Math-Net.Ru

Общероссийский математический портал

И. Д. Шкредов, Несколько замечаний к теореме о разложимости Балога–Вули и величинах D^+ , $D^\times$, *Совр. пробл. матем.*, 2017, выпуск 24, 85–103

DOI: <https://doi.org/10.4213/spm71>

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: 34.227.88.159

26 апреля 2023 г., 15:05:18

Несколько замечаний к теореме о разложимости Балога–Вули и величинах D^+ , $D^\times$

И. Д. Шкредов

Математический институт им. В. А. Стеклова Российской академии наук
ilya.shkredov@gmail.com

1. Введение

Пусть $A, B \subset \mathbb{R}$ – конечные множества. Определим *сумму*, *произведение* и *частное* множеств A и B как

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

и

$$\frac{A}{B} := \left\{ \frac{a}{b} : a \in A, b \in B, b \neq 0 \right\}$$

соответственно. Гипотеза Эрдеша–Семереди [1] гласит, что для любого $\epsilon > 0$ выполнено

$$\max\{|A + A|, |AA|\} \gg |A|^{2-\epsilon}.$$

Грубо говоря, утверждается, что произвольное множество действительных (или целых) чисел не может одновременно иметь хорошую аддитивную и мультипликативную структуру. Современные оценки по данной гипотезе содержатся в [2]–[4].

Определим через

$$E^+(A, B) := |\{(a, a', b, b') \in A^2 \times B^2 : a + b = a' + b'\}|$$

и

$$E^\times(A, B) := |\{(a, a', b, b') \in A^2 \times B^2 : ab = a'b'\}|$$

аддитивную и мультипликативную общую энергию множеств A и B , соответственно. Числа $E^+(A, A)$, $E^\times(A, A)$ суть иные показатели для измерения аддитивной и мультипликативной структуры множества, нежели мощность множества сумм или произведений.

В [5] была доказана следующая теорема.

ТЕОРЕМА 1. Пусть $A \subset \mathbb{R}$ – конечное множество и $\delta = 2/33$. Тогда найдутся два непересекающиеся множества B и C такие, что $A = B \sqcup C$ и

$$\max\{E^+(B, B), E^\times(C, C)\} \ll |A|^{3-\delta} (\log |A|)^{1-\delta}, \quad (1.1)$$

а также

$$\max\{E^+(B, C), E^\times(B, C)\} \ll |A|^{3-\delta/2} (\log |A|)^{(1-\delta)/2}. \quad (1.2)$$

Здесь и ниже мы полагаем, что $|A| \geq 2$. Все логарифмы берутся по основанию 2. Знаки $\ll$ и $\gg$ суть обычные символы Виноградова, а именно $a \ll b$ тогда и только тогда, когда

$a = O(b)$. Будем писать $a \lesssim b$ или $b \gtrsim a$, когда $a = O(b \cdot \log^c |A|)$, $c > 0$. Если $a \lesssim b$ и $b \lesssim a$, то мы используем обозначение $a \sim b$.

Результаты, подобные теореме 1, достаточно полезны (см., например, работу [6]) и, по мнению автора, найдут в будущем и другие приложения. Также в [5] было доказано, что число δ нельзя взять большим, чем $2/3$.

В работе [4] был использован иной метод, который позволил получить такой результат.

ТЕОРЕМА 2. Пусть $A \subset \mathbb{R}$ – конечное множество и $\delta = 1/5$. Тогда найдутся два непересекающихся множества B и C такие, что $A = B \sqcup C$ и

$$\max\{E^+(B, B), E^\times(C, C)\} \lesssim |A|^{3-\delta}.$$

На самом деле имеет место еще более сильное утверждение. Будем писать

$$E_3^+(A) = |\{(a_1, a'_1, a_2, a'_2, a_3, a'_3) \in A^6 : a_1 - a'_1 = a_2 - a'_2 = a_3 - a'_3\}|$$

и, аналогично, $E_3^\times(A)$. Используя тот факт, что величины $(E_3^+(f))^{1/6}, (E_3^\times(f))^{1/6}$ являются нормами вещественнозначной функции f (см. более точную формулировку в разделе 4), мы получаем

ТЕОРЕМА 3. Пусть $A \subset \mathbb{R}$ – конечное множество и $\delta_1 = 2/5$. Тогда найдутся два непересекающихся множества B и C такие, что $A = B \sqcup C$ и

$$\max\{E_3^+(B), E_3^\times(C)\} \lesssim |A|^{4-\delta_1}, \quad (1.3)$$

Кроме того, неравенство (1.3) не может выполняться с $\delta_1 > 3/4$.

Применяя неравенство Гёльдера

$$(E^+(A, A))^2 \leq E_3^+(A)|A|^2, \quad (E^\times(A, A))^2 \leq E_3^\times(A)|A|^2,$$

легко видеть, что теорема 3 влечет теорему 2.

Оказывается, что наше доказательство позволяет сказать о множествах B, C гораздо больше, чем это содержится в теореме 3. Мы рассматриваем две величины $D^+, D^\times$ (см. определения в разделе 3) и доказываем самый сильный результат о разложимости.

ТЕОРЕМА 4. Пусть $A \subset \mathbb{R}$ – конечное множество и $\delta_2 = 2/5$. Тогда найдутся два непересекающихся множества B и C такие, что $A = B \sqcup C$ и

$$\max\{D^+(B), D^\times(C)\} \lesssim |A|^{1-\delta_2}. \quad (1.4)$$

Кроме того, неравенство (1.4) не может выполняться с $\delta_2 > 3/4$.

Легко проверить, что теорема 4 влечет обе теоремы 2, 3 (см. обсуждение в разделе 5). Величины $D^+, D^\times$ играют важную роль в аддитивной комбинаторике (см., например, [3], [4], [7]). Отметим, что именно изучение этих характеристик множеств позволило усилить знаменитый $4/3$ результат Шоймоши (см. [2]).

Также в разделе 5 мы получаем несколько других форм теоремы Балога–Вули, изучаем величины $D^+(A), D^\times(A)$ и находим ряд новых приложений к вопросам теории сумм произведений (см., например, теорему 23 ниже).

Автор планирует получить аналогичные результаты в своей будущей статье и для поля $\mathbb{F}_p$.

2. Обозначения

Пусть $\mathbf{G}$ – абелева группа с групповой операцией $+$. Если группа $\mathbf{G}$ конечна, то обозначим через N мощность $\mathbf{G}$. Хорошо известно [8], что в этом случае двойственная группа $\widehat{\mathbf{G}}$ изоморфна группе $\mathbf{G}$. Пусть f – произвольная функция из $\mathbf{G}$ в $\mathbb{C}$. Преобразование Фурье функции f обозначается $\widehat{f}$ и определяется формулой

$$\widehat{f}(\xi) = \sum_{x \in \mathbf{G}} f(x) e(-\xi \cdot x), \quad (2.1)$$

где $e(x) = e^{2\pi i x}$, а ξ – любой гомоморфизм из $\widehat{\mathbf{G}}$ в $\mathbb{R}/\mathbb{Z}$, $\xi: x \rightarrow \xi \cdot x$. Мы будем использовать несколько основных формул

$$\sum_{x \in \mathbf{G}} |f(x)|^2 = \frac{1}{N} \sum_{\xi \in \widehat{\mathbf{G}}} |\widehat{f}(\xi)|^2, \quad (2.2)$$

$$\sum_{y \in \mathbf{G}} \left| \sum_{x \in \mathbf{G}} f(x) g(y - x) \right|^2 = \frac{1}{N} \sum_{\xi \in \widehat{\mathbf{G}}} |\widehat{f}(\xi)|^2 |\widehat{g}(\xi)|^2 \quad (2.3)$$

и

$$f(x) = \frac{1}{N} \sum_{\xi \in \widehat{\mathbf{G}}} \widehat{f}(\xi) e(\xi \cdot x). \quad (2.4)$$

Если

$$(f * g)(x) := \sum_{y \in \mathbf{G}} f(y) g(x - y) \quad \text{и} \quad (f \circ g)(x) := \sum_{y \in \mathbf{G}} f(y) g(y + x), \quad (2.5)$$

то

$$\widehat{f * g} = \widehat{f} \widehat{g} \quad \text{и} \quad \widehat{f \circ g} = \widehat{f}^c \widehat{g} = \overline{\widehat{f}} \widehat{g}, \quad (2.6)$$

где для функции $f: \mathbf{G} \rightarrow \mathbb{C}$ мы положили $f^c(x) := f(-x)$. Очевидно, что $(f * g)(x) = (g * f)(x)$ и $(f \circ g)(x) = (g \circ f)(-x)$, $x \in \mathbf{G}$; k -я свертка, $k \in \mathbb{N}$, обозначается как $*_k$ и задается индуктивным образом $*_k := (*_{k-1})$.

