О множествах с малым удвоением *

Шкредов И.Д.

Аннотация.

Пусть G — произвольная абелева группа и A — любое конечное подмножество G. Множество A называется множеством с малой суммой, если для некоторого числа K выполнено $|A+A| \leq K|A|$. Структурные свойства таких множеств изучались в работах Г.А. Фреймана, Ю. Билу, И. Ружи, М.Ч.–Чанг, Б. Грина и Т.Тао. В настоящей статье мы доказываем, что при некоторых ограничениях на K для любого множества с малой суммой найдется множество Λ, $\Lambda \ll_\varepsilon K\log|A|$ такое, что $|A \cap \operatorname{Span}\Lambda| \gg |A|/K^{1/2+\varepsilon}$, где $\varepsilon > 0$. В отличие от результатов предшествующих авторов наша теорема нетривиальна даже для достаточно больших K. Например, в качестве K можно взять $|A|^\eta$, где $\eta > 0$. Используемый нами метод доказательства совершенно элементарен.

1. Введение.

Пусть G — абелева группа и A, B — произвольные конечные подмножества G. Обозначим групповую операцию знаком $+$. Суммой (по Минковскому) множеств A и B называется множество $C = \{a+b \ : \ a \in A, b \in B\}$. Сумма множеств A и B обозначается $A+B$. Пусть $\log$ означает логарифм по основанию два.

В работах [4, 5, 6, 7, 9, 10, 13, 14, 15, 16] изучались множества A, обладающие тем свойством, что $|A+A| \leq K|A|$, где $K \geq 1$ — некоторое число, достаточно малое по сравнению с мощностью множества A (например, $K = \log\log|A|$ или $K = 2$). Такие множества называются *множествами с малой суммой*. Г.А. Фрейман (см. [4]) доказал замечательный результат о строении множеств с малой суммой.

Напомним, что множество $Q \subseteq G$ называется *d–мерной арифметической прогрессией*, если

$$Q = \{n_0 + n_1\lambda_1 + \cdots + n_d\lambda_d \ : \ 0 \leq \lambda_i < m_i\},$$

где m_i — натуральные, а n_i — целые числа.

Пусть $G = \mathbb{Z}$.

Теорема 1.1 (Фрейман) *Пусть $K \geq 1$ — некоторое действительное число и $A \subseteq \mathbb{Z}$ — произвольное конечное множество. Пусть также $|A+A| \leq K|A|$. Тогда найдутся числа $d = d(K)$ и $C = C(K)$, зависящие только от K и d–мерная арифметическая прогрессия Q такая, что $|Q| \leq C|A|$ и $A \subseteq Q$.*

Зависимость величин d и C от K изучалась в работах [6, 7]. Так, в статье [7] М.–Ч. Чанг показала, что $d = O(K^2\log^2 K)$ и $C = \exp(O(K^2\log^2 K))$ (мы, как обычно, пишем

*Работа выполнена при финансовой поддержке РФФИ N 06-01-00383, гранта Президента РФ N 1726.2006.1, гранта НШ-691.2008.1 и INTAS (грант N 03–51–5-70).

$X = O(Y)$ или $X \ll Y$, если найдется некоторая абсолютная константа M такая, что $X \le MY$).

Пусть n — натуральное число. Множества с малой суммой в группах $G = (\mathbb{Z}/2\mathbb{Z})^n$ изучались в работах [9, 17, 13, 14, 16]. Важность для комбинаторной теории чисел групп $(\mathbb{Z}/q\mathbb{Z})^n$, где q — простое, обсуждалась в обзоре [12]. Сформулируем, например, одну теорему из [9]. Заметим, что группа $(\mathbb{Z}/2\mathbb{Z})^n$ обладает естественной стурктурой векторного пространства.

Теорема 1.2 *Пусть $K \ge 1$ — действительное число. Пусть $A \subseteq (\mathbb{Z}/2\mathbb{Z})^n$ — некоторое множество такое, что $|A+A| \le K|A|$. Тогда множество A содержится в подпространстве H, причем $|H| \le K^2 2^{K^4}|A|$.*

В настоящее время в тематике, связанной с множествами с малой суммой, усилился интерес к результатам следующего типа. Пусть A — множество с малой суммой. Требуется доказать, что A сильно *пересекается* с некоторой многомерной арифметической прогрессией не очень большой размерности. Например, в работе [14] был получен следующий результат.

Теорема 1.3 *Пусть $K \ge 1$ — действительное число. Пусть $A \subseteq (\mathbb{Z}/2\mathbb{Z})^n$ — некоторое множество такое, что $|A+A| \le K|A|$. Тогда найдется подпространство H такое, что $|H| \ll K^{O(1)}|A|$ и $|A \cap H| \gg \exp(-K^{O(1)})|A|$.*

Наконец, в недавней работе [16] Б. Грин и Т. Тао доказали теорему.

Теорема 1.4 *Пусть $K \ge 1$ — действительное число. Пусть $A \subseteq (\mathbb{Z}/2\mathbb{Z})^n$ — некоторое множество такое, что $|A+A| \le K|A|$. Тогда найдется подпространство H и $x \in (\mathbb{Z}/2\mathbb{Z})^n$ такие, что $|H| \gg K^{-O(\sqrt{K})}|A|$ и $|A \cap (x+H)| \ge \frac{1}{2K}|H|$.*

Сформулируем наш основной результат.

Пусть $E = \{e_1, \dots, e_{|E|}\} \subseteq G$ — произвольное конечное множество. Обозначим через $\operatorname{Span} E$ множество $\operatorname{Span} E = \{ \sum_{i=1}^{|E|} \varepsilon_i e_i \ : \ \varepsilon_i \in \{-1, 0, 1\} \}$.

Теорема 1.5 *Пусть G — абелева группа. Пусть K, ε — действительные числа, $\varepsilon \in (0, 1/2]$, $A \subseteq G$ — произвольное конечное множество, $|A| \ge 2^{32/\varepsilon}$, $1 \le K \le \min\{ (2^{-58}\varepsilon^4 \frac{|A|}{\log|A|})^{(3/2+\varepsilon)^{-1}}, |A|^{\varepsilon} \}$. Пусть также число решений уравнения $a_1+a_2 = a_3+a_4$, где $a_i \in A$, $i = 1,2,3,4$ не меньше $|A|^3/K$. Тогда найдется множество Λ такое, что $|\operatorname{Span}\Lambda \cap A| \ge \frac{1}{2} \cdot \frac{|A|}{K^{1/2+\varepsilon}}$ и $|\Lambda| \le 2^{30}\varepsilon^{-2}K\log|A|$.*

Общее свойство теорем 1.1,1.2,1.3,1.4 состоит в том, что число K не может быть слишком большим по сравнению с мощностью множества A. Например, в теореме 1.4 необходимо, чтобы $K \ll \left(\frac{\log|A|}{\log\log|A|}\right)^2$, в противном случае эта теорема становится тривиальной. Наша теорема 1.5 имеет несколько отличий от вышеназванных результатов. Во–первых, теорема 1.5 дает некоторую информацию о структуре множества A при очень больших K (например, можно выбрать $K = |A|^{\eta}$, где η — любое достаточно малое число). Во–вторых, в отличие от теорем 1.1,1.2,1.3,1.4 в нашем результате мощность множества Λ зависит не только от K, но и от $|A|$. Кроме того, и это наименее важно, в теореме 1.5 речь идет о множествах A с большим числом решений уравнения

$$a_1 + a_2 = a_3 + a_4\,, \qquad \text{где } a_i \in A, \quad i = 1,2,3,4\,, \tag{1}$$

а не о множествах с малым удвоением. Легко видеть, что любое множество с малым удвоением имеет большое число решений уравнения (1) (см. следствие 3.3). Наоборот, произвольное множество с большим количеством решений (1) содержит подмножество с малым удвоением (см. работы [1, 2, 3]). Поэтому, свойство множества A иметь большое

число решений (1) и свойство A быть множеством с малой суммой являются, в некотором грубом смысле, эквивалентными.

Скажем несколько слов о содержании настоящей статьи. В параграфе 2 мы изучаем, так называемые, "связные множества" в конечных абелевых группах. Мы доказываем, что любое такое множество сильно пересекается с $\operatorname{Span}\Lambda$ для некоторого не очень большого множества Λ (более подробно см. предложения 2.8, 2.10). Кроме того, в этом же параграфе мы показываем, что при выполнении некоторых простых условий всякое множество содержит достаточно большое связное подмножество. Из этих двух фактов и вытекает теорема 1.5. Мы приводим ее полное доказательство в параграфе 3. В последнем параграфе 4 разъясняется причина употребления нами термина "связность". Мы показываем, что наше определение связных множеств в абелевых группах является переносом одного теоретико–графового определения связности из статьи И. Ружи и Г. Элекеша [8].

Автор выражает благодарность доктору физико–математических наук, профессору Н. Г. Мощевитину за постоянное внимание к работе, а также доктору физико–математических наук, профессору С. В. Конягину за ряд ценных замечаний.

2. О связных множествах в абелевых группах.

Пусть G — абелева группа. Обозначим групповую операцию знаком $+$. Пусть $A \subseteq G$ — произвольное конечное множество и $k \geq 2$ — натуральное число. Обозначим через $T_k(A)$ число решений уравнения

$$T_k(A) := |\{a_1 + \cdots + a_k = a'_1 + \cdots + a'_k \ : \ a_1, \ldots, a_k, a'_1, \ldots, a'_k \in A\}| \,.$$

Будем обозначать той же буквой A характеристическую функцию множества A. Для краткости мы будем писать $\sum_x$ вместо $\sum_{x\in G}$.

