О суммах диссоциативных множеств *

Шкредов И.Д.

Аннотация.

Эта работа посвящена изучению подмножеств Q сумм диссоциативных множеств. Мы находим точную верхнюю оценку для количества решений уравнения

$$q_1 + \dots + q_p = q_{p+1} + \dots + q_{2p}\,, \quad q_i \in Q \tag{1}$$

в группе $\mathbf{F}_2^n$. Наш подход позволяет легко получить последний результат Ж. Бургена о множествах больших тригонометрических сумм и даже немного усилить его. Кроме того, в работе рассматривается обратная задача. Пусть множество Q принадлежит сумме диссоциативных множеств и имеет большое число решений уравнения (1). Оказывается, что тогда большая часть Q является чрезвычайно структурированным множеством.

1. Введение.

Пусть $G = (G, +)$ — конечная абелева группа с аддитивной групповой операцией $+$. Пусть A — подмножество G. Очень удобно обозначить через $A(x)$ характеристическую функцию этого множества. Иными словами $A(x) = 1$, если $x \in A$ и $A(x) = 0$ иначе. Обозначим через $\widehat{G}$ двойственную группу для G. Иными словами пусть $\widehat{G}$ — группа гомоморфизмов ξ из G в $\mathbf{T}$, $\xi : x \to \xi \cdot x$. Хорошо известно, что группа $\widehat{G}$ — изоморфна G. Обозначим через N мощность G. Пусть $f : G \to \mathbb{C}$ — произвольная функция. Преобразование Фурье функции f задается формулой

$$\widehat{f}(r) = \sum_{x \in G} f(x) e(-r \cdot x)\,, \tag{2}$$

где $e(x) = e^{2\pi i x}$ и $r \in \widehat{G}$.

Пусть δ, α — действительные числа, $0 < \alpha \le \delta \le 1$ и пусть A — некоторое подмножество G мощности δN. Рассмотрим множество $\mathcal{R}_\alpha$ больших тригонометрических сумм A

$$\mathcal{R}_\alpha = \mathcal{R}_\alpha(A) = \{\ r \in \widehat{G}\ :\ |\widehat{A}(r)| \ge \alpha N\ \}\,. \tag{3}$$

Для многих задач комбинаторной теории чисел важно знать структуру множества $\mathcal{R}_\alpha$ (см. [1]). Иными словами, какими нетривиальными свойствами обладает множество $\mathcal{R}_\alpha$?

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

Ясно, что вопрос о строении $\mathcal{R}_\alpha$ относится к обратным задачам аддитивной теории чисел (см. [2, 24]).

Первый нетривиальный результат о структуре множеств больших тригонометрических сумм был получен М.–Ч. Чанг [6] в 2002 году. Напомним, что множество $\mathcal{D} = \{d_1, \dots, d_{|\mathcal{D}|}\} \subseteq G$ называется *диссоциативным*, если из равенства

$$\sum_{i=1}^{|\mathcal{D}|} \varepsilon_i d_i = 0 \pmod N, \tag{4}$$

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

Обозначим через $\log$ логарифм по основанию два. Пусть p — натуральное число. Через $[p]$ обозначим отрезок натурального ряда $\{1, \dots, p\}$.

Теорема 1.1 (Чанг) *Пусть δ, α — действительные числа, $0 < \alpha \le \delta \le 1$, A — произвольное подмножество G мощности δN и множество $\mathcal{R}_\alpha$ определено равенством (3). Тогда любое диссоциативное множество Λ, $\Lambda \subseteq \mathcal{R}_\alpha$ имеет мощность не больше $2(\delta/\alpha)^2 \log(1/\delta)$.*

Простое применение равенства Парсеваля дает следующую оценку на мощность множества Λ : $|\Lambda| \le \delta/\alpha^2$. Отсюда легко видеть, что теорема Чанг нетривиальна когда величина δ мала.