Если $S \subseteq \mathbf{G}$ – некоторое множество, то будем писать $S(x)$ для его характеристической функции $S: \mathbf{G} \rightarrow \{0, 1\}$. Через $|S|$ обозначим мощность S . Для натурального n пишем $[n] = \{1, \dots, n\}$.

Число $E^+(A, B)$ называется *совместной аддитивной энергией* двух множеств $A, B \subseteq \mathbf{G}$ (см., например, [9]) и равно

$$E^+(A, B) = |\{(a_1, a_2, b_1, b_2) \in A^2 \times B^2 : a_1 + b_1 = a_2 + b_2\}|.$$

Если $A = B$, то вместо $E^+(A, A)$ мы пишем для краткости $E^+(A)$. Очевидно, что

$$E^+(A, B) = \sum_x (A * B)(x)^2 = \sum_x (A \circ B)(x)^2 = \sum_x (A \circ A)(x) (B \circ B)(x).$$

Отметим также простую оценку

$$E^+(A, B) \leq \min\{|A|^2|B|, |B|^2|A|, |A|^{3/2}|B|^{3/2}\}. \quad (2.7)$$

Далее, по неравенству Коши–Буняковского

$$E^+(A, B) \geq \frac{|A|^2|B|^2}{|A \pm B|}. \quad (2.8)$$

Если мы рассматриваем группу $\mathbf{G} = (\mathbf{G}, \times)$, то тогда мы пишем $E^\times(A, B)$ вместо $E^+(A, B)$. Таким образом,

$$E^\times(A, B) = |\{(a_1, a_2, b_1, b_2) \in A^2 \times B^2 : a_1 b_1 = a_2 b_2\}|.$$

Последняя величина называется *совместной мультипликативной энергией* двух множеств $A, B \subseteq \mathbf{G} = (\mathbf{G}, +)$. Очевидным образом, мультипликативная энергия $E^\times(A, B)$ может быть выражена через мультипликативные свертки, аналогичные задаваемым формулой (2.5). Пусть также

$$\sigma_k(A) := (A *_k A)(0) = |\{(a_1, \dots, a_k) \in A^k : a_1 + \dots + a_k = 0\}|.$$

Более общо, положим

$$E_k(A) = \sum_{x \in \mathbf{G}} (A \circ A)(x)^k = \sum_{x \in \mathbf{G}} |A_x|^k = |\{(a_1, a'_1, \dots, a_k, a'_k) \in A^k : a_1 - a'_1 = \dots = a_k - a'_k\}| \quad (2.9)$$

и

$$E_k(A, B) = \sum_{x \in \mathbf{G}} (A \circ B)^k(x) = |\{(a_1, \dots, a_k) \in A^k, (b_1, \dots, b_k) \in B^k : a_1 - b_1 = \dots = a_k - b_k\}|. \quad (2.10)$$

Величины выше суть *старшие энергии* множеств A и B (см. [10]). Здесь $A_x = A \cap (A - x)$, $x \in A - A$. Подобным образом, мы пишем $E_k(f, g) = \sum_x (\bar{f} \circ g)^k(x)$ для любых двух комплексных функций f, g и даже более общо, рассматриваем

$$E_k(f_1, \dots, f_k) = \sum_x (\bar{f}_1 \circ f_1)(x) \cdots (\bar{f}_k \circ f_k)(x).$$

Существует простая связь между энергиями E_k и E_2 . В самом деле,

$$E_{k+1}(A) = E(\Delta_k(A), A^k), \quad (2.11)$$

где

$$\Delta(A) = \Delta_k(A) := \{(a, a, \dots, a) \in A^k\}.$$

Равенство (2.11) позволяет нам использовать нижнюю оценку (2.8) для оценки старших энергий E_k^+ , $E_k^\times$. В частности,

$$|A|^6 \leq E_3^+(A) |A^2 \pm \Delta(A)| \quad (2.12)$$

и аналогичным образом для $E_3^\times$.

Величины $E_k(A, B)$ могут быть записаны в терминах старших свертков. Пусть $f_1, \dots, f_{k+1} : \mathbf{G} \rightarrow \mathbb{C}$ – произвольные функции, и пусть $F = (f_1, \dots, f_{k+1}) : \mathbf{G} \rightarrow \mathbb{C}^{k+1}$. Обозначим через

$$\mathcal{C}_{k+1}(F)(x) = \mathcal{C}_{k+1}(f_1, \dots, f_{k+1})(x_1, \dots, x_k)$$

функцию

$$\mathcal{C}_{k+1}(F)(x) = \mathcal{C}_{k+1}(f_1, \dots, f_{k+1})(x_1, \dots, x_k) = \sum_z f_1(z) f_2(z + x_1) \cdots f_{k+1}(z + x_k).$$

Таким образом,

$$\mathcal{C}_2(f_1, f_2)(x) = (f_1 \circ f_2)(x).$$

Если $f_1 = \dots = f_{k+1} = f$, то мы пишем $\mathcal{C}_{k+1}(f)(x_1, \dots, x_k)$ для $\mathcal{C}_{k+1}(f, \dots, f)(x_1, \dots, x_k)$.

По лемме 5 ниже имеем

$$E_{k+1}(A, B) = \sum_{x_1, \dots, x_k} \mathcal{C}_{k+1}(A)(x_1, \dots, x_k) \mathcal{C}_{k+1}(B)(x_1, \dots, x_k).$$

3. Предварительные результаты

Мы начнем с леммы из [11] о “коммутативности” обобщенных сверток.

ЛЕММА 5. Для произвольных функций $f_i, g_j: \mathbf{G} \rightarrow \mathbb{C}$ выполнено

$$\begin{aligned} \sum_{x_1, \dots, x_{l-1}} C_l(f_0, \dots, f_{l-1})(x_1, \dots, x_{l-1}) C_l(g_0, \dots, g_{l-1})(x_1, \dots, x_{l-1}) \\ = \sum_z (f_0 \circ g_0)(z) \cdots (f_{l-1} \circ g_{l-1})(z) \quad (\text{скалярное произведение}), \end{aligned} \quad (3.1)$$

более того,

$$\begin{aligned} \sum_{x_1, \dots, x_{l-1}} C_l(f_0)(x_1, \dots, x_{l-1}) \cdots C_l(f_{k-1})(x_1, \dots, x_{l-1}) \\ = \sum_{y_1, \dots, y_{k-1}} C_k^l(f_0, \dots, f_{k-1})(y_1, \dots, y_{k-1}) \quad (\text{мультиסקалярное произведение}) \end{aligned} \quad (3.2)$$

и

$$\begin{aligned} \sum_{x_1, \dots, x_{l-1}} C_l(f_0)(x_1, \dots, x_{l-1}) (C_l(f_1) \circ \cdots \circ C_l(f_{k-1}))(x_1, \dots, x_{l-1}) \\ = \sum_z (f_0 \circ \cdots \circ f_{k-1})^l(z) \quad (\sigma_k \text{ для } C_l). \end{aligned} \quad (3.3)$$

Следующая лемма показывает, что “старшие суммы” могут быть выражены в терминах обычных сумм (см., например, [10]).

ЛЕММА 6. Пусть $A \subseteq \mathbf{G}$ – произвольное множество. Тогда

$$|A^2 \pm \Delta(A)| = \sum_{x \in A-A} |A \pm A_x|. \quad (3.4)$$

Основные величины, которые изучаются в настоящей статье – это $D^+(A)$, $D^\times(A)$. Напомним их определения.

ОПРЕДЕЛЕНИЕ 7. Конечное множество $A \subset \mathbb{R}$ имеет *аддитивный Семереди–Гроттесковский тип* (кратко СТ-тип) с параметром $D^+ = D^+(A) > 0$, если неравенство

$$|\{s \in A - B \mid |A \cap (B + s)| \geq \tau\}| \leq \frac{D^+ |A| |B|^2}{\tau^3} \quad (3.5)$$

справедливо для любого конечного множества $B \subset \mathbb{R}$ и произвольного действительного числа $\tau \geq 1$.

Величину $D(A)$ можно понимать как инфимум чисел D , для которых неравенство (3.5) имеет место для любых множеств B и чисел $\tau \geq 1$. Разумеется, определение 7 наиболее эффективно только для множеств A с малым значением $D^+(A)$. Легко видеть, что $D^+(A) \leq |A|$, таким образом, мощность A может рассматриваться как тривиальная верхняя оценка для величины $D^+(A)$. Заметим также, что $D^+(A) \geq 1$ (нужно просто взять в качестве B любое одноэлементное множество, что даст $\tau = 1$ в формуле (3.5)).