Определение 2.1 Пусть $k \geq 2$ — натуральное число и $\beta \in [0,1]$ — действительное число. Непустое конечное множество $A \subseteq G$ называется (C,β)*–связным порядка* k, если для всякого множества $B \subseteq A$, $|B| \geq \beta|A|$ выполнено

$$T_k(B) \geq C^{2k} \left(\frac{|B|}{|A|}\right)^{2k} T_k(A) \,. \qquad (2)$$

Из определения вытекает, что $C \leq 1$. Если $\beta = 0$, то будем называть множество C*–связным порядка* k. Иногда, для краткости, мы будем называть (C,β)–связные и C–связные порядка k множества просто связными.

Класс (C,β)–связных порядка k множеств достаточно широк. С одной стороны, сильно структурированные множества, такие как прогрессии, многомерные прогрессии, подпространства являются связными множествами порядка k (см. следствие 2.4 ниже). С другой стороны, в этот класс входят, так называемые, *диссоциативные* множества (см. определение 2.5 и замечание 2.7). Другие примеры связных порядка k множеств будут рассмотрены в параграфе 4. Отметим, наконец, что любое множество из двух элементов является 1–связным.

Выразим величину T_k в терминах свертки.

Определение 2.2 Пусть $f, g : G \to \mathbb{R}$ — произвольные функции. Обозначим через $(f * g)(x)$ функцию

$$(f * g)(x) = \sum_s f(s) g(x - s) \,. \qquad (3)$$

Ясно, что $(f*g)(x)=(g*f)(x)$, $x\in G$. Через $(f\circ g)(x)$ обозначим функцию

$$(f\circ g)(x)=\sum_s f(s)g(s-x)\,. \qquad (4)$$

Очевидно $(f\circ g)(x)=(g\circ f)(-x)$, $x\in G$.

Если $A,B\subseteq G$ — произвольные множества, то $(A*B)(x)\neq 0$ тогда и только тогда, когда $x\in A+B$, а $(A\circ B)(x)\neq 0$ тогда и только тогда, когда $x\in A-B$. Отсюда $T_2(A)=\sum_x(A*A)^2(x)$ и $T_k(A)=\sum_x(A*_{k-1}A)^2(x)$, где через $*_{k-1}$ мы обозначили результат взятия $k-1$ раз операции $*$. Так как

$$T_2(A):=|\{a_1+a_2=a_1'+a_2'\ :\ a_1,a_2,a_1',a_2'\in A\}|=|\{a_1-a_1'=a_2'-a_2\ :\ a_1,a_2,a_1',a_2'\in A\}|\,,$$

то $T_2(A)=\sum_x(A\circ A)^2(x)$.

Пусть $f:G\to\mathbb{R}$ — произвольная функция. Через $T_k(f)$ обозначим величину $T_k(f)=\sum_x(f*_{k-1}f)^2(x)$. Справедлива лемма.

Лемма 2.3 *Пусть p_1,p_2 — натуральные числа и $k_1=2^{p_1}$, $k_2=2^{p_2}$. Пусть также $f_1,\dots,f_{k_1},g_1,\dots,g_{k_2}:G\to\mathbb{R}$ — некоторые функции. Тогда*

$$\left|\sum_x(f_1*\dots*f_{k_1})(x)\cdot(g_1*\dots*g_{k_2})(x)\right|\le$$

$$\le(T_{k_1}(f_1))^{1/2k_1}\dots(T_{k_1}(f_{k_1}))^{1/2k_1}(T_{k_2}(g_1))^{1/2k_2}\dots(T_{k_2}(g_{k_2}))^{1/2k_2}\,. \qquad (5)$$

Доказательство. Сначала рассмотрим ситуацию, когда $k_1=k_2=k=2^p$, p — натуральное число. Докажем лемму методом индукции по k. Пусть $\sigma=\sum_x(f_1*\dots*f_k)(x)\cdot(g_1*\dots g_k)(x)$. Применяя неравенство Коши–Буняковского, находим

$$\sigma^2\le\sum_x(f_1*\dots*f_k)^2(x)\cdot\sum_x(g_1*\dots*g_k)^2(x)=\sigma_1\sigma_2\,. \qquad (6)$$

Рассмотрим сумму σ_1. Используя определение операций $*,\circ$, получаем

$$\sigma_1=\sum_x((f_1\circ f_1)*\dots*(f_{2^{p-1}}\circ f_{2^{p-1}}))(x)\cdot((f_{2^{p-1}+1}\circ f_{2^{p-1}+1})*\dots*(f_k\circ f_k))(x)\,.$$

Из индукционного предположения вытекает, что

$$\sigma_1\le(T_{2^{p-1}}(f_1\circ f_1))^{1/k}\dots(T_{2^{p-1}}(f_k\circ f_k))^{1/k}\,. \qquad (7)$$

Кроме того $T_{2^{p-1}}(f_1\circ f_1)=T_k(f_1)$. Отсюда

$$\sigma_1\le(T_k(f_1))^{1/k}\dots(T_k(f_k))^{1/k}\,. \qquad (8)$$

Аналогично

$$\sigma_2\le(T_k(g_1))^{1/k}\dots(T_k(g_k))^{1/k}\,. \qquad (9)$$

Подставляя неравенства (8) и (9) в (6), получаем, что в случае $k_1=k_2$ неравенство (5) выполнено.

Пусть теперь $k_1=2^{p_1}$, $k_2=2^{p_2}$ и $p_1\neq p_2$. Пусть $\sigma'=\sum_x(f_1*\dots*f_{k_1})(x)\cdot(g_1*\dots g_{k_2})(x)$. Применяя неравенство Коши–Буняковского, находим

$$\sigma'^2\le\sum_x(f_1*\dots*f_{k_1})^2(x)\cdot\sum_x(g_1*\dots*g_{k_2})^2(x)=\sigma_1'\sigma_2'\,. \qquad (10)$$

Используя неравенство (5) для сумм σ_1', σ_2', получаем неравенство

$$|\sigma'| \le (T_{k_1}(f_1))^{1/2k_1} \dots (T_{k_1}(f_{k_1}))^{1/2k_1} (T_{k_2}(g_1))^{1/2k_2} \dots (T_{k_2}(g_{k_2}))^{1/2k_2} . \qquad (11)$$

Лемма доказана.

Выведем одно следствие из леммы 2.3. Пусть n — натуральное число, q — простое, а группа G есть $(\mathbb{Z}/q\mathbb{Z})^n$. Тогда G обладает естественной структурой векторного пространства.

Следствие 2.4 *Пусть n, p — натуральные числа, $k = 2^p$, q — простое и $G = (\mathbb{Z}/q\mathbb{Z})^n$. Пусть также P — подпространство G. Тогда P является 1–связным порядка k множеством.*

Доказательство. Пусть $B \subseteq P$ — произвольное множество и пусть $\sigma(B) := \sum_x (B * P *_{k-2} P)(x) \cdot (P *_{k-1} P)(x)$. Сумма $\sigma(B)$ равна числу решений уравнения $b + p_2 + \dots + p_k = p_1' + \dots + p_k'$, где $b \in B$ и $p_2, \dots, p_k, p_1', \dots, p_k' \in P$. Так как P — подпространство $(\mathbb{Z}/q\mathbb{Z})^n$, то $b + p_2 + \dots + p_k - p_1' - \dots - p_k' \in P$. Отсюда $\sigma(B) \ge |B||P|^{2k-2}$. В частности, $\sigma(P) = T_k(P) \ge |P|^{2k-1}$. Так как $T_k(P) \le |P|^{2k-1}$, то $T_k(P) = |P|^{2k-1}$. Применяя лемму 2.3 с $f_1 = B$, $f_2 = \dots = f_k = g_1 = \dots = g_k = P$, находим

$$\sigma^{2k}(B) \le T_k(B) \cdot T_k^{2k-1}(P) . \qquad (12)$$

Соединяя последнее неравенство с нижней оценкой для $\sigma(B)$, получаем

$$T_k(B) \ge \frac{\sigma^{2k}(B)}{T_k^{2k-1}(P)} \ge \frac{|B|^{2k}|P|^{(2k-2)2k}}{|P|^{(2k-1)^2}} = \left(\frac{|B|}{|P|}\right)^{2k} |P|^{2k-1} = \left(\frac{|B|}{|P|}\right)^{2k} T_k(P) .$$

Следствие доказано.

Таким образом, такие хорошо структурированные множества, как подпространства, являются связными. Рассмотрим другие примеры связных множеств.

Напомним определение диссоциативного множества (см. [18] или [7]).

Определение 2.5 Множество $\Lambda = \{\lambda_1, \dots, \lambda_{|\Lambda|}\} \subseteq G$ называется *диссоциативным*, если из равенства

$$\sum_{i=1}^{|\Lambda|} \varepsilon_i \lambda_i = 0 , \qquad (13)$$

где $\varepsilon_i \in \{-1, 0, 1\}$ вытекает, что все ε_i равны нулю.

Для диссоциативных множеств имеется хорошая оценка на T_k. Говоря точнее, справедливо следующее утверждение, вытекающее из известного неравенства Рудина (см. [18], а также [11, 19]).

Утверждение 2.6 *Существует абсолютная константа $M > 0$ такая, что для произвольного диссоциативного множества $\Lambda \subseteq G$ и любого натурального $k \ge 2$ выполнено неравенство*

$$T_k(\Lambda) \le M^k k^k |\Lambda|^k , \qquad (14)$$

при этом константу M можно взять равной 288.