Развивая подход из [5] (см. также [4]) Чанг применила свой результат в доказательстве количественного варианта знаменитой теоремы Г.А. Фреймана [3] о множествах с маленькой суммой. Другие приложения теоремы 1.1 получил Б. Грин в статье [7], Б. Грин и Имре Ружа в [9], Т. Сандерс (см., например, [12, 13, 14]), а также Т. Чоен в [23]. Вопрос о структуре множества $\mathcal{R}_\alpha$, когда параметр α близок к δ, изучался в работах [17, 18, 19], см. также обзор [20].

В работе [26] Ж. Бурген получил аналог теоремы Чанг на случай нескольких сумм диссоциативного множества Λ и применил его для доказательства своего замечательного результата о плотности подмножеств $[N]$, не содержащих прогрессий длины три. Дальнейшие приложения теоремы ниже были получены в работе [15].

Обозначим через $A_1 \dot{+} A_2 \dot{+} \dots \dot{+} A_d$ множество, образованное суммой различных элементов из множеств $A_1, \dots, A_d$. Множество, состоящее из суммы d различных элементов множества A обозначим через $d\dot{A}$.

Теорема 1.2 (Бурген) *Пусть d — натуральное число, δ, α — действительные числа, $0 < \alpha \le \delta \le 1$, A — произвольное подмножество G мощности δN и множество $\mathcal{R}_\alpha$ определено равенством (3). Пусть также Λ — диссоциативное множество. Тогда для всех $d \ge 1$ выполнено $|d\dot{\Lambda} \bigcap \mathcal{R}_\alpha| \le 8(\delta/\alpha)^2 \log^d(1/\delta)$.*

В статьях [28, 29] были получены другие результаты о множествах больших тригонометрических сумм. В частности, там была доказана следующая теорема.

Теорема 1.3 *Пусть δ, α — действительные числа, $0 < \alpha \le \delta$, A — произвольное подмножество $\mathbb{Z}_N$ мощности δN, $k \ge 2$ — натуральное число и множество $\mathcal{R}_\alpha$ определено равенством (3). Пусть также $B \subseteq \mathcal{R}_\alpha \setminus \{0\}$ — произвольное множество. Тогда величина*

$$T_k(B) := |\{ \ (r_1, \dots, r_k, r'_1, \dots, r'_k) \in B^{2k} \ : \ r_1 + \dots + r_k = r'_1 + \dots + r'_k \ \}| \tag{5}$$

не меньше, чем

$$\frac{\delta \alpha^{2k}}{2^{4k} \delta^{2k}} |B|^{2k} . \tag{6}$$

Если не обращать внимание на абсолютные константы, появляющиеся в оценках для мощности диссоциативного множества Λ, то как было показано в работе [29], из теоремы 1.3 и известного неравенства В. Рудина [21, 22] о диссоциативных множествах, вытекает теорема М.–Ч. Чанг. В настоящей статье мы показываем, что подходящий аналог результата Рудина и теорема 1.3 дает теорему 1.2 (см. параграф 2). Наш подход элементарен и не требует довольно сложной техники из [26], связанной с гиперсжимаемостью. Мы показываем, что для любого множества $Q \subseteq d\dot{\Lambda}$, Λ — диссоциативное, величина $T_k(Q)$ не превосходит $C^{dk}k^{dk}|Q|^k$, где $C > 0$ — абсолютная константа. Применяя полученное утверждение к множеству $d\dot{\Lambda} \bigcap \mathcal{R}_\alpha$ и используя теорему 1.3, получаем теорему 1.2. На самом деле наш подход позволяет чуть усилить последний результат (см. теорему 2.9).

В параграфе 4 мы рассматриваем обратную задачу в ситуации когда $d = 2$. Пусть множество Q принадлежит $2\dot{\Lambda}$, где множество Λ — диссоциативное. Предположим, что величина $T_k(Q)$ по порядку совпадает со своим максимальным значением. Что можно сказать о строении Q? Оказывается, в этом случае, множество Q содержит сумму двух диссоциативных множеств (см. теорему 4.9). В некотором смысле нами получено полное описание всех подмножеств $2\dot{\Lambda}$ с большое величиной T_k.