Любое множество СТ-типа обладает тем свойством, что у него можно оценить число решений для широкого класса линейных уравнений (см., например, следствие 8 из [3]), где, тем не менее, использовалась другая величина $D(A)$, и леммы 7, 8 из [7].

ЛЕММА 8. Пусть $A_1, A_2 \subset \mathbb{R}$ – произвольные конечные множества. Тогда

$$E^+(A_1, A_2) \ll (D^+(A_1))^{1/2} |A_1| |A_2|^{3/2}$$

и

$$E_3^+(A_1, A_2) \ll D^+(A_1) |A_1| |A_2|^2 \cdot \log(\min\{|A_1|, |A_2|\}).$$

Подобным образом рассмотрим “двойственную” характеристику множества действительных чисел.

ОПРЕДЕЛЕНИЕ 9. Конечное множество $A \subset \mathbb{R}$ имеет мультипликативный Семерди–Троттеровский тип с параметром $D^\times = D^\times(A) > 0$, если неравенство

$$|\{s \in A/B \mid |A \cap sB| \geq \tau\}| \leq \frac{D^\times |A| |B|^2}{\tau^3} \quad (3.6)$$

справедливо для любого конечного множества $B \subset \mathbb{R}$ и произвольного действительного числа $\tau \geq 1$.

Конечно справедлив и мультипликативный аналог леммы 8.

ЛЕММА 10. Пусть $A_1, A_2 \subset \mathbb{R}$ – произвольные конечные множества. Тогда

$$E^\times(A_1, A_2) \ll (D^\times(A_1))^{1/2} |A_1| |A_2|^{3/2},$$

и

$$E_3^\times(A_1, A_2) \ll D^\times(A_1) |A_1| |A_2|^2 \cdot \log(\min\{|A_1|, |A_2|\}).$$

4. Нормы E_k

Для произвольной функции $f: \mathbf{G} \rightarrow \mathbb{C}$ и любого целого $k \geq 1$ положим

$$\|f\|_{E_k} := (E_k(f))^{1/2k} = \left(\sum_x (\bar{f} \circ f)(x)^k \right)^{1/2k}. \quad (4.1)$$

По формуле (2.6) получаем

$$\|f\|_{E_k}^{2k} = N^{-(k-1)} \sum_{x_1 + \dots + x_k = 0} |\hat{f}(x_1)|^2 \dots |\hat{f}(x_k)|^2, \quad (4.2)$$

и, значит, выражение выше неотрицательно. Другой взгляд на величину $\|f\|_{E_k}$ дает нам формула (3.1) леммы 5, по которой мы имеем

$$\|f\|_{E_k}^{2k} = \sum_{x_1, \dots, x_{k-1}} |\mathcal{C}_k(f)(x_1, \dots, x_{k-1})|^2. \quad (4.3)$$

Заметим, что существуют ненулевые функции f с $\|f\|_{E_k} = 0$. Пусть, например, $\mathbf{G} = \mathbb{F}_p$, p – простое число, $k < p$ и $f(x) = e^{2\pi i x/p}$. Если мы ограничимся только рассмотрением вещественных функций, то все равно возможно найти ненулевые функции f , для которых $\|f\|_{E_k} = 0$.

ПРИМЕР 11. Пусть $\mathbf{G} = \mathbb{F}_2^n$ и $f(x) = f(x_1, \dots, x_n) = (-1)^{x_1 + \dots + x_n}$. Тогда $\hat{f}(r) = 0$ для всех $r \neq (1, \dots, 1)$. Таким образом, по формуле (4.2) мы имеем $\|f\|_{E_k} = 0$ для всех нечетных k .

Если $k \geq 2$ четное, то последняя ситуация уже невозможна.

ЛЕММА 12. Пусть $f: \mathbf{G} \rightarrow \mathbb{R}$ – произвольная функция и $k \geq 2$ – четное число. Тогда $\|f\|_{E_k} = 0$ тогда и только тогда, когда $f \equiv 0$.

ДОКАЗАТЕЛЬСТВО. Мы приведем даже три доказательства. Первое из них использует анализ Фурье, а два другие – нет. Применяя формулу (4.2), мы видим, что

$$|\widehat{f}(x_1)|^2 \cdots |\widehat{f}(x_k)|^2 = 0 \quad (4.4)$$

для всех $x_1, \dots, x_k \in \mathbf{G}$ таких, что $x_1 + \cdots + x_k = 0$. По нашему предположению функция f вещественная, таким образом $\widehat{f}(-x) = \overline{\widehat{f}(x)}$. Используя этот факт и подставляя переменные

$$x_1 = x, \quad x_2 = -x, \quad x_3 = x, \quad x_4 = -x, \quad \dots, \quad x_{k-1} = x, \quad x_k = x$$

в формулу (4.4), мы получаем $|\widehat{f}(x)|^{2k} = 0$ для всех x и, значит, $f \equiv 0$.

В нашем втором доказательстве мы используем тождество (4.3) и замечаем, что

$$C_k(f)(x_1, \dots, x_{k-1}) = \sum_z f(z)f(z+x_1) \cdots f(z+x_{k-1}) = 0$$

для всех $x_1, \dots, x_{k-1} \in \mathbf{G}$. Полагая $x_1 = \cdots = x_{k-1} = 0$ на основе предположения о том, что k четное, а также о том, что функция f вещественная, мы получаем $\sum_z f^k(x) = \sum_z |f(z)|^k = 0$, откуда вытекает, что $f \equiv 0$.

Наконец, используя условия доказываемой леммы, из определения (4.1) легко видеть, что $\|f\|_{E_k} \geq \|f\|_2$ (надо просто подставить $x = 0$ в (4.1)). Лемма доказана.

ЛЕММА 13. Для любого $k \geq 1$ и произвольных функций $f_1, f'_1, \dots, f_k, f'_k: \mathbf{G} \rightarrow \mathbb{C}$ имеем

$$\left| \sum_x (f_1 \circ f'_1)(x) \cdots (f_k \circ f'_k)(x) \right| \leq \prod_{j=1}^k \|f_j\|_{E_k} \|f'_j\|_{E_k}. \quad (4.5)$$

Если $k \geq 2$ четное и все функции выше вещественные, то можно убрать модули из формулы (4.5).

ДОКАЗАТЕЛЬСТВО. По формуле (3.1) леммы 5, имеем

$$\begin{aligned} \sigma &:= \sum_x (f_1 \circ f'_1)(x) \cdots (f_k \circ f'_k)(x) \\ &= \sum_{x_1, \dots, x_k} C_{k+1}(f_1, \dots, f_k)(x_1, \dots, x_k) C_{k+1}(f'_1, \dots, f'_k)(x_1, \dots, x_k). \end{aligned}$$

Применяя неравенство Коши–Буняковского и формулу (3.1) леммы 5 еще раз, получаем

$$\begin{aligned} |\sigma|^2 &\leq \sum_{x_1, \dots, x_k} |C_{k+1}(f_1, \dots, f_k)(x_1, \dots, x_k)|^2 \cdot \sum_{x_1, \dots, x_k} |C_{k+1}(f'_1, \dots, f'_k)(x_1, \dots, x_k)|^2 \\ &= \sum_x (\overline{f_1} \circ f_1)(x) \cdots (\overline{f_k} \circ f_k)(x) \cdot \sum_x (\overline{f'_1} \circ f'_1)(x) \cdots (\overline{f'_k} \circ f'_k)(x). \end{aligned}$$

По неравенству Гёльдера достаточно доказать, что для любой функции $f: \mathbf{G} \rightarrow \mathbb{C}$ выполнено

$$|\sigma| = \sum_x |(\overline{f} \circ f)(x)|^k \leq \sum_x (|f| \circ |f|)(x)^k = \| |f| \|_{E_k}^{2k}.$$

Если k четное и f – действительная функция, то мы должны проверить, что

$$\sigma = \sum_x (f \circ f)(x)^k = \|f\|_{E_k}^{2k},$$

но это просто определение нормы E_k . Лемма доказана.

ПРИМЕР 14. Пусть $\mathbf{G} = \mathbb{F}_2^n$,

$$f_1(x) = f_{\vec{\lambda}'}(x) = f_1(x_1, \dots, x_n) = (-1)^{\lambda_1 x_1 + \dots + \lambda_n x_n}, \quad \vec{\lambda}' = (\lambda_1, \dots, \lambda_n),$$

и, аналогично, $f_2(x) = f_{\vec{\lambda}''}(x)$, $f_3(x) = f_{\vec{\lambda}''' }(x)$. Возьмем три ненулевые вектора $\vec{\lambda}'$, $\vec{\lambda}''$, $\vec{\lambda}'''$ такие, что $\vec{\lambda}' + \vec{\lambda}'' + \vec{\lambda}''' = 0$. Тогда простые вычисления дают нам

$$\sum_x (f_1 \circ f_1)(x)(f_2 \circ f_2)(x)(f_3 \circ f_3)(x) = 2^{4n},$$

но, с другой стороны, для всех $j = 1, 2, 3$ имеем $\sum_x (f_j \circ f_j)^3(x) = 0$. Таким образом, (4.5) не выполнена без $|\cdot|$ в случае нечетного k и вещественных функций f_j .