Замечание 2.7 Выше мы уже отмечали, что диссоциативные множества входят в класс связных множеств. Действительно, для любого диссоциативного множества A справедливо неравенство $T_k(A) \le M^k k! |A|^k$, где M — некоторая абсолютная константа, а k — произвольное натуральное число. Всякое множество с указанной оценкой на T_k будет

$(1/\sqrt{2M}, 2k/|A|)$–связным порядка k множеством. Последнее утверждение следует из цепочки неравенств

$$T_k(B) \geq 2^{-k} k! |B|^k \geq 2^{-k} k! \left(\frac{|B|}{|A|}\right)^{2k} |A|^k \geq \left(\frac{|B|}{|A|}\right)^{2k} T_k(A)(2M)^{-k}\,, \qquad (15)$$

где $B \subseteq A$ — произвольное.

Отметим одно свойство C–связных порядка k множеств.

Предложение 2.8 *Пусть $k \geq 2$ — натуральное число и пусть $A \subseteq G$ — C–связное порядка k множество. Тогда существует множество $\Lambda \subseteq A$, $|\Lambda| \leq 288C^{-2}k\frac{|A|^2}{T_k^{1/k}(A)}$, такое, что любой элемент a из множества A представляется в виде*

$$a = \sum_{i=1}^{|\Lambda|} \varepsilon_i \lambda_i\,, \qquad (16)$$

где $\varepsilon_i \in \{-1, 0, 1\}$.

Доказательство. Пусть Λ — максимальное (по мощности) диссоциативное подмножество A. Докажем, что любой элемент $a \in A$ представляется в виде

$$a = \sum_{i=1}^{|\Lambda|} \varepsilon_i \lambda_i\,, \qquad (17)$$

где $\varepsilon_i \in \{-1, 0, 1\}$. Если $a = 0$, то равенство (17), очевидно, выполнятся, если положить $\varepsilon_i = 0$, $i = 1, 2, \ldots, |\Lambda|$. Пусть a — произвольный элемент из $A \setminus \Lambda$, $a \neq 0$. Рассмотрим все соотношения вида $\sum_{i=1}^{|\Lambda|+1} \varepsilon_i \tilde{\lambda}_i = 0$, где $\tilde{\lambda}_i \in \Lambda \bigsqcup \{a\}$ и $\varepsilon_i \in \{-1, 0, 1\}$, $i \in \{1, 2, \ldots, |\Lambda| + 1\}$. Если все такие соотношения тривиальны, то есть если для любого такого соотношения выполнено $\varepsilon_i = 0$, $i \in \{1, 2, \ldots, |\Lambda|+1\}$, то мы получаем противоречие с максимальностью Λ. Значит, существует нетривиальное соотношение вида $\varepsilon a + \sum_{i=1}^{|\Lambda|} \varepsilon_i \lambda_i = 0$, $\varepsilon, \varepsilon_i \in \{-1, 0, 1\}$ такое, что не все числа $\varepsilon, \varepsilon_i$ равны нулю. Если $\varepsilon = 0$, то получаем противоречие с тем, что Λ диссоциативно. Отсюда любой элемент $a \in A$ представляется в виде (16).

Получим оценку $|\Lambda| \leq 288C^{-2}k\frac{|A|^2}{T_k^{1/k}(A)}$. Применяя утверждение 2.6, находим $T_k(\Lambda) \leq (288)^k k^k |\Lambda|^k$. С другой стороны, множество A является C–связным порядка k. Следовательно, $T_k(\Lambda) \geq C^{2k}(|\Lambda|/|A|)^{2k} \cdot T_k(A)$. Отсюда $|\Lambda| \leq 288C^{-2}k\frac{|A|^2}{T_k^{1/k}(A)}$. Предложение доказано.

Нам понадобится еще одно, более техническое, определение связных множеств.

Определение 2.9 Пусть $k \geq 2$ — натуральное число и $\beta_1, \beta_2 \in [0, 1]$ — действительные числа, $\beta_1 \leq \beta_2$. Непустое множество $A \subseteq G$ называется (C, β_1, β_2)–*связным порядка* k, если для всякого множества $B \subseteq A$, $\beta_1|A| \leq |B| \leq \beta_2|A|$ выполнено

$$T_k(B) \geq C^{2k} \left(\frac{|B|}{|A|}\right)^{2k} T_k(A)\,. \qquad (18)$$

Если $\beta_1 > 0$ и $[\beta_2|A|] < \beta_1|A|$, то семейство (C, β_1, β_2)–связных порядка k множеств — пустое. Если же $\beta_1 > 0$, $[\beta_2|A|] \geq \beta_1|A|$, то рассматривая математическое ожидание величины $T_k(\cdot)$ по множествам $B \subseteq A$ удовлетворяющих условию $|B| = [\beta_2|A|]$ получаем, что константа C в неравенстве (18) не превосходит единицы.

Ясно, что любое (C,β)–связное порядка k множество является и (C,β,β_2)–связным порядка k, где $\beta_2 \in [\beta,1]$ — любое число. Таким образом, свойство множества быть (C,β_1,β_2)–связным слабее свойства (C,β_1)–связности. Тем не менее, для (C,β_1,β_2)–связных порядка k множеств выполнен следующий ослабленный аналог предложения 2.8.

Предложение 2.10 *Пусть $k \geq 2$ — натуральное число, $0 < \beta_1 \leq \beta_2$ — действительные числа. Пусть также $A \subseteq G$ — (C,β_1,β_2) — связное порядка k множество. Предположим, что $\beta_2 \geq \beta_1 + 1/|A|$, $T_k(A) \geq 2^{14k}C^{-2k}k^k|A|^k$ и $|A| \geq 1/\beta_1$. Тогда существует множество $\Lambda \subseteq A$,*

$$|\Lambda| \leq 2^{13}C^{-2}k\frac{|A|^2}{T_k^{1/k}(A)}\,, \tag{19}$$

такое, что $|\mathrm{Span}\,\Lambda \cap A| \geq (1-\beta_1)|A|$.

Доказательство. Доказательство предложения представляет собой алгоритм. Пусть Λ_1 — диссоциативное подмножество A такое, что $|\mathrm{Span}\,\Lambda_1 \cap A| \geq (1-\beta_1)|A|$. Ясно, что такое множество Λ_1 существует, например, в качестве Λ_1 можно взять максимальное (по мощности) диссоциативное подмножество A. Пусть $l = [2^{13}C^{-2}k\frac{|A|^2}{T_k^{1/k}(A)}]$. Так как $\beta_1 > 0$, то $C \leq 1$. Кроме того $T_k(A) \leq |A|^{2k}$, откуда $l > 1$. Если $|\Lambda_1| \leq l$, то предложение доказано. Пусть теперь $|\Lambda_1| > l$. Возьмем любое множество $\Lambda_1' \subseteq \Lambda_1$ мощности l. Ясно, что Λ_1' — диссоциативное множество. Рассмотрим множество $A_1 = A \setminus \Lambda_1'$. Если $|A_1| < (1-\beta_1)|A|$, то закончим наш алгоритм. Если же $|A_1| \geq (1-\beta_1)|A|$, то пусть Λ_2 — диссоциативное подмножество A_1 такое, что $|\mathrm{Span}\,\Lambda_2 \cap A_1| \geq (1-\beta_1)|A|$. Предположим, что $|\Lambda_2| \leq l$. Тогда $|\mathrm{Span}\,\Lambda_2 \cap A| \geq |\mathrm{Span}\,\Lambda_2 \cap A_1| \geq (1-\beta_1)|A|$ и предложение доказано. Значит, $|\Lambda_2| > l$. Возьмем любое множество $\Lambda_2' \subseteq \Lambda_2$ мощности l и рассмотрим множество $A_2 = A_1 \setminus \Lambda_2'$. И так далее. Мы получим множества $A_0 = A, A_1, A_2, \ldots, A_s$ и непересекающиеся диссоциативные множества $\Lambda_1', \ldots, \Lambda_s'$ из A. При этом $|A_s| < (1-\beta_1)|A|$. Так как для всех $l = 1,2,\ldots,s$ выполнено $A_l = A \setminus \bigsqcup_{i=1}^{l}\Lambda_i'$, то $\sum_{i=1}^{s}|\Lambda_i'| = |A| - |A_s| > \beta_1|A|$. Пусть $B = \bigsqcup_{i=1}^{s}\Lambda_i'$. Тогда $|B| > \beta_1|A|$. Выкинув, если это необходимо, несколько элементов из множества Λ_s', можно добиться того, чтобы мощность множества $\bigsqcup_{i=1}^{s}\Lambda_i'$ стала равна $[\beta_1|A|]+1$. Обозначим той же буквой B множество, получающееся после выкидывания этих элементов из Λ_s'. Имеем $B \subseteq A$ и $|B| \geq \beta_1|A|$. Так как $\beta_2 \geq \beta_1 + 1/|A|$, то $|B| \leq \beta_2|A|$. По условию, множество A является (C,β_1,β_2) — связным порядка k. Отсюда

$$T_k(B) \geq C^{2k}\beta_1^{2k}T_k(A)\,. \tag{20}$$

С другой стороны

$$T_k(B) \leq T_k\left(\bigsqcup_{i=1}^{s}\Lambda_i'\right) = \sum_{i_1,\ldots,i_k=1}^{s}\sum_{j_1,\ldots,j_k=1}^{s}\sum_{x}(\Lambda_{i_1}' * \cdots * \Lambda_{i_k}')(x)\cdot(\Lambda_{j_1}' * \cdots * \Lambda_{j_k}')(x)\,. \tag{21}$$

Применяя лемму 2.3, утверждение 2.6 и равенство (21) получаем, что

$$T_k(B) \leq s^{2k}\max_{i=1,\ldots,s}T_k(\Lambda_i') \leq s^{2k}(288)^k k^k l^k\,. \tag{22}$$

По условию $T_k(A) \geq 2^{14k}C^{-2k}k^k|A|^k$. Отсюда $|A| \geq 2^{14}C^{-2}k\frac{|A|^2}{T_k^{1/k}(A)} \geq 2l$ и либо мы уже доказали наше предложение, либо $s \geq 2$. Так как $\bigsqcup_{i=1}^{s-1}\Lambda_i' \subseteq B$ и $|A| \geq 1/\beta_1$, то $sl/2 \leq$

$(s-1)l \le |B| \le 2\beta_1|A|$. Следовательно, $s \le 4\beta_1|A|/l$. Подставляя последнее неравенство в (22), находим

$$T_k(B) \le 2^{4k}\beta_1^{2k}(288)^k k^k \frac{|A|^{2k}}{l^k}\,.$$

Получаем противоречие с неравенством (20). Предложение доказано.

