z \sqcup (H^z + x) \quad \text{и} \quad H = A + A = H^z \sqcup (H^z + x) \sqcup (H^z + 2x).$$

Обозначим

$$A_1 = A \cap H^z, \quad A_2 = A \cap (H^z + x).$$

Тогда из $|A_1| + |A_2| = |A|$ следует, что для $i = 1, 2$ выполнено

$$|A_i| \geq |A| - |H^z| > \frac{4}{7}|H| - |H^z| = \left(\frac{12}{7} - 1\right)|H^z| = \frac{5}{7}|H^z| > \frac{1}{2}|H^z|.$$

Получаем, что для $i, j = 1, 2$ имеет место $|A_i| + |A_j| > |H^z|$, откуда $|A_i + A_j| = |H^z|$.
Можем посчитать

$$\begin{aligned} A^2 + \Delta(A) &= ((A_1, A_1) \sqcup (A_1, A_2) \sqcup (A_2, A_1) \sqcup (A_2, A_2)) + ((A_1, A_1) \sqcup (A_2, A_2)) \\ &\subseteq [(H^z, H^z) \sqcup (H^z, H^z + x) \sqcup (H^z + x, H^z) \sqcup (H^z + x, H^z + x)] \\ &\quad \cup [(H^z + x, H^z + x) \sqcup (H^z + x, H^z + 2x) \sqcup (H^z + 2x, H^z + x) \\ &\quad \sqcup (H^z + 2x, H^z + 2x)] = (H^z, H^z) \sqcup (H^z, H^z + x) \\ &\quad \sqcup (H^z + x, H^z) \sqcup (H^z + x, H^z + x) \sqcup (H^z + x, H^z + 2x) \\ &\quad \sqcup (H^z + 2x, H^z + x) \sqcup (H^z + 2x, H^z + 2x), \end{aligned} \quad (46)$$

причем вместо включения в выражении выше можно написать равенство; доказательство этого факта аналогично изложенным в леммах 4 и 5. Отсюда следует, что

$$|A^2 + \Delta(A)| = 7|H^z|^2.$$

Так как $A \subseteq H^z \sqcup (H^z + x)$, то $|A| \leq 2|H^z|$; значит,

$$|A^2 + \Delta(A)| = 7|H^z|^2 \geq \frac{7}{4}|A|^2,$$

получаем противоречие с условием. Таким образом, предположение (42) верно и лемма 7 доказана.

Автор выражает благодарность С. В. Конягину за ряд ценных замечаний и полезные обсуждения.

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

- [1] T. Tao, V. H. Vu, *Additive Combinatorics*, Cambridge Stud. Adv. Math., **105**, Cambridge Univ. Press, Cambridge, 2010.
- [2] M. B. Nathanson, *Additive Number Theory. Inverse Problems and Geometry of Sumsets*, Grad. Texts in Math., **165**, Springer, New York, 1996.
- [3] B. Green, I. Z. Ruzsa, “Sets with small sumset and rectification”, *Bull. London Math. Soc.*, **38**:1 (2006), 43–52.
- [4] T. Sanders, “Additive structures in sumsets”, *Math. Proc. Camb. Philos. Soc.*, **144**:2 (2008), 289–316.
- [5] И. Д. Шкредов, “О множествах с малым удвоением”, *Матем. заметки*, **84**:6 (2008), 927–947.

- [6] Д. А. Москвин, Г. А. Фрейман, А. А. Юдин, “Структурная теория сложения множеств и локальные предельные теоремы для независимых решетчатых случайных величин”, *ТВП*, **19**:1 (1974), 52–62.
- [7] T. Schoen, I. D. Shkredov, “Higher moments of convolutions”, *J. Number Theory*, **133**:5 (2013), 1693–1737.
- [8] M. Kneser, “Abschätzung der asymptotischen Dichte von Summenmengen”, *Math. Z.*, **58** (1953), 459–484.
- [9] T. Sanders, *An Analytic Approach to a Weak Non-Abelian Kneser-Type Theorem*, [arXiv: 1212.0457](#).
- [10] И. В. Вьюгин, И. Д. Шкредов, “Об аддитивных сдвигах мультипликативных подгрупп”, *Матем. сб.*, **203**:6 (2012), 81–100.

А. А. Увакин

Московский государственный университет

имени М.В.Ломоносова

E-mail: artemuvakin@gmail.com

Поступило

18.09.2014

Исправленный вариант

31.03.2015