Нам понадобится комбинаторная лемма. Пусть l – положительное целое, и пусть $\Omega_l = \{0, 1\}^l$. Для любого $\varepsilon \in \Omega_l$ пусть $\text{wt}(\varepsilon)$ равно числу единиц в ε . Наконец, если $k_1, \dots, k_s$ – произвольные целые неотрицательные такие, что $k_1 + \dots + k_s = k$, то будем писать $\binom{k}{k_1, \dots, k_s}$ для $k!/(k_1! \dots k_s!)$.

ЛЕММА 15. Пусть n, k, l – положительные числа, $n \leq lk$. Тогда

$$\sum_{\varepsilon \in \Omega_l} n_\varepsilon = k, \quad \sum_{\varepsilon \in \Omega_l} \text{wt}(\varepsilon) n_\varepsilon = n \quad \frac{k!}{\prod_{\varepsilon \in \Omega_l} n_\varepsilon!} = \frac{(lk)!}{n! (lk - n)!}. \quad (4.6)$$

В частности,

$$\sum_{n_1 + n_2 + n_3 + n_4 = k, \quad 2n_1 + n_2 + n_3 = n} \frac{k!}{n_1! n_2! n_3! n_4!} = \frac{(2k)!}{n! (2k - n)!}. \quad (4.7)$$

ДОКАЗАТЕЛЬСТВО. Имеем

$$\begin{aligned} \sum_n \binom{lk}{n} x^n &= (1+x)^{lk} = \left(\sum_{i=0}^l \binom{l}{i} x^i \right)^k \\ &= \sum_{m_0 + m_1 + \dots + m_l = k} x^{\sum_{j=1}^l j m_j} \binom{k}{m_0, m_1, \dots, m_l} \prod_{r=0}^l \binom{l}{r}^{m_r}. \end{aligned}$$

Отсюда

$$\begin{aligned} \binom{lk}{n} &= \sum_{m_0 + m_1 + \dots + m_l = k, \quad \sum_{j=1}^l j m_j = n} \binom{k}{m_0, m_1, \dots, m_l} \prod_{r=0}^l \binom{l}{r}^{m_r} \\ &= \sum_{m_0 + m_1 + \dots + m_l = k, \quad \sum_{j=1}^l j m_j = n} \binom{k}{m_0, m_1, \dots, m_l} \prod_{r=0}^l \sum_{s_1 + \dots + s_{\binom{l}{r}} = m_r} \binom{m_r}{s_1, \dots, s_{\binom{l}{r}}}. \end{aligned}$$

Зафиксируем $r \in 0, \dots, l$ и обозначим $s_{\binom{l}{r}}$ переменных $s_{\binom{l}{r}}$ через n_ε , где $\varepsilon \in \Omega_l$ выбираются так, что $\text{wt}(\varepsilon) = r$. Таким образом, мы переобозначили все 2^l переменных $s_{\binom{l}{r}}$, $r = 0, \dots, l$, переменными n_ε , $\varepsilon \in \Omega_l$. Заметим, что $\sum_{\varepsilon \in \Omega_l} n_\varepsilon = m_0 + m_1 + \dots + m_l = k$. Далее, из нашего способа перенумеровки n_ε мы имеем $\sum_{\varepsilon \in \Omega_l} \text{wt}(\varepsilon) n_\varepsilon = \sum_{j=1}^l j m_j = n$. Таким образом, получаем

$$\binom{lk}{n} = \sum_{\varepsilon \in \Omega_l} n_\varepsilon = k, \quad \sum_{\varepsilon \in \Omega_l} \text{wt}(\varepsilon) n_\varepsilon = n \quad \frac{k!}{\prod_{\varepsilon \in \Omega_l} n_\varepsilon!},$$

что и требовалось.

Используя леммы выше, мы готовы доказать основной результат этого раздела.

ПРЕДЛОЖЕНИЕ 16. Пусть $k \geq 2$ – целое число. Тогда для любой пары функций $f, g: \mathbf{G} \rightarrow \mathbb{C}$ выполнено

$$\|f + g\|_{E_k} \leq \|f\|_{E_k} + \|g\|_{E_k}.$$

Если мы рассматриваем только вещественные функции и если число k четное, то $\|\cdot\|_{E_k}$ задает норму.

ДОКАЗАТЕЛЬСТВО. Имеем

$$\begin{aligned} \sigma &:= \|f + g\|_{E_k}^{2k} = \sum_x ((\bar{f} \circ f)(x) + (\bar{f} \circ g)(x) + (\bar{g} \circ f)(x) + (\bar{g} \circ g)(x))^k \\ &= \sum_{n_1+n_2+n_3+n_4=k} \binom{k}{n_1, n_2, n_3, n_4} \sum_x (\bar{f} \circ f)^{n_1}(x) (\bar{f} \circ g)^{n_2}(x) (\bar{g} \circ f)^{n_3}(x) (\bar{g} \circ g)^{n_4}(x). \end{aligned}$$

Применяя лемму 13, а также лемму 15 в случае $l = 2$, получаем

$$\begin{aligned} \sigma &\leq \sum_{n_1+n_2+n_3+n_4=k} \binom{k}{n_1, n_2, n_3, n_4} \|f\|_{E_k}^{2n_1+n_2+n_3} \|g\|_{E_k}^{n_2+n_3+2n_4} \\ &= \sum_{n+m=2k} \frac{(2k)!}{n!m!} \|f\|_{E_k}^n \|g\|_{E_k}^m = (\|f\|_{E_k} + \|g\|_{E_k})^{2k}, \end{aligned}$$

как и требовалось.

Если f, g – вещественные функции и число k четное, то, используя вторую часть леммы 13, получаем $\|f + g\|_{E_k} \leq \|f\|_{E_k} + \|g\|_{E_k}$. Кроме того, лемма 12 говорит нам, что в этом случае $\|f\|_{E_k} = 0$ тогда и только тогда, когда $f \equiv 0$. Предложение доказано.

5. Доказательство теоремы 4

В следующих двух разделах будут доказаны теоремы 3, 4. Мы начнем с более сильной теоремы 4, а затем воспользуемся аналогичными аргументами, соединенными с результатами раздела 4, и докажем теорему 3.

Прежде всего выразим величины $D^+(A)$, $D^\times(A)$ в терминах энергий $E_3^+(A, B)$, $E_3^\times(A, B)$. Достаточно рассмотреть случай $D^+(A)$, поскольку второй вариант аналогичен. Для конечно-го множества $A \subset \mathbb{R}$ положим

$$q^+(A) := \max_{B \neq \emptyset} \frac{E_3^+(A, B)}{|A||B|^2}. \quad (5.1)$$

Легко видеть, что максимум в (5.1) достигается. В самом деле, используя сдвиг, мы можем считать, что $0 \in B$; далее, размер B ограничен в терминах $|A|$, и лемма 5 дает нам

$$E_3^+(A, B) = \sum_{(x,y) \in A^2 - \Delta(A)} C_3(B)(x, y) C_3(A)(x, y). \quad (5.2)$$

Следовательно, мы видим по индукции, что $B \subseteq k(A - A)$, где k ограничено в терминах $|A|$. Таким образом, максимум в (5.1) действительно достигается.

Приведем несколько простых оценок для величины $q^+(A)$. Ввиду (2.7), (2.9) мы, очевидно, имеем

$$1 \leq \frac{E_3^+(A)}{|A|^3} \leq q^+(A) \leq |A|. \quad (5.3)$$

Более того, по формулам (2.7), (5.2) и неравенству Коши–Буняковского получаем

$$q^+(A) \leq \frac{(\mathbb{E}_3^+(A))^{1/2}}{|A|} \leq |A|. \quad (5.4)$$

Теперь мы готовы показать, что величины $D^+(A)$ и $q^+(A)$ пропорциональны с точностью до логарифмов.