Докажем теперь, что у произвольного множества $A \subseteq G$ найдется достаточно большое (C,β_1,β_2)–связное порядка k подмножество. Нам понадобится определение.

Определение 2.11 Пусть $A \subseteq G$ — произвольное конечное множество, $|A| \ge 2$ и $k \ge 2$ — натуральное число. Через $\zeta_k(A)$ обозначим величину

$$\zeta_k = \zeta_k(A) := \frac{\log T_k(A)}{\log |A|}\,.$$

Иными словами, $T_k(A) = |A|^{\zeta_k}$. Ясно, что для любого множества A выполнено $k \le \zeta_k(A) \le 2k-1$.

Пусть $A \subseteq G$ — произвольное конечное множество, $|A| = m \ge 2$, p — натуральное число и $k = 2^p$. Обозначим через ζ число $\zeta_k(A)$.

Теорема 2.12 *Пусть $\beta_1, \beta_2 \in (0,1)$ — действительные числа, $\beta_1 \le \beta_2$. Тогда найдется множество $A' \subseteq A$ такое, что*

1) *A' является (C,β_1,β_2)–связным порядка k множеством, причем в качестве константы C можно взять любое число не превосходящее $1/32$.*

2) $|A'| \ge m \cdot 2^{\frac{\log((2k-1)/\zeta)}{\log(1+\kappa)}\log(1-\beta_2)}$, *где* $\kappa = \frac{\log((1-\beta_1)^{-1})}{\log m}(1-16C)$.

3) $\zeta_k(A') \ge \zeta_k(A)$.

Доказательство. Пусть $C \le 1/32$ — некоторое число. Доказательство теоремы 2.12 представляет собой алгоритм. Если множество A является (C,β_1,β_2)–связным множеством порядка k, то доказывать нечего. Пусть теперь множество A не является (C,β_1,β_2)–связным порядка k множеством. Тогда найдется множество $B \subseteq A$, $\beta_1|A| \le |B| \le \beta_2|A|$ такое, что неравенство (18) не выполнено. Заметим, что в этом случае $|A| > 2$. Пусть $\overline{B} = A \setminus B$. Имеем

$$T_k(A) = \sum_x (A *_{k-1} A)^2(x) =$$

$$= \sum_x (B * A *_{k-2} A)(x)(A *_{k-1} A)(x) + \sum_x (\overline{B} * A *_{k-2} A)(x)(A *_{k-1} A)(x) = \sigma_1 + \sigma_2\,. \quad (23)$$

Применяя лемму 2.3 с $f_1 = B$, $f_2 = \ldots = f_k = g_1 = \ldots = g_k = A$, находим

$$\sigma_1^{2k} \le T_k(B) \cdot T_k^{2k-1}(A)\,. \quad (24)$$

Аналогично

$$\sigma_2^{2k} \le T_k(\overline{B}) \cdot T_k^{2k-1}(A)\,. \quad (25)$$

Пусть $c_B = |B|/|A|$. Так как $T_k(B) < C^{2k}c_B^{2k}T_k(A)$, то из неравенства (24) вытекает, что $\sigma_1 < Cc_BT_k(A)$. Применяя последнее неравенство, равенство (23) и неравенство (25), получаем

$$T_k(\overline{B}) > T_k(A)(1-Cc_B)^{2k}\,. \quad (26)$$

Пусть $\overline{\zeta} = \zeta_k(\overline{B})$, $b = |B|$ и $\overline{b} = |\overline{B}| = m - b$. Используя неравенство (26), находим

$$\overline{\zeta}\log\overline{b} > \zeta\log m + 2k\log(1-Cc_B)\,.$$

Применяя последнюю оценку и неравенства $\zeta \geq k$, $C \leq 1/32$, получаем

$$\overline{\zeta} > \frac{\zeta \log m + 2k \log(1 - Cc_B)}{\log \overline{b}} = \frac{\zeta \log m + 2k \log(1 - Cc_B)}{\log m + \log(1 - b/m)} = \frac{\zeta + 2k \frac{\log(1-Cc_B)}{\log m}}{1 + \frac{\log(1-c_B)}{\log m}} \geq$$

$$\geq \left(\zeta + 2k \frac{\log(1 - Cc_B)}{\log m}\right)\left(1 - \frac{\log(1 - c_B)}{\log m}\right) =$$

$$= \zeta + \zeta \frac{\log((1 - c_B)^{-1})}{\log m} + 2k \frac{\log(1 - Cc_B)}{\log m} + 2k \frac{\log(1 - Cc_B)}{\log m} \cdot \frac{\log(1 - c_B)^{-1}}{\log m} \geq$$

$$\geq \zeta + \zeta \frac{\log((1 - c_B)^{-1})}{\log m}\left(\frac{2 \log(1 - Cc_B)}{\log((1 - c_B)^{-1})} + \frac{2 \log(1 - Cc_B)}{\log m}\right) \geq$$

$$\geq \zeta + \zeta \frac{\log((1 - c_B)^{-1})}{\log m}(1 - 8C - 4C) \geq \zeta + \zeta \frac{\log((1 - c_B)^{-1})}{\log m}(1 - 16C) \geq$$

$$\geq \zeta(1 + \frac{\log((1 - \beta_1)^{-1})}{\log m}(1 - 16C)) = \zeta(1 + \kappa)\,, \tag{27}$$

где $\kappa = \frac{\log((1-\beta_1)^{-1})}{\log m}(1-16C) > 0$. Кроме того, из определения (C, β_1, β_2)–связности порядка k вытекает неравенство

$$|\overline{B}| \geq (1 - \beta_2)m = (1 - \beta_2)|A|\,. \tag{28}$$

Таким образом, если множество A не является (C, β_1, β_2)–связным порядка k, то найдется множество $\overline{B} \subseteq A$ для которого выполнены неравенства (27), (28). Положим $A_1 = \overline{B}$ и применим изложенные выше рассуждения к множеству A_1. И так далее. Мы получим множества $A_0 = A, A_1, A_2, \ldots, A_s$. Ясно, что для любого A_i справедливо неравенство $\zeta(A_i) \leq 2k - 1$. Отсюда и неравенства (27) вытекает, что наш процесс закончится менее, чем через $\frac{\log((2k-1)/\zeta)}{\log(1+\kappa)}$ шагов. На последнем шаге алгоритма мы найдем множество $A' = A_s \subseteq A$, которое будет (C, β_1, β_2)–связным порядка k и, при этом, $\zeta_k(A') \geq \zeta = \zeta_k(A)$. Таким образом неравенства 1) и 3) теоремы 2.12 для множества A' выполнены. Докажем 2). Применяя неравенство (28) и оценку $s \leq \frac{\log((2k-1)/\zeta)}{\log(1+\kappa)}$, получаем

$$|A'| \geq (1 - \beta_2)^s m \geq m \cdot 2^{\frac{\log((2k-1)/\zeta)}{\log(1+\kappa)} \log(1-\beta_2)}\,.$$

Теорема доказана.

Следствие ниже показывает, что любое достаточно плотное подмножество A конечной абелевой группы содержит большое связное подмножество $A' \subseteq A$.

Следствие 2.13 *Пусть G — конечная абелева группа, ε, δ — действительные числа, $\varepsilon \in (0, 1/8]$, $\delta \in (0, 1]$, $\delta \geq |G|^{-\varepsilon}$ и пусть $A \subseteq G$ — произвольное подмножество, $|A| \geq \delta|G| \geq 2$. Пусть также p — натуральное число, $k = 2^p$ и $\beta_1, \beta_2 \in (0, 1)$ — действительные числа, $\beta_1 \leq \beta_2$, $\beta_1 \leq 1 - |A|^{-2\varepsilon}$. Тогда найдется множество $A' \subseteq A$ такое, что*
1) *A' является (C, β_1, β_2)–связным порядка k множеством, причем в качестве константы C можно взять $1/32$.*
2) $|A'| \geq |G| \cdot \delta^{\left(\frac{2}{2k-1} + 32\varepsilon\right) \cdot \frac{\log(1-\beta_2)}{\log(1-\beta_1)} + 1}$.
3) $\zeta_k(A') \geq \zeta_k(A)$.

В частности, если $\beta_2 = \beta_1$, $k = 2$ и $\varepsilon = 1/8$, то мощность множества $|A'|$ не меньше $\delta^6|G|$.