ЛЕММА 17. Пусть $A \subset \mathbb{R}$ – конечное множество. Тогда

$$q^+(A) \lesssim D^+(A) \leq q^+(A). \quad (5.5)$$

ДОКАЗАТЕЛЬСТВО. Нижняя оценка в (5.5) немедленно вытекает из леммы 8. Предположим теперь, что для некоторого $B \subset \mathbb{R}$ и $\tau \geq 1$ выполнено $D^+(A)|A||B|^2 = \tau^3|S_\tau(A, B)|$, где

$$S_\tau(A, B) := \{s \in A - B : |A \cap (B + s)| \geq \tau\}.$$

Тогда

$$\mathbb{E}_3^+(A, B) = \sum_s (A \circ B)^3(s) \geq \sum_{s \in S_\tau(A, B)} (A \circ B)^3(s) \geq \tau^3|S_\tau(A, B)| = |A||B|^2 D^+(A).$$

Из последней формулы вытекает, что $q^+(A) \geq D^+(A)$. Лемма доказана.

Лемма выше, соединенная с леммами 8, 10 и неравенством (5.4), влечет, что между соответствующими величинами $D^+(A)$, $D^\times(A)$ и $\mathbb{E}_3^+(A)$, $\mathbb{E}_3^\times(A)$ имеется тесная связь.

СЛЕДСТВИЕ 18. Пусть $A \subset \mathbb{R}$ – конечное множество. Тогда

$$|A|^2(D^+(A))^2 \leq \mathbb{E}_3^+(A) \lesssim D^+(A)|A|^3.$$

То же самое справедливо для $D^\times(A)$.

Теперь мы отметим, что, величины D^+ , $D^\times$ обладают некоторым свойством “субаддитивности”. На самом деле наши результаты справедливы для любых абелевых групп $\mathbf{G}$.

ЛЕММА 19. Пусть $A_1, \dots, A_k \subset \mathbb{R}$ – конечные множества. Тогда

$$D(A_1 \cup \dots \cup A_k) \lesssim k^3 \cdot \frac{1}{|A|} \sum_{j=1}^k D(A_j)|A_j|,$$

где $D = D^+$ или $D^\times$.

ДОКАЗАТЕЛЬСТВО. Рассмотрим случай величины $D^\times$; ситуация с D^+ аналогичная. Мы приведем даже два доказательства. Положим $A = A_1 \cup \dots \cup A_k$. Рассмотрим произвольное множество $G \subset \mathbb{R}$ и действительное число $\tau \geq 1$. Мы должны оценить сверху размер множества

$$S_\tau = S_\tau(A, G) := \{s \in A/G : |A \cap sG| \geq \tau\}.$$

Для любого $s \in S_\tau$ имеем

$$\tau \leq |A \cap sG| \leq \sum_{j=1}^k |A_j \cap sG| \lesssim \sum_{j \in \Omega_\Delta(s)} |A_j \cap sG| \leq 2\Delta(s)|\Omega_\Delta(s)|, \quad (5.6)$$

где через $\Delta(s)$ мы обозначили некоторое число вида 2^j , $j \geq 0$, для которого

$$\Omega_\Delta(s) = \{j : \Delta(s) < |A_j \cap sG| \leq 2\Delta(s)\} \subseteq [k]$$

и $\tau k^{-1} \lesssim \Delta(s)$. Существование числа $\Delta(s)$ и множества $\Omega_\Delta(s)$ вытекает из принципа Дирихле. Используя принцип Дирихле еще раз, мы находим множество $S'_\tau \subseteq S_\tau$ такое, что $|S'_\tau| \gtrsim |S_\tau|$, и, далее, число Δ со свойством

$$\Omega_\Delta(s) = \{j : \Delta < |A_j \cap sG| \leq 2\Delta\} \subseteq [k]$$

и

$$\tau k^{-1} \lesssim \Delta \quad (5.7)$$

и такое, что для любого $s \in S'_\tau$ справедлив аналог (5.6), а именно

$$\tau \leq |A \cap sG| \lesssim \Delta |\Omega_\Delta(s)|.$$

По нашему построению имеем $S'_\tau \subseteq \bigcup_{j=1}^k S_\Delta(A_j, G)$. Ввиду (5.7) получаем

$$\begin{aligned} |S_\tau| &\lesssim |S'_\tau| \leq \sum_{j=1}^k |S_\Delta(A_j, G)| \leq \frac{|G|^2}{\Delta^3} \sum_{j=1}^k D(A_j) |A_j| \lesssim \frac{|G|^2 k^3}{\tau^3} \sum_{j=1}^k D(A_j) |A_j| \\ &= \frac{|G|^2 |A| k^3}{\tau^3} \cdot \frac{1}{|A|} \sum_{j=1}^k D(A_j) |A_j|. \end{aligned}$$

По определению это означает, что

$$D(A) \lesssim \frac{k^3}{|A|} \sum_{j=1}^k D(A_j) |A_j|.$$

Теперь мы приведем другое доказательство, которое будет использовать величину q . Прменяя неравенство Гёльдера и леммы 8, 10, имеем

$$\begin{aligned} E_3\left(\bigcup_{i=1}^k A_i, B\right) &\leq \sum_x \left(\sum_{i=1}^k A_i \circ B\right)^3(x) = \sum_x \left(\sum_{i=1}^k (A_i \circ B)(x)\right)^3 \\ &= \sum_{i_1, i_2, i_3=1}^k \sum_x (A_{i_1} \circ B)(x) (A_{i_2} \circ B)(x) (A_{i_3} \circ B)(x) \\ &\leq \left(\sum_{i=1}^k \left(\sum_x (A_i \circ B)^3(x)\right)^{1/3}\right)^3 \\ &\leq k^3 \sum_{i=1}^k \sum_x (A_i \circ B)^3(x) \lesssim k^3 |A| |B|^2 \cdot \frac{1}{|A|} \sum_{j=1}^k D(A_j) |A_j|. \end{aligned}$$

Таким образом, по лемме 17 получаем $D(A) \leq q(A) \lesssim \frac{k^3}{|A|} \sum_{j=1}^k D(A_j) |A_j|$, где q равно q^+ или $q^\times$ соответственно. Лемма доказана.

В [4] мы рассматривали две другие характеристики множеств A . Положим

$$\text{Sym}_t^\times(Q, R) = \{x : |Q \cap xR^{-1}| \geq t\}$$

и

$$d^+(A) = \min_{t>0} \min_{\emptyset \neq Q, R \subset \mathbb{R} \setminus \{0\}} \frac{|Q|^2 |R|^2}{|A| t^3}, \quad (5.8)$$

где второй минимум в (5.8) берется по произвольным Q, R таким, что $A \subseteq \text{Sym}_t^\times(Q, R)$ и $\max\{|Q|, |R|\} \geq |A|$.

Подобным образом для произвольных множеств Q, R и действительного числа $t > 0$ положим

$$\text{Sym}_t^+(Q, R) := \{x : |Q \cap (x - R)| \geq t\}$$

и рассмотрим величину

$$d^\times(A) := \min_{t>0} \min_{\emptyset \neq Q, R \subset \mathbb{R} \setminus \{0\}} \frac{|Q|^2 |R|^2}{|A| t^3}, \quad (5.9)$$

где второй минимум в (5.9) берется по произвольным Q, R таким, что $A \subseteq \text{Sym}_t^+(Q, R)$ и $\max\{|Q|, |R|\} \geq |A|$. Легко видеть [4], что $1 \leq d^+(A), d^\times(A) \leq |A|$. В [4] был доказан такой результат.

ЛЕММА 20. Пусть $A \subset \mathbb{R}$ – конечное множество. Тогда A имеет аддитивный Семереди–Троттеровский тип с $O(d^+(A))$ и A имеет мультипликативный Семереди–Троттеровский тип с $O(d^\times(A))$.

Теперь мы можем сформулировать наш новый результат, который влечет теорему 2 с параметром $\delta = 1/5$, если соединить теорему 21 ниже с леммами 8, 10.