Доказательство. Применяя теорему 2.12 с $C = 1/32$ находим множество $A' \subseteq A$ для которого выполнены свойства 1)—3) этой теоремы. Докажем, что $|A'| \geq |G| \cdot \delta^{\left(\frac{2}{2k-1}+32\varepsilon\right)\cdot\frac{\log(1-\beta_2)}{\log(1-\beta_1)}+1}$. Пусть $N = |G|$, $m = |A|$ и $\zeta = \zeta_k(A)$. Ясно, что $T_k(A) \geq \delta^{2k} N^{2k-1}$. Отсюда

$$\zeta \geq 2k - 1 + (2k-1)\frac{\log(1/\delta)}{\log N} - \frac{2k}{1-\varepsilon}\frac{\log(1/\delta)}{\log N}\,. \tag{29}$$

Так как $\delta \geq N^{-\varepsilon}$, то

$$2k - 1 - \zeta \leq \frac{\log(1/\delta)}{\log N}(1 + 4k\varepsilon) \quad \text{и} \quad \zeta \geq (2k-1)(1-3\varepsilon)\,. \tag{30}$$

Отсюда

$$\frac{2k-1}{\zeta} = 1 + \frac{2k-1-\zeta}{\zeta} \leq 1 + \frac{1}{2k-1}\frac{\log(1/\delta)}{\log N} + 16k\varepsilon\frac{\log(1/\delta)}{\log N}\,. \tag{31}$$

По теореме 2.12 имеем $|A'| \geq m \cdot 2^{\frac{\log((2k-1)/\zeta)}{\log(1+\kappa)}\log(1-\beta_2)}$, где $\kappa = \frac{\log((1-\beta_1)^{-1})}{2\log m}$. Применяя последнее неравенство, неравенства $\beta_1 \leq 1 - |A|^{-2\varepsilon}$, $k \geq 2$ и (31), находим

$$|A'| \geq m \cdot 2^{\left(\frac{2}{2k-1}+32\varepsilon\right)\cdot\frac{\log(1-\beta_2)}{\log(1-\beta_1)}\cdot\frac{\log\delta}{\log N}\log m} \geq N \cdot \delta^{\left(\frac{2}{2k-1}+32\varepsilon\right)\cdot\frac{\log(1-\beta_2)}{\log(1-\beta_1)}+1}\,.$$

Следствие доказано.

Замечание 2.14 Константа 32 во втором пункте следствия 2.13, безусловно, может быть понижена. Мы не стремились сделать эту константу как можно меньшей. Появление числа 2 в дроби $\frac{2}{2k-1}$ зависит от выбора верхней границы для C. Если взять C меньше, чем $1/32$, то константа 2 также понизится.

3. Доказательство основного результата.

Из леммы 2.3 вытекает простая оценка для величины $T_k(A)$.

Лемма 3.1 *Пусть A — произвольное непустое конечное множество и k — любое натуральное число, $k \geq 2$. Тогда $T_k(A) \geq T_2^{k-1}(A)/|A|^{k-2}$.*

Замечание 3.2 Лемму 3.1, безусловно, можно доказать применяя метод преобразования Фурье. Однако поскольку мы используем только элементарные методы, мы получим лемму 3.1 используя лишь неравенство Коши–Буняковского.

Доказательство. Докажем лемму 3.1 по индукции. Для $k = 2$ лемма очевидна. Пусть $k \geq 3$ и для всех меньших k лемма доказана. Число k имеет вид $2s-1$, $s \geq 2$ или $2s-2$, $s \geq 3$. Пусть $k = 2s-1$, $s \geq 2$. Применяя неравенство Коши–Буняковского, находим

$$T_s^2(A) = \left(\sum_x (A *_{s-1} A)^2(x)\right)^2 = \left(\sum_x ((A *_{s-1} A) \circ (A *_{s-2} A))(x) \cdot A(x)\right)^2 \leq$$

$$\leq \sum_x ((A *_{s-1} A) \circ (A *_{s-2} A))^2(x) \cdot |A| = T_{2s-1}(A) \cdot |A|\,. \tag{32}$$

По индукционному предположению $T_s(A) \geq T_2^{s-1}(A)/|A|^{s-2}$. Отсюда и неравенства (32), получаем

$$T_{2s-1}(A) \geq \frac{T_2^{2s-2}(A)}{|A|^{2(s-2)}|A|} = \frac{T_2^{2s-2}(A)}{|A|^{2s-3}}$$

и в этом случае лемма доказана.

Пусть теперь $k = 2s-2$, $s \geq 3$. Имеем

$$T_s^2(A) = \left(\sum_x (A *_{s-1} A)^2(x)\right)^2 = \left(\sum_x ((A *_{s-1} A) \circ (A *_{s-3} A))(x) \cdot (A * A)(x)\right)^2 \leq$$

$$\leq \sum_x ((A *_{s-1} A) \circ (A *_{s-3} A))^2(x) \cdot T_2(A) = T_{2s-2}(A) \cdot T_2(A)\,. \qquad (33)$$

Применяя индукционное предположение, находим

$$T_{2s-2}(A) \geq \frac{T_s^2(A)}{T_2(A)} \geq \frac{T_2^{2s-3}(A)}{|A|^{2s-4}}\,.$$

Лемма доказана.

Доказательство теоремы 1.5 Пусть $m = |A|$, $\beta_1 = 1/2$, $\beta_2 = \beta_1 + 1/\log m$, $C = \varepsilon 2^{-7}$, $k = 2^p$, $p = [\log\ln m] + 1$. Ясно, что $C \leq 1/32$. Применяя теорему 2.12 к множеству A, находим множество $A' \subseteq A$, удовлетворяющее пунктам 1) — 3) теоремы. По условию, имеем $T_2(A) \geq |A|^3/K$. Из леммы 3.1 вытекает, что $T_k(A) \geq T_2^{k-1}(A)/|A|^{k-2} \geq |A|^{2k-1}/K^{k-1}$. Отсюда

$$\zeta = \zeta_k(A) \geq 2k - 1 - (k-1)\frac{\log K}{\log m}\,. \qquad (34)$$

Применяя оценку $K \leq m^{\varepsilon}$ и неравенство (34), находим

$$\zeta \geq (2k-1)\left(1 - \frac{k-1}{2k-1}\frac{\log K}{\log m}\right) \geq \qquad (35)$$

$$\geq (2k-1)\left(1 - \frac{\varepsilon}{2}\right)\,. \qquad (36)$$

По свойству пункта 2) теоремы 2.12 имеем

$$|A'| \geq m \cdot 2^{-\frac{\log((2k-1)/\zeta)}{\log(1+\kappa)}\log((1-\beta_2)^{-1})} = m2^{-\sigma}\,, \qquad (37)$$

где $\kappa = \frac{\log((1-\beta_1)^{-1})}{\log m}(1-16C)$. Оценим число σ сверху. Пользуясь неравенствами $\log(1+x) \leq \frac{x}{\ln 2}$, $\log(1+x) \geq \frac{1}{\ln 2}(x - x^2/2)$, $x \geq 0$, $m \geq 2^{32/\varepsilon}$ и неравенствами (34), (35), (36) получаем

$$\sigma \leq \log\left(1 + \frac{2k-1-\zeta}{\zeta}\right)\frac{\ln 2}{\kappa}(1+\kappa)\log((1-\beta_2)^{-1}) \leq$$

$$\leq \frac{k-1}{2k-1}\cdot\frac{\log K}{\log m}(1+\varepsilon)\frac{\log m}{1-16C}\left(1 + \frac{1}{\log m}\right)\frac{\log((1-\beta_2)^{-1})}{\log((1-\beta_1)^{-1})} \leq$$

$$\leq \log K^{1/2}(1+\varepsilon)(1+32C)\left(1 + \frac{8}{\log m}\right) \leq \log K^{1/2+\varepsilon}\,.$$

Следовательно, $|A'| \geq \frac{m}{K^{1/2+\varepsilon}}$. Так как $\zeta_k(A') \geq \zeta_k(A)$, то легко видеть, что

$$T_k(A') \geq \frac{|A'|^{2k-1}}{K^{k-1}} \geq \frac{|A'|^{2k-1}}{K^k}\,. \qquad (38)$$

Имеем $C = \varepsilon 2^{-7}$, а также $k = 2^p$ и $p = [\log\ln m] + 1$. Отсюда $k \le 2\ln m$. Используя последнее неравенство, оценку $|A'| \ge \frac{m}{K^{1/2+\varepsilon}}$, неравенство (38) и условие $K \le (2^{-58}\varepsilon^4 \frac{|A|}{\log|A|})^{(3/2+\varepsilon)^{-1}}$ легко видеть, что

$$T_k(A') \ge \frac{|A'|^{2k-1}}{K^{k-1}} \ge |A'|^k \frac{m^{k-1}}{K^{(k-1)(3/2+\varepsilon)}} \ge 2^{14k} C^{-2k} k^k |A'|^k \,.$$

Применяя предложение 2.10 к множеству A', находим множество Λ такое, что $|\mathrm{Span}\,\Lambda \cap A'| \ge |A'|/2$ и

$$|\Lambda| \le 2^{27}\varepsilon^{-2} k \frac{|A'|^2}{T_k^{1/k}(A')} \,. \tag{39}$$

Имеем

$$|\mathrm{Span}\,\Lambda \cap A| \ge |\mathrm{Span}\,\Lambda \cap A'| \ge \frac{|A'|}{2} \ge \frac{1}{2}\cdot\frac{m}{K^{1/2+\varepsilon}} \,. \tag{40}$$

Нам осталось доказать неравенство $|\Lambda| \le 2^{30}\varepsilon^{-2}K\log m$. Соединяя неравенства (39) и (38), получаем

$$|\Lambda| \le 2^{27}\varepsilon^{-2}Kk|A'|^{1/k} \le 2^{27}\varepsilon^{-2}Kkm^{1/k} \,.$$

Вспоминая, что $k = 2^p$, $p = [\log\ln m] + 1$, окончательно находим $|\Lambda| \le 2^{30}\varepsilon^{-2}K\log m$. Теорема доказана.