ТЕОРЕМА 21. Пусть $A \subset \mathbb{R}$ – конечное множество и $\delta = 2/5$. Тогда найдутся два непесекающиеся множества B и C такие, что $A = B \sqcup C$ и

$$\max\{D^+(B), D^\times(C)\} \lesssim |A|^{1-\delta}.$$

ДОКАЗАТЕЛЬСТВО. Пусть $1 \leq M \leq |A|$ – некоторый параметр, который мы выберем позже. Наше доказательство представляют собой алгоритм. В процессе работы этого алгоритма будет построена убывающая последовательность множеств

$$C_1 = A \supseteq C_2 \supseteq \dots \supseteq C_k,$$

а также возрастающая последовательность множеств

$$B_0 = \emptyset \subseteq B_1 \subseteq \dots \subseteq B_{k-1} \subseteq A$$

таких, что для любого $j = 1, 2, \dots, k$ множества C_j и B_{j-1} не пересекаются и, более того, $A = C_j \sqcup B_{j-1}$. Если на некотором шаге j алгоритма выполнено $D^\times(C_j) \leq |A|/M$, то мы останавливаем его работу, полагая $C = C_j$, $B = B_{j-1}$ и $k = j - 1$. В противном случае, мы имеем $D^\times(C_j) > |A|/M$. Положим $C' = C_j$. По определению найдутся число $\tau \geq 1$ и конечное множество $G = G_j \subset \mathbb{R}$ такие, что множество

$$S_\tau = S_\tau(G_j, C') := \{s \in C' / G : |C' \cap sG| \geq \tau\}$$

имеет размер не меньше чем $|C'|^2 |G|^2 / (M\tau^3)$. Тогда

$$\tau |S_\tau| \leq \sum_{s \in S_\tau} |C' \cap sG| = \sum_{a \in C'} |S_\tau \cap aG^{-1}|.$$

По принципу Дирихле существуют множество $A' \subseteq C'$ и число q такие, что $|A'|q \sim \tau |S_\tau|$ и $q < |S_\tau \cap aG^{-1}| \leq 2q$ для любого $a \in A'$. Другими словами, $A' \subseteq \text{Sym}_q^\times(S_\tau, G)$. Применяя лемму 20 с $P = S_\tau$, $Q = G$, находим

$$D^+(A') \ll d^+(A') \leq \frac{|S_\tau|^2 |G|^2}{q^3 |A'|}. \quad (5.10)$$

Далее, мы знаем, что $|A'|q \sim \tau|S_\tau|$ и $|S_\tau| > |C'|^2|G|^2/(M\tau^3)$. Соединяя эти неравенства с оценкой (5.10), получаем

$$D^+(A') \ll d^+(A') \lesssim \frac{|A'|^2|G|^2}{\tau^3|S_\tau|} < \frac{|A'|^2M}{|C'|^2}. \quad (5.11)$$

Так как $1 \leq d^+(A')$, то выполнено $|A'| \gtrsim |C'|M^{-1/2}$. Тривиальным образом $A' \subseteq C'$ и, значит, $D^+(A') \lesssim M$.

После этого мы полагаем $D_j = A'$, $C_{j+1} = C_j \setminus D_j$, $B_j = B_{j-1} \sqcup D_j$ и делаем следующий шаг алгоритма. Очевидно, что на шаге k мы имеем $B_k = \bigsqcup_{j=1}^k D_j$, и поскольку $|D_j| \gtrsim |C_j|M^{-1/2}$, то после некоторых вычислений получаем, что $k \lesssim M^{1/2}$. Таким образом, число шагов k конечно. Осталось оценить величину $D^+(B_k) = D^+(D_1 \cup \dots \cup D_k)$. Положим

$$U_j = \{i \in [k] : 2^{j-1} \leq D^+(D_i) \leq 2^j\}, \quad j \in [t], \quad k_j = |U_j|.$$

Поскольку для любого i выполнено $D^+(D_i) \lesssim M$, то число множеств U_j есть $t \lesssim 1$. Пусть также $B_k^{(j)} = \bigcup_{i \in U_j} D_i$. Применяя лемму 19, находим

$$D^+(B_k) \lesssim \frac{1}{|B_k|} \sum_{j=1}^t D^+(B_k^{(j)})|B_k^{(j)}|. \quad (5.12)$$

Фиксируя $j \in [t]$, мы видим, что $k_j \lesssim M^{1/2}2^{-j/2}$. Используя лемму 19 еще раз, получаем

$$D^+(B_k^{(j)}) \lesssim \frac{k_j^3}{|B_k^{(j)}|} \sum_{i \in U_j} D^+(D_i)|D_i| \lesssim M^{3/2}2^{-j/2} \frac{1}{|B_k^{(j)}|} \sum_{i \in U_j} |D_i| = M^{3/2}2^{-j/2}.$$

Подставляя полевную оценку в (5.12), имеем

$$D^+(B_k) \lesssim \frac{M^{3/2}}{|B_k|} \sum_{j=1}^t 2^{-j/2} |B_k^{(j)}| \ll M^{3/2}.$$

Выбирая значение параметра M оптимальным образом, т.е. полагая $M = |A|^{2/5}$, получаем требуемый результат. Теорема доказана.

Для доказательства нижних оценок в теоремах 3, 4 мы используем небольшую модификацию конструкции из [5]. Контрпример представляет собой так называемое $(H + \Lambda)$ -множество, см. [11].

ТЕОРЕМА 22. *Для любого положительного целого N найдется множество $A \subseteq \mathbb{N}$, $|A| = N$, такое, что для произвольного $B \subseteq A$ с $|B| \geq |A|/2$ выполнено $E_3^+(B), E_3^\times(B) \gg |A|^{13/4}$ и $D^+(B), D^\times(B) \gtrsim |A|^{1/4}$.*

ДОКАЗАТЕЛЬСТВО. Возьмем целочисленный параметр $1 \leq K \ll N$, точное значение которого будет выбрано позднее, $t = \lceil N/K \rceil$ и положим $G = \{2^i\}_{i=1}^K$, $P = \{3 = p_1 < p_2 < \dots < p_t\}$ суть t последовательных нечетных простых. Наконец, положим $A = PG$, $|A| = tK = N + \theta K$, где $|\theta| \leq 1$. Таким образом, переопределяя, если это необходимо, число N , можно считать, что $|A| = N$.

Рассмотрим произвольное $B \subseteq A$ такое, что $|B| \geq |A|/2$. Для любого $j \in [K]$ положим $B_j = B \cap (P \cdot 2^j)$. По теореме о плотности простых чисел и оценкам (2.8) или (2.12) находим

$$E_3^+(B_j) \geq \frac{|B_j|^6}{|P + P|^2} \gtrsim \frac{|B_j|^6}{|P|^2}.$$

Таким образом, применяя неравенство Коши–Буняковского, получаем

$$E_3^+(B) \geq \sum_{j=1}^K E_3^+(B_j) \gtrsim |P|^{-2} \sum_{j=1}^K |B_j|^6 \geq \frac{|B|^6}{|P|^2 K^5} \gg \frac{N^4}{K^3}. \quad (5.13)$$

Теперь вычислим величину $E_3^\times(B)$. По формуле (2.12) имеем

$$|A|^6 \ll |B|^6 \leq E_3^\times(B) |B^2 \cdot \Delta(B)| \leq E_3^\times(B) |A^2 \cdot \Delta(A)|, \quad (5.14)$$

и, таким образом, нам достаточно оценить размер множества $A^2 \cdot \Delta(A)$. Положим $A_x = A \cap xA$. Применяя формулу (3.4) леммы 6 в мультипликативной форме, находим

$$\begin{aligned} |A^2 \cdot \Delta(A)| &= \sum_{x \in A/A} |AA_x| = \sum_{x \in G/G} |AA_x| + \sum_{x \in (A/A) \setminus (G/G)} |AA_x| \\ &\leq |G/G| |GGP| + \sum_{x \in (A/A) \setminus (G/G)} |AA_x| \ll N^2 + \sigma. \end{aligned} \quad (5.15)$$

Докажем, что $\sigma \ll N^3/K$. Возьмем $x \in (A/A) \setminus (G/G)$. Другими словами, $x = g_1/g_2 \cdot p_1/p_2$ и $p_1 \neq p_2$. Теперь берем $a \in A_x$ и получаем

$$a = p'g' = \frac{g_1 p_1 p'' g''}{g_2 p_2},$$

или, что эквивалентно,

$$p'p_2 \cdot g'g_2 = p''p_1 \cdot g''g_1,$$

где $p', p'' \in P$, $g', g'' \in G$. Таким образом $p' = p_1$, $p'' = p_2$ и $g'g_2 = g''g_1$. Значит, $A_x = p_1 g_1 g_2^{-1} \cdot G$ и $|AA_x| \leq |GGP| \leq 2N$. Отсюда

$$\sigma \leq 2|A/A|N \ll N|G/G \cdot P/P| \ll N^3/K.$$

Возвращаясь к (5.14), (5.15) и вспоминая, что $K \ll N$, находим

$$N^6 \ll E_3^\times(B) \cdot \frac{N^3}{K}.$$

Ввиду (5.13) оптимальный выбор K есть $K \sim N^{1/4}$.

Наконец, неравенства $D^+(B), D^\times(B) \gtrsim |A|^{1/4}$ немедленно вытекают из полученных ниже оценок для $E_3^+(B), E_3^\times(B)$, формулы (5.3) и леммы 17. Теорема доказана.

Объединяя теорему 22 с теоремой 21, мы получаем теорему 4, а также теорему 3. Легко видеть, что неравенство (1.1), соединенное с неравенством Коши–Буняковского, влечет оценку (1.2) теоремы 1, и, следовательно, при таком подходе теряется величина $\delta/2$. Наш метод позволяет избежать таких потерь.