Применим теорему выше к множествам с малым удвоением.

Следствие 3.3 *Пусть G — абелева группа. Пусть K, ε — действительные числа, $\varepsilon \in (0, 1/2]$, $A \subseteq G$ — произвольное конечное множество, $|A| \ge 2^{32/\varepsilon}$, $1 \le K \le \min\{\ (2^{-58}\varepsilon^{-4}\frac{|A|}{\log|A|})^{(3/2+\varepsilon)^{-1}}, |A|^{\varepsilon}\ \}$. Пусть также $|A+A| \le K|A|$. Тогда найдется множество Λ такое, что $|\mathrm{Span}\,\Lambda \cap A| \ge \frac{1}{2}\cdot\frac{|A|}{K^{1/2+\varepsilon}}$ и $|\Lambda| \le 2^{30}\varepsilon^{-2}K\log|A|$.*

Доказательство. Имеем $|A+A| \le K|A|$. По неравенству Коши–Буняковского

$$|A|^4 = \left(\sum_x (A*A)(x)\right)^2 \le \sum_x (A*A)^2(x)\cdot|A+A| \le T_2(A)\cdot K|A| \,.$$

Отсюда $T_2(A) \ge |A|^3/K$. Применяя теорему 1.5, получаем требуемый результат. Следствие доказано.

4. О других видах связности.

В этом разделе мы объясним термин "связность", употреблявшийся нами в предыдущих параграфах.

Пусть $\Gamma = (V, f)$ — произвольный неориентированный граф, V — непустое множество вершин, f — характеристическая функция некоторого симметричного подмножества $V \times V$. Пусть $X, Y \subseteq V$ — произвольные подмножества. Обозначим число вершин между X и Y, то есть сумму $\sum_{x\in X}\sum_{y\in Y} f(x,y)$ через $e(X,Y)$. Как известно, граф Γ называется *связным*, если для любой вершины x выполнено $e(x, V\setminus\{x\}) > 0$. В работе [8] Ружа и Элекеш обобщили понятие связных графов следующим образом.

Определение 4.1 Пусть $\alpha \in (0, 1]$ — действительное число. Граф $\Gamma = (V, f)$ называется *связным с плотностью* α, если для любого разбиения множества вершин на два непересекающихся подмножества E и F, $E \bigsqcup F = V$ выполнено

$$e(E,F) \ge \alpha|E||F| \,.$$

Мы определим аналог понятия связных графов с плотностью α для подмножеств абелевых групп. Пусть G — абелева группа и $A \subseteq G$ — произвольное конечное множество. В работах [2, 3, 7] с множеством A связывался, так называемый, граф "популярных разностей" — $\Gamma_A = (V_A, f_A)$. Этот граф сыграл значительную роль в различных задачах комбинаторной теории чисел (см. статьи [2, 3, 7] и книгу [21]). Множество вершин V_A графа Γ_A состоит из самого множества A, а функция f_A есть характеристическая функция множества "популярных разностей"

$$f(x,y) = \begin{cases} 1, & \text{если} \quad |\{x-y = a_1 - a_2 \ : \ a_1, a_2 \in A\}| \geq h\,, \\ 0, & \text{иначе.} \end{cases}$$

Здесь h — некоторое число, $0 \leq h \leq |A|$. Обычно в приложениях h полагают, по–порядку, равным величине $T_2(A)/|A|^2$. Таким образом, функция $f(x,y)$ равна 1, если $(A \circ A)(x-y) \geq h$ и равна 0 в противном случае. Ружа и Элекеш применяли связные с плотностью α подграфы графа Γ_A для доказательства некоторых результатов о сложении множеств (более подробно см. [8]).

Мы определим новый (обобщенный) граф $\Gamma'_A = (V'_A, f'_A)$, у которого симметричная функция f'_A не является характеристической функцией некоторого подмножества $V'_A \times V'_A$. Положим $V'_A := A$ и $f'_A(x,y) := (A \circ A)(x-y)$. Получившийся граф Γ'_A есть некоторая аппроксимация графа Γ_A в том смысле, что функция f_A является нормированной и "обрезанной" версией функции f'_A : $f_A(x,y) = \theta(f'_A(x,y)/h)$, где θ — сдвинутая функция Хейвисайда : $\theta(x) = 1$, если $x \geq 1$ и $\theta(x) = 0$, если $x < 1$. Посмотрим, что означает условие связности с плотностью α для графа Γ'_A. Граф Γ'_A является связным с плотностью α, если для для любого разбиения множества A на два непересекающихся подмножества E и F, $E \bigsqcup F = A$ выполнено

$$e(E,F) = \sum_{x \in E} \sum_{y \in F} (A \circ A)(x-y) = \sum_z (E \circ F)(z) \cdot (A \circ A)(z) \geq \alpha |E||F|\,. \qquad (41)$$

Множество A для которого справедливо неравенство (41) назовем *сильно связным*. Как было сказано выше, обычно в приложениях в качестве h берут число равное, по–порядку, $T_2(A)/|A|^2$. Нам также будет удобно положить $\alpha = C \cdot T_2(A)/|A|^2$, где $C > 0$ — некоторая константа. Наконец, отметим, что определение выше можно обобщить на случай нескольких операций $\circ$. Суммируя вышесказанное, мы получаем следующее определение.

Определение 4.2 Пусть $k \geq 2$ — натуральное число. Непустое конечное множество $A \subseteq G$ называется *C–сильно связным порядка k*, если для любых двух непересекающихся множеств $E, F \subseteq A$, $E \bigsqcup F = A$ выполнено

$$\sum_x (E \circ F)(x) \cdot ((A *_{k-2} A) \circ (A *_{k-2} A))(x) \geq C c_E c_F T_k(A)\,, \qquad (42)$$

где $c_E = |E|/|A|$, $c_F = |F|/|A|$.

Прежде всего покажем, что сильно связные множества являются связными.

Утверждение 4.3 *Пусть p — натуральное число и $k = 2^p$. Если множество A является C–сильно связным порядка k, то A есть $C/8$–связное порядка k множество.*

Доказательство. Если множество A имеет мощность меньше, чем два, то доказывать нечего. Пусть $|A| \geq 2$ и пусть B — произвольное подмножество A и $\overline{B} = A \setminus B$. Пусть также

$$\sigma = \sum_x (B \circ \overline{B})(x) \cdot ((A *_{k-2} A) \circ (A *_{k-2} A))(x)\,. \qquad (43)$$

Так как множество A является C–сильно связным порядка k, то

$$\sigma \geq C\frac{|B|}{|A|}\frac{|\overline{B}|}{|A|}\cdot T_k(A)\,. \tag{44}$$

Имеем

$$\sigma = \sum_x (B * A *_{k-2} A)(x)\cdot(\overline{B} * A *_{k-2} A)(x)\,. \tag{45}$$

Применяя лемму 2.3, получаем $\sigma^{2k} \leq T_k(B)T_k(\overline{B})T_k^{2k-2}(A)$. Соединяя последнее неравенство с неравенством (44), находим

$$T_k(B)T_k(\overline{B}) \geq C^{2k}\frac{|B|^{2k}}{|A|^{2k}}\cdot\frac{|\overline{B}|^{2k}}{|A|^{2k}}T_k^2(A)\,. \tag{46}$$

Если $|B| \leq |A|/2$, то $|\overline{B}| \geq |A|/2$. Применяя последнее неравенство и оценку $T_k(\overline{B}) \leq T_k(A)$, получаем

$$T_k(B) \geq \left(\frac{C}{2}\right)^{2k}\left(\frac{|B|}{|A|}\right)^{2k}T_k(A) \tag{47}$$

и утверждение доказано. Если же $|B| > |A|/2$, то пусть B_1 — любое подмножество B мощности $[|A|/2]$. Ясно, что $|B| \leq 4|B_1|$. По неравенству (47) имеем

$$T_k(B) \geq T_k(B_1) \geq \left(\frac{C}{2}\right)^{2k}\left(\frac{|B_1|}{|A|}\right)^{2k}T_k(A) \geq \left(\frac{C}{8}\right)^{2k}\left(\frac{|B|}{|A|}\right)^{2k}T_k(A)\,.$$

Утверждение доказано.

Итак, сильно связные множества являются связными. В частности, для сильно связных множеств справедливо предложение 2.8 и, следовательно, любое сильно связное множество содержится в $\operatorname{Span}\Lambda$ для некоторого не очень большого множества Λ. По–видимому, тот факт, что сильно связные множества экономно содержатся в подгруппах специального вида, был впервые отмечен Ж. Бургеном и С.В. Конягиным в работе [20] (см. также другую формулировку в книге [21] стр. 114, упр. 2.6.10). Мы сформулируем их результат в наших терминах и приведем, для полноты изложения, доказательство.

Утверждение 4.4 *Пусть $k \geq 2$ — натуральное число. Пусть также $A \subseteq G$ — C–сильно связное порядка k множество и пусть*

$$S = \left\{ x \in G \ : \ ((A *_{k-2} A)\circ(A *_{k-2} A))(x) \geq C\frac{T_k(A)}{|A|^2} \right\}\,.$$

Тогда найдется элемент группы $a \in G$ такой, что $A \subseteq \langle S\rangle + a$, где $\langle S\rangle$ — подгруппа группы G, натянутая на множество S.