6. Другое доказательство теоремы 3 и дальнейшие замечания

В [4] было показано, что $d^+(A), d^\times(A)$ ограничены сверху величинами

$$d_*^+(A) := \min_{B \neq \emptyset} \frac{|AB|^2}{|A||B|} \quad \text{и} \quad d_*^\times(A) := \min_{B \neq \emptyset} \frac{|A+B|^2}{|A||B|}$$

соответственно (см. также [12]). Существует результат о суммах произведений, включающий величины $d_*^+(A), d_*^\times(A)$, но не суммы или произведения множеств (которые, тем не менее, спрятаны в определениях $d_*^+(A), d_*^\times(A)$).

ТЕОРЕМА 23. Пусть $A \subset \mathbb{R}$ – конечное множество. Тогда

$$|A| \lesssim d_*^+(A) \cdot d_*^\times(A). \quad (6.1)$$

ДОКАЗАТЕЛЬСТВО. Применяя лемму 20, лемму 17 и неравенство Гёльдера, мы получаем для любого непустого конечного множества $B \subset \mathbb{R}$, что

$$\frac{|A|^2|B|}{|A+B|^2} \leq \frac{E_3^+(A, -B)}{|A||B|^2} \leq q^+(A) \lesssim D^+(A) \ll d^+(A) \leq d_*^+(A).$$

Другими словами, для произвольного множества B выполнено

$$|A| \lesssim d_*^+(A) \cdot \frac{|A+B|^2}{|A||B|},$$

что и требовалось.

Конечно, оценка (6.1) оптимальна с точностью до логарифмов. На самом деле, в процессе доказательства теоремы 23 было установлено, что $|A| \lesssim D^+(A) \cdot d_*^\times(A)$ и $|A| \lesssim D^\times(A) \cdot d_*^+(A)$. Приведем другие нижние оценки для величин d_*^+ , $d_*^\times$.

ЗАМЕЧАНИЕ 24. Пусть $d := d_*^\times = |A+B|^2/(|A||B|)$. Прежде всего, заметим, что тривиальное неравенство $|A+B| \geq |A|$ влечет, что $|B| \geq |A|/d$. Далее, по неравенству Плоннеке–Ружи (см., например, [9] для всех целых $n, m \geq 1$) имеем

$$|nA - mA| \leq \frac{|A+B|^{n+m}}{|B|^{n+m-1}} \leq d^{n+m-1}|A|.$$

В частности,

$$\frac{|A-A|}{|A|} \leq d_*^\times(A) \leq \frac{|A \pm A|^2}{|A|^2}$$

и

$$\frac{|A+A-A|}{|A|} \leq d_*^\times(A)^2 \leq \frac{|A \pm A|^4}{|A|^4}.$$

Таким образом, величина $d_*^\times(A)$ тесно связана с суммами. Например, $d_*^\times(A) = O(1)$ тогда и только тогда, когда $|A \pm A| = O(|A|)$. Подобная эквивалентность выполняется и для $d_*^+(A)$.

Теорема 21, соединенная с леммами 8, 10, дает нам аналог теоремы 2 (либо же можно повторить рассуждения из работы [4] напрямую; мы оставляем это упражнение заинтересованному читателю).

СЛЕДСТВИЕ 25. Пусть $A \subset \mathbb{R}$ – конечное множество и $\delta = 1/5$. Тогда найдутся два непересекающихся множества B и C такие, что $A = B \sqcup C$ и

$$\max\{E^+(A, B), E^\times(A, C)\} \lesssim |A|^{3-\delta}.$$

Разумеется, теорема 21 и леммы 8, 10 позволяют вычислять старшие энергии разбивающих A множеств B, C . Мы приводим схему более прямого доказательства для энергий $E_3^+, E_3^\times$, которое использует предложение 16.

ТЕОРЕМА 26. Пусть $A \subset \mathbb{R}$ – конечное множество и $\delta_1 = 2/5$. Тогда найдутся два непересекающихся множества B и C такие, что $A = B \sqcup C$ и

$$\max\{E_3^+(B), E_3^\times(C)\} \lesssim |A|^{4-\delta_1}.$$

СХЕМА ДОКАЗАТЕЛЬСТВА. Используя аргументы из доказательства теоремы 20 работы [4], мы находим множество $A_1 \subseteq A$ такое, что $|A_1| \gtrsim (E_3^\times(A))^{1/2}|A|^{-1}$ и

$$|A_1|^5|A|^2 \gtrsim E_3^\times(A)E_3^+(A_1)$$

(подобным образом справедлива и двойственная версия неравенства выше). После этого применяя обозначения и алгоритм доказательства следствия 21 из этой статьи или же следуя схеме доказательства теоремы 21, а также предложения 16, мы получаем

$$E_3^+(D_j) \lesssim M|A|^{-2}|D_j|^5,$$

где

$$|D_j| \gtrsim |A|M^{-1/2}, \quad (6.2)$$

и из неравенства Гёльдера имеем

$$\begin{aligned} (E_3^+(B_k))^{1/6} &= (E_3^+(D_1 \cup \dots \cup D_k))^{1/6} \leq \sum_{j=1}^k (E_3^+(D_j))^{1/6} \lesssim (M|A|^{-2})^{1/6} \sum_{j=1}^k |D_j|^{5/6} \\ &\leq (M|A|^{-2})^{1/6} |A|^{5/6} k^{1/6} \lesssim M^{1/4} |A|^{1/2}. \end{aligned}$$

Последнее использованное неравенство, а именно $k \lesssim M^{1/2}$, есть следствие (6.2). Значит,

$$E_3^+(B_k) \lesssim M^{3/2} |A|^3.$$

Выбирая значение параметра M оптимальным образом, т.е. полагая $M = |A|^{2/5}$, получаем требуемый результат.

Мы не рассматриваем случай еще более старших энергий (хотя предложение 16 и позволяет делать это), поскольку они не адекватны нашей ситуации. Дело в том, что теорема Семереди–Троттера естественным образом соответствует только энергиям $E_3^+(A)$, $E_3^\times(A)$.

В работе [13] автор рассмотрел несколько более общий контекст, чем обычно предполагает задача о суммах произведений. Данный подход, соединенный с аргументами из [4], позволяет, в частности, доказать вариант теоремы 2.

ТЕОРЕМА 27. Пусть $A \subset \mathbb{R}$ – конечное множество, $\alpha \neq 0$ – действительное число и $\delta = 1/5$. Тогда найдутся два непересекающихся множества B и C такие, что $A = B \sqcup C$ и

$$\max\{E^\times(B), E^\times(C + \alpha)\} \lesssim |A|^{3-\delta}.$$

Кроме того, существуют два непересекающихся множества B' и C' такие, что $A = B' \sqcup C'$ и

$$\max\{E^+(B'), E^+(\alpha/C')\} \lesssim |A|^{3-\delta}.$$

Конечно, можно доказать аналогичный результат и для энергий $E_3^+(B)$, $E_3^\times(C + \alpha)$, и для величин $D^+(B)$, $D^\times(C + \alpha)$, но мы оставляем это для заинтересованного читателя. Вместо этого выведем одно следствие результата выше.

СЛЕДСТВИЕ 28. Пусть $A \subset \mathbb{R}$ – конечное множество. Положим

$$R[A] = \left\{ \frac{a_1 - a}{a_2 - a} : a, a_1, a_2 \in A, a_2 \neq a \right\}.$$

Тогда найдутся два множества $R', R'' \subseteq R[A]$, $|R'|, |R''| \geq |R[A]|/2$ такие, что $E^\times(R') \lesssim |R'|^{3-1/5}$ и $E^+(R'') \lesssim |R''|^{3-1/5}$.

ДОКАЗАТЕЛЬСТВО. Прежде всего докажем существование множества R' . Положим $R = R[A]$, $R^* = R \setminus \{0\}$ и $\delta = 1/5$. Применяя теорему 27, находим $B, C \subseteq R$ такие, что $R = B \sqcup C$ и

$$\max\{E^\times(B), E^\times(C - 1)\} \lesssim |R|^{3-\delta}.$$

Если $|B| \geq |R|/2$, то все доказано. В противном случае $|C| \geq |R|/2$ и ввиду формулы $R = 1 - R$ (см. [13]), мы имеем $C' := 1 - C \subseteq R$, $|C'| = |C| \geq |R|/2$ и

$$E^\times(C') = E^\times(1 - C) = E^\times(C - 1) \lesssim |R|^{3-\delta}.$$

Таким образом, полагая R' равным B или C' , мы получаем требуемый результат.