Доказательство. Предположим противное. Пусть $H = \langle S\rangle$ и пусть $A_1, \ldots, A_r \subseteq A$ — пересечения смежных классов подгруппы H с множеством A. Пусть существует не менее двух непустых пересечений смежных классов подгруппы H с A, скажем, A_i и A_j, $i < j$, $i, j \in \{1, \ldots, r\}$. Пусть $E = \bigsqcup_{l=1}^{i} A_l$ и $F = A \setminus E$. Тогда множества E и F — непустые. Так как для любых $e \in E$ и $f \in F$ выполнено $e - f \notin H$ и, следовательно, $e - f \notin S$, то

$$\sum_x (E\circ F)(x)\cdot((A *_{k-2} A)\circ(A *_{k-2} A))(x) \leq$$

$$\le \sum_{x\notin S}(E\circ F)(x)\cdot((A*_{k-2}A)\circ(A*_{k-2}A))(x) < C|E||F|\cdot\frac{T_k(A)}{|A|^2}\,,$$

что противоречит определению C–сильной связности порядка k. Утверждение доказано.

Мы закончим этот параграф доказательством аналога теоремы 2.12 для сильно связных множеств.

Пусть $E,F\subseteq A$ — произвольные множества. Обозначим через $e(E,F)$ число $\sum_x(E\circ F)(x)\cdot((A*_{k-2}A)\circ(A*_{k-2}A))(x)$. Ясно, что $e(E_1\bigsqcup E_2,F)=e(E_1,F)+e(E_2,F)$. Для любого множества $E\subseteq A$ обозначим через c_E отношение $|E|/|A|$.

Нам понадобится следующее техническое определение сильно связных множеств порядка k.

Определение 4.5 Пусть $k\ge 2$ — натуральное число и $\beta\in[0,1]$ — действительное число. Непустое конечное множество $A\subseteq G$ называется *сильно (C,β)—связным порядка k*, если найдется множество $B\subseteq A$, $|B|\ge\beta|A|$ такое, что для любых двух непересекающихся множеств $E,F\subseteq B$, $E\bigsqcup F=B$ выполнено

$$\sum_x(E\circ F)(x)\cdot((A*_{k-2}A)\circ(A*_{k-2}A))(x)\ge Cc_Ec_FT_k(A)\,. \qquad (48)$$

Следующее утверждение доказывается аналогично утверждению 4.3.

Утверждение 4.6 *Пусть p — натуральное число, $k=2^p$ и $\beta\in[0,1]$ — действительное число. Пусть множество A является сильно (C,β)—связным порядка k так, что неравенство (48) справедливо для некоторого множества $B\subseteq A$, $|B|\ge\beta|A|$. Тогда множество B является $C\beta^2/8$–связным порядка k.*

Теоретико–графовый вариант леммы 4.7 ниже доказан в [8].

Лемма 4.7 *Пусть $k\ge 2$ — натуральное число, $\varepsilon_1\in[0,1]$ — действительное число и пусть $A\subseteq G$ — произвольное конечное множество. Тогда существует разбиение A на непересекающиеся множества $A_1,\dots,A_l$ такое, что*

1) *Для всех $i,j\in\{1,\dots,l\}$, $i\ne j$ выполнено $e(A_i,A_j)\le\varepsilon_1c_{A_i}c_{A_j}T_k(A)$.*

2) *Для произвольного $i\in\{1,\dots,l\}$ множество A_i обладает следующим свойством : для любых двух непересекающихся множеств $E,F\subseteq A_i$, $E\bigsqcup F=A_i$ выполнено $e(E,F)\ge\varepsilon_1c_Ec_FT_k(A)$.*

Кроме того, разбиение $A_1,\dots,A_l$ обладает свойством

3) $\sum_{i=1}^l T_k(A_i)\ge T_k(A)\cdot(1-(2k-1)\varepsilon_1)$.

Доказательство. Рассмотрим всевозможные разбиения множества A на множества $A_1,\dots,A_s$, где s — произвольное натуральное число. Выберем из этих разбиений то, для которого сумма

$$\sigma(A_1,\dots,A_s)=\sum_{1\le i<j\le k}(\ e(A_i,A_j)-\varepsilon_1c_{A_i}c_{A_j}T_k(A)\ ) \qquad (49)$$

минимальна. Если разбиений, на которых достигается минимальное значение суммы (49) несколько, то выберем любое из них. Мы получим разбиение A на множества $A_1,\dots,A_l$. Из минимальности разбиения $A_1,\dots,A_l$ вытекает, что для всех $i\in\{1,\dots,l\}$ справедливо свойство 2) леммы.

Докажем свойство 1). Пусть для некоторых $i,j\in\{1,\dots,l\}$, $i\ne j$ выполнено $e(A_i,A_j)>\varepsilon_1c_{A_i}c_{A_j}T_k(A)$. Рассматривая новое разбиение $\mathcal{P}=\{A_r\}_{r\ne i,j}\bigsqcup(A_i\bigsqcup A_j)$ и используя последнее неравенство, находим

$$\sigma(\mathcal{P})=\sigma(A_1,\dots,A_s)-(e(A_i,A_j)-\varepsilon_1c_{A_i}c_{A_j}T_k(A))<\sigma(A_1,\dots,A_s)\,.$$

Опять получаем противоречие с минимальностью разбиения $A_1, \dots, A_l$.

Из только что доказанного свойства 1) вытекает третий пункт леммы. Действительно

$$T_k(A) = \sum_x (A *_{k-1} A)^2(x) = \sum_{i,j=1}^{l} \sum_x (A_i * A *_{k-2} A)(x) \cdot (A_j * A *_{k-2} A)(x) =$$

$$= \sum_{i=1}^{l} \sum_x (A_i * A *_{k-2} A)(x) \cdot (A_i * A *_{k-2} A)(x) + \sum_{i,j=1,\, j\neq i}^{l} \sum_x (A_i * A *_{k-2} A)(x) \cdot (A_j * A *_{k-2} A)(x)$$

$$= \sum_{i=1}^{l} \sum_x (A_i * A *_{k-2} A)(x) \cdot (A_i * A *_{k-2} A)(x) + \sum_{i,j=1,\, j\neq i}^{l} \sum_x (A_i \circ A_j)(x) \cdot ((A *_{k-2} A) \circ (A *_{k-2} A))(x)$$

$$\leq \sum_{i=1}^{l} \sum_x (A_i * A *_{k-2} A)(x) \cdot (A_i * A *_{k-2} A)(x) + \varepsilon_1 \sum_{i,j=1}^{l} c_{A_i} c_{A_j} T_k(A) \leq$$

$$\leq \sum_{i=1}^{l} \sum_x (A_i * A *_{k-2} A)(x) \cdot (A_i * A *_{k-2} A)(x) + \varepsilon_1 T_k(A)\,.$$

Отсюда $\sum_{i=1}^{l} \sum_x (A_i * A *_{k-2} A)(x) \cdot (A_i * A *_{k-2} A)(x) \geq (1-\varepsilon_1) T_k(A)$. Аналогично

$$\sum_{i=1}^{l} \sum_{j=1}^{l} \sum_x (A_i * A_j * A *_{k-3} A)(x) \cdot (A_i * A *_{k-2} A)(x) \leq$$

$$\leq \sum_{i=1}^{l} \sum_x (A_i * A_i * A *_{k-3} A)(x) \cdot (A_i * A *_{k-2} A)(x) +$$

$$+ \sum_{i=1}^{l} \sum_{j=1,\, j\neq i}^{l} \sum_x (A * A_j * A *_{k-3} A)(x) \cdot (A_i * A *_{k-2} A)(x)$$

$$\leq \sum_{i=1}^{l} \sum_x (A_i * A_i * A *_{k-3} A)(x) \cdot (A_i * A *_{k-2} A)(x) +$$

$$+ \sum_{i=1}^{l} \sum_{j=1,\, j\neq i}^{l} \sum_x (A_i \circ A_j)(x) \cdot ((A *_{k-2} A) \circ (A *_{k-2} A))(x) \leq$$

$$\leq \sum_{i=1}^{l} \sum_x (A_i * A_i * A *_{k-3} A)(x) \cdot (A_i * A *_{k-2} A)(x) + \varepsilon_1 T_k(A)\,.$$

И так далее. Окончательно, находим

$$\sum_{i=1}^{l} T_k(A_i) = \sum_{i=1}^{l} \sum_x (A_i *_{k-1} A_i)(x) \cdot (A_i *_{k-1} A_i)(x) \geq (1 - (2k-1)\varepsilon_1) \cdot T_k(A)\,.$$

Лемма доказана.

Замечание 4.8 Из третьего пункта леммы 4.7 вытекает, что найдется индекс $i_0 \in \{1,\dots,l\}$ такой, что $|A_{i_0}| \geq (1-(2k-1)\varepsilon_1)\cdot m^{\frac{\zeta_k(A)-1}{2k-2}} \geq (1-(2k-1)\varepsilon_1)\cdot m^{1/2}$. Действительно

$$m^{\zeta_k(A)}(1-(2k-1)\varepsilon_1) \leq \sum_{i=1}^{l} T_k(A_i) \leq (\max_{i=1,\dots,l}|A_i|)^{2k-2}\sum_{i=1}^{l}|A_i| \leq (\max_{i=1,\dots,l}|A_i|)^{2k-2}m$$

откуда и вытекает требуемое неравенство. Следовательно, если положить $\beta = (1-(2k-1)\varepsilon_1)m^{-1/2}$, то *любое* множество $A \subseteq G$, $|A| = m$ является сильно (C,β)—связным порядка k, с константой $C = \varepsilon_1$, $\varepsilon_1 < 1/(2k-1)$. Поэтому нетривиальные утверждения о структуре множества A получаются, если доказать, что множество A является сильно β—связным при *достаточно больших* β.