Для того чтобы убедиться в существовании множества R'' , заметим, что $(R^*)^{-1} = R^*$. После этого воспользуемся второй частью теоремы 27, а также рассуждениями выше. Следствие доказано.

В частности, следствие 28 утверждает, что множество R имеет большую сумму $R + R$ и произведение RR (последнее известно из статьи [13] или же может быть получено прямым применением теоремы Семереди–Троттер).

То же самое доказательство позволяет найти подмножество A'_s множества

$$A_s \cup (A_{-s}) = A_s \cup (A_s - s), \quad A_s = A \cap (A + s), \quad s \in (A - A) \setminus \{0\},$$

имеющее мощность $|A_s|/2$, такое, что $E^\times(A'_s) \lesssim |A'_s|^{3-1/5}$ (подобным образом можно рассмотреть множество $A \cap (s - A)$ и найти в нем подмножество мощности $|A \cap (s - A)|/2$ с малой мультипликативной энергией). Этот вопрос двойственен тому, который поднимался в работах [3], [4]. Тот же самый результат имеет место и для мультипликативного аналога множеств A_s , а именно $A_s^* = A \cap (s/A)$, $s \in AA \setminus \{0\}$.

7. Добавление

Мы заканчиваем нашу статью обсуждением обобщения норм E_k . Поскольку наши рассуждения почти повторяют аргументы раздела 5, мы иногда приводим только схему доказательства.

Рассмотрим две числа $l \geq 2$, $k \geq 2$ и предположим, что либо k , либо l четное. В основном мы ограничимся рассмотрением вещественных функций. Для любой такой функции f положим

$$\|f\|_{E_{k,l}}^{kl} := \sum_{x_1, \dots, x_{k-1}} C_k^l(f)(x_1, \dots, x_{k-1}) = \sum_{y_1, \dots, y_{l-1}} C_l^k(f)(y_1, \dots, y_{l-1}) \geq 0. \quad (7.1)$$

При выводе второго равенства в последней формуле (7.1) мы воспользовались формулой (3.2) леммы 5. Для четных k и l имеем $\|f\|_{E_{k,l}} \geq \|f\|_l, \|f\|_k$, и, следовательно, в этом случае $\|f\|_{E_{k,l}} = 0$ тогда и только тогда, когда $f \equiv 0$.

Аналогично получаем аналог леммы 13.

ЛЕММА 29. Для любых $k, l \geq 2$ и произвольных функций $\varphi_1, \dots, \varphi_k: \mathbf{G} \rightarrow \mathbb{C}^l$, $\varphi_j = (\varphi_j^{(1)}, \dots, \varphi_j^{(l)})$, выполнено

$$\left| \sum_{x \in \mathbf{G}^{l-1}} C_l(\varphi_1)(x) \cdots C_l(\varphi_k)(x) \right| \leq \prod_{j=1}^k \prod_{i=1}^l \|\varphi_j^{(i)}\|_{E_{k,l}}. \quad (7.2)$$

Если $k, l \geq 2$ четные и все функции выше вещественные, то можно убрать модули из формулы (7.2).

ДОКАЗАТЕЛЬСТВО. Пусть $\varphi = (\varphi^{(1)}, \dots, \varphi^{(l)})$. По неравенству Гёльдера достаточно рассмотреть суммы

$$\sum_{x \in \mathbf{G}^{l-1}} \mathcal{C}_l^k(\varphi)(x) = \sum_{x \in \mathbf{G}^{k-1}} \mathcal{C}_k(\varphi^{(1)})(x) \cdots \mathcal{C}_k(\varphi^{(l)})(x),$$

где равенство выше вытекает из формулы (3.2) леммы 5. Применяя неравенство Гёльдера еще раз, мы получаем требуемый результат.

Аналог предложения 16 следующий.

ПРЕДЛОЖЕНИЕ 30. Пусть $k, l \geq 2$ – целые числа. Тогда для любой пары функций $f, g: \mathbf{G} \rightarrow \mathbb{C}$ выполнено

$$\|f + g\|_{E_{k,l}} \leq \|f\|_{E_{k,l}} + \|g\|_{E_{k,l}}.$$

Если мы рассматриваем только вещественные функции и если числа k, l четные, то $\|\cdot\|_{E_{k,l}}$ задает норму.

ДОКАЗАТЕЛЬСТВО. Напомним, что $\Omega_l := \{0, 1\}^l$. Имеем

$$\begin{aligned} \sigma := \|f + g\|_{E_{k,l}}^{kl} &= \sum_{x \in \mathbf{G}^{l-1}} \mathcal{C}_l^k(f + g)(x) = \sum_{x \in \mathbf{G}^{l-1}} \left(\sum_{\varepsilon \in \Omega_l} \mathcal{C}_l(\varphi_\varepsilon)(x) \right)^k \\ &= \sum_{\varepsilon \in \Omega_l} \sum_{n_\varepsilon = k} \binom{k}{n_1, \dots, n_{2^l}} \sum_{x \in \mathbf{G}^{l-1}} \prod_{\varepsilon \in \Omega_l} \mathcal{C}_l^{n_\varepsilon}(\varphi_\varepsilon)(x), \end{aligned}$$

где для $\varepsilon = (\varepsilon_1, \dots, \varepsilon_l) \in \Omega_l$ мы положили $\varphi_\varepsilon = (\varphi_{\varepsilon_1}, \dots, \varphi_{\varepsilon_l})$ и $\varphi_1 = f$, $\varphi_0 = g$. Пусть $n = (n_\varepsilon) \in \mathbb{N}_0^{2^l}$ и $q(n) := \sum_{\varepsilon \in \Omega_l} \text{wt}(\varepsilon) n_\varepsilon$. Применяя лемму 29 и лемму 15, получаем

$$\begin{aligned} \sigma &\leq \sum_{\varepsilon \in \Omega_l} \sum_{n_\varepsilon = k} \binom{k}{n_1, \dots, n_{2^l}} \|f\|_{E_{k,l}}^{q(n)} \|g\|_{E_{k,l}}^{kl-q(n)} \\ &= \sum_{i+j=kl} \frac{(kl)!}{i!j!} \|f\|_{E_{k,l}}^i \|g\|_{E_{k,l}}^j = (\|f\|_{E_{k,l}} + \|g\|_{E_{k,l}})^{kl}, \end{aligned}$$

что и требовалось.

Автор благодарен С. В. Конягину за плодотворные обсуждения.

Список литературы

- [1] P. Erdős, E. Szemerédi, “On sums and products of integers”, *Studies in Pure Mathematics*, Birkhäuser, Basel, 1983, 213–218.
- [2] J. Solymosi, “Bounding multiplicative energy by the sumset”, *Adv. Math.*, **222**:2 (2009), 402–408.
- [3] С. В. Конягин, И. Д. Шкредов, “О суммах множеств, имеющих малое произведение”, *Современные проблемы математики, механики и математической физики*, Тр. МИАН, **290**, МАИК, М., 2015, 304–316.
- [4] С. В. Конягин, И. Д. Шкредов, “Новые результаты о суммах и произведениях в $\mathbb{R}$ ”, *Современные проблемы математики, механики и математической физики. II*, Сборник статей, Тр. МИАН, **294**, МАИК, М., 2016, 87–98.
- [5] A. Balog, T. D. Wooley, *A Low-Energy Decomposition Theorem*, 2015, arXiv: [1510.03309](https://arxiv.org/abs/1510.03309).
- [6] B. Hanson, *Estimates for Character Sums with Various Convolutions*, 2015, arXiv: [1509.04354](https://arxiv.org/abs/1509.04354).

- [7] И. Д. Шкредов, “О суммах множеств Семереди–Троттера”, *Избранные вопросы математики и механики*, Тр. МИАН, **289**, МАИК, М., 2015, 318–327.
- [8] W. Rudin, *Fourier Analysis on Groups*, John Wiley & Sons, New York, 1990.
- [9] T. Tao, V. Vu, *Additive Combinatorics*, Cambridge Stud. Adv. Math., **105**, Cambridge Univ. Press, Cambridge, 2006.
- [10] T. Schoen, I. D. Shkredov, “Higher moments of convolutions”, *J. Number Theory*, **133**:5 (2013), 1693–1737.
- [11] I. D. Shkredov, “Energies and structure of additive sets”, *Electron. J. Combin.*, **21**:3 (2014), P3.44.
- [12] O. E. Raz, O. Roche-Newton, M. Sharir, *Sets with Few Distinct Distances Do Not Have Heavy Lines*, 2014, arXiv: [1410.1654](https://arxiv.org/abs/1410.1654).
- [13] I. D. Shkredov, “Difference sets are not multiplicatively closed”, *Discrete Anal.*, **17** (2016), 1–20.