Теорема 4.9 *Пусть $A \subseteq G$ — произвольное множество. Пусть также $\varepsilon, \beta \in (0,1)$, — действительные числа и $|A| \geq \varepsilon/(2\beta^2)$. Тогда существует разбиение A на множества $A_1,\dots,A_t$ и Ω такое, что*

1) *Все множества A_i, $i = 1,\dots,t$ являются сильно (C,β)—связными порядка 2, причем в качестве константы C можно взять любое число не превосходящее $\varepsilon\log(1/\beta)/(6\log(2|A|/\varepsilon))$.*

2) $\sum_{i=1}^{t} T_2(A_i) \geq (1-\varepsilon)\cdot T_2(A)$.

Доказательство. Пусть $m = |A|$, $s_0 = \lceil \log(2m/\varepsilon)/(2\log(1/\beta))\rceil \geq 1$ и $\varepsilon' = \varepsilon/(6s_0)$. Пусть $C \leq \varepsilon'$ — некоторое число. Доказательство теоремы 4.9 представляет собой алгоритм. Если множество A является сильно (C,β)–связным порядка 2 множеством, то доказывать нечего. Пусть теперь множество A не является сильно (C,β)–связным порядка 2 множеством. Применяя лемму 4.7 с $\varepsilon_1 = \varepsilon'$, находим разбиение $\mathcal{P}^{(1)}$ множества A на подмножества $A_1,\dots,A_l$ так, что выполненены пункты 1) — 3) леммы. Так как A не является сильно (C,β)–связным порядка 2 множеством, то для любого $i \in \{1,\dots,l\}$ выполнено $|A_i| < \beta|A|$. По пункту 3) леммы 4.7 имеем

$$\sum_{\mathcal{A}\in\mathcal{P}^{(1)}} T_2(\mathcal{A}) = \sum_{i=1}^{l} T_2(A_i) \geq (1-3\varepsilon')T_2(A)\,.$$

Пусть

$$B^{(1)} = \{A_i \text{ — не является сильно } (C,\beta)-\text{связным порядка 2}\}$$

и $G^{(1)}$ — все остальные множества A_i. Построим новое разбиение множества A. Множества A_i из $G^{(1)}$ оставим без изменения. Для каждого A_i из $B^{(1)}$ применим лемму 4.7 с $\varepsilon_1 = \varepsilon'$. Получим разбиение A_i на подмножества A_{ij}, $j \in \{1,\dots,l(i)\}$. Мы построили новое разбиение $\mathcal{P}^{(2)}$ множества A. Для любого $A_i \in B^{(1)}$ выполнено $\sum_{j=1}^{l(i)} T_2(A_{ij}) \geq (1-3\varepsilon')T_2(A_i)$. Отсюда

$$\sum_{\mathcal{A}\in\mathcal{P}^{(2)}} T_2(\mathcal{A}) \geq (1-3\varepsilon')^2\cdot T_2(A)\,. \tag{50}$$

Пусть

$$B^{(2)} = \{A_{ij} \text{ — не является сильно } (C,\beta)-\text{связным порядка 2}\}\,.$$

Для каждого A_{ij} из $B^{(2)}$ применим лемму 4.7 с $\varepsilon_1 = \varepsilon'$. Получим разбиение множеств A_{ij} на новые множества A_{ijr}. И так далее. На s–ом шаге алгоритма, мы построим разбиение $\mathcal{P}^{(s)}$ для которого

$$\sum_{\mathcal{A}\in\mathcal{P}^{(s)}} T_2(\mathcal{A}) \geq (1-3\varepsilon')^s\cdot T_2(A) \geq (1-3\varepsilon' s)\cdot T_2(A)\,. \tag{51}$$

Если для некоторого $s \le s_0$ выполнено

$$\sum_{\mathcal{A}\in\mathcal{P}^{(s)}\setminus B^{(s)}} T_2(\mathcal{A}) \ge (1-\varepsilon)\cdot T_2(A)\,, \tag{52}$$

то теорема доказана. Действительно, положив $\Omega = \bigsqcup_{\mathcal{A}\in B^{(s)}} \mathcal{A}$ мы получим разбиение A на множества $\mathcal{A} \in \mathcal{P}^{(s)} \setminus B^{(s)}$ и множество Ω для которых справедливы все утверждения теоремы. Пусть для всех $s \le s_0$ неравенство (52) не выполнено. Так как $s \le s_0$, то из (51) вытекает неравенство $\sum_{\mathcal{A}\in\mathcal{P}^{(s)}} T_2(\mathcal{A}) \ge (1-\varepsilon/2)\cdot T_2(A)$. Следовательно

$$\sum_{\mathcal{A}\in B^{(s)}} T_2(\mathcal{A}) \ge \frac{\varepsilon}{2}\cdot T_2(A) \ge \frac{\varepsilon m^2}{2}\,. \tag{53}$$

Для любого $\mathcal{A} \in B^{(s)}$ выполнено $|\mathcal{A}| < \beta^s m$. Отсюда

$$\sum_{\mathcal{A}\in B^{(s)}} T_2(\mathcal{A}) < (\beta^s m)^2 \sum_{\mathcal{A}\in\mathcal{P}^{(s)}} |\mathcal{A}| = \beta^{2s} m^3\,. \tag{54}$$

Последнее неравенство противоречит (53), если $s = s_0$. Значит, для некоторого $s < s_0$ справедливо неравенство (52). Теорема доказана.

Главное отличие результата выше от теоремы 2.12 состоит в том, что в теореме 4.9 речь идет о *разбиении* множества A на сильно β–связные компоненты и некоторое остаточное множество Ω, тогда как в теореме 2.12 доказывается существование у A лишь *одного* связного подмножества. Кроме того, из теоремы 4.9 вытекает, что остаточное множество Ω мало в смысле величины T_2. Действительно, по свойству 2) имеем $\sum_{i=1}^{t} T_2(A_i) \ge (1-\varepsilon)\cdot T_2(A)$, откуда $T_2(\Omega) \le \varepsilon T_2(A)$.

Список литературы

[1] *Balog A., Szemerédi E.* A statistical theorem of set addition // Combinatorica **14** (1994), 263–268.

[2] *Gowers W. T.* A new proof of Szemerédi's theorem for arithmetic progressions of length four // Geom. Funct. Anal. **8** (1998), 529–551.

[3] *Gowers W. T.* A new proof of Szemerédi's theorem // Geom. Funct. Anal. **11** (2001), 465–588.

[4] *Фрейман Г. А.* Основания структурной теории сложения множеств / Казанский гос. пед. инст., Казань, 1966.

[5] *Bilu Y.* Structure of sets with small sumset // Structure Theory of Sets Addition, Astérisque, Soc. Math. France, Montrouge **258** (1999), 77–108.

[6] *Ruzsa I.* Generalized arithmetic progressions and sumsets // Acta Math. Hungar. **65** (1994), 379–388.

[7] *Chang M.–C.,* A polynomial bound in Freiman's theorem // Duke Math. J. **113** (2002) no. 3, 399–419.

[8] *Elekes G., Ruzsa I.* The structure of sets with few sums along a graph // http://www.cs.elte.hu/ elekes/Abstracts/alag.ps, представлено в печать.

[9] *Ruzsa I.* An analog of Freiman's theorem in groups // Structure theory of set addition // Astérisque No. **258** (1999), 323–326.

[10] *Green B., Ruzsa I.* An analoge of Freiman's theorem in an arbitrary abelian group // J. London Math. Soc., представлено в печать.

[11] *Green B.* Spectral structure of sets of integers // Fourier analysis and convexity (survey article, Milan 2001), Appl. Numer. Harmon. Anal., Birkhauser Boston, Boston, MA (2004), 83–96.

[12] *Green B.* Finite field model in additive combinatorics // Surveys in Combinatorics 2005, LMS Lecture Notes **329**, 1–29.

[13] *Green B.* The polynomial Freiman–Ruzsa conjecture // http:// www.dpmms.cam.ac.uk./ bjg23.

[14] *Green B.* Boolean functions with small spectral norm // Geom. Funct. Anal., представлено в печать.

[15] *Green B.* An inverse theorem for the Gowers U^3–norm, with applications // Proc. Edin. Math. Soc., представлено в печать.

[16] *Green B.* A note on the Freiman and Balog–Szemerédi–Gowers theorems in finite fields // http:// www.arXiv:math.CO/0701585 v1, представлено в печать.

[17] *Sanders T.* A note on Freiman's theorem in vector spaces // http://www.arXiv:math.NT/0605523.

[18] *Rudin W.* Fourier analysis on groups / Wiley 1990 (репринт издания 1962 года).

[19] *Rudin W.* Trigonometric series with gaps // J. Math. Mech. **9** (1960), 203–227.

[20] *Bourgain J., Konygin S.* Estimates for the number of sums and products and for exponential sums over subgroups in fields of prime order // C. R. Acad. Sci. Paris, Ser. I **337** (2003), 75–80.

[21] *Tao T., Vu V.* Additive combinatorics / Cambridge University Press 2006.