Мы доказываем наши результаты в группе $\mathbf{F}_2^n$, хотя они могут быть перенесены и на случай произвольных абелевых групп (плодотворность подхода, при котором используются группы $\mathbf{F}_p^n$, p — простое, обсуждается в обзоре [11]). Мы планируем получить соответствующие обощения в наших последующих статьях.

Автор выражает благодарность доктору физико–математических наук, профессору Н. Г. Мощевитину, а также доктору физико–математических наук, профессору С. В. Конягину за внимание к работе и полезные обсуждения.

2. Элементарное доказательство одного результата Бургена.

Обозначим через G группу $\mathbf{F}_2^n$. Пусть $A \subseteq G$ — произвольное множество и $k \geq 2$ — натуральное число. Обозначим через $T_k(A)$ число решений уравнения

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

Если $A_1, \dots, A_{2k} \subseteq G$ — некоторые множества, то через $T_k(A_1, \dots, A_{2k})$ обозначим число решений уравнения

$$T_k(A_1, \dots, A_{2k}) := |\{a_1 + \dots + a_k = a_{k+1} + \dots + a_{2k} \ : \ a_i \in A_i, \, i = 1, \dots, 2k\}| \, .$$

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

Выразим величину $T_k(A)$ в терминах свертки.

Определение 2.1 Пусть $f, g \ : \ G \to \mathbb{C}$ — произвольные функции. Обозначим через $(f * g)(x)$ функцию

$$(f * g)(x) = \sum_s f(s) g(x - s) \, . \qquad (7)$$

Ясно, что $(f * g)(x) = (g * f)(x)$, $x \in G$. Далее, определим по индукции операцию $*_k$, где k — натуральное число, $*_k = *(*_{k-1})$.

Если $A, B \subseteq G$ — произвольные множества, то $(A * B)(x) \neq 0$ тогда и только тогда, когда $x \in A + B$. Отсюда $T_2(A) = \sum_x (A * A)^2(x)$. Пусть $f : G \to \mathbb{C}$ — произвольная функция. Через $T_k(f)$ обозначим величину $T_k(f) = \sum_x |(f *_{k-1} f)(x)|^2$. Справедлива лемма.

Лемма 2.2 *Пусть s,t — натуральные числа, $s \geq 2$, $t \geq 2$ и пусть $f_1, \dots, f_s, g_1, \dots, g_t : G \to \mathbb{R}$ — некоторые функции. Тогда*

$$\left| \sum_x (f_1 * \dots * f_s)(x) \cdot (g_1 * \dots * g_t)(x) \right| \leq$$

$$\leq (T_s(f_1))^{1/2s} \dots (T_s(f_s))^{1/2s} (T_t(g_1))^{1/2t} \dots (T_t(g_t))^{1/2t} . \qquad (8)$$

Доказательство. Так как $\widehat{(f * g)}(r) = \widehat{f}(r)\widehat{g}(r)$, то

$$\sigma := \sum_x (f_1 * \dots * f_s)(x) \cdot (g_1 * \dots * g_t)(x) = \frac{1}{N} \sum_r \widehat{f_1}(r) \dots \widehat{f_s}(r) \overline{\widehat{g_1}(r)} \dots \overline{\widehat{g_t}(r)} .$$

Применяя несколько раз неравенство Гельдера, находим

$$\sigma \leq \left(\frac{1}{N} \sum_r |\widehat{f_1}(r)|^{2s} \right)^{\frac{1}{2s}} \dots \left(\frac{1}{N} \sum_r |\widehat{f_s}(r)|^{2s} \right)^{\frac{1}{2s}} \cdot$$

$$\cdot \left(\frac{1}{N} \sum_r |\widehat{g_1}(r)|^{2t} \right)^{\frac{1}{2t}} \dots \left(\frac{1}{N} \sum_r |\widehat{g_t}(r)|^{2t} \right)^{\frac{1}{2t}} =$$

$$= (T_s(f_1))^{1/2s} \dots (T_s(f_s))^{1/2s} (T_t(g_1))^{1/2t} \dots (T_t(g_t))^{1/2t}$$

Лемма доказана.

Следствие 2.3 *Пусть A, B — произвольные конечные подмножества группы G. Тогда*

$$T_k^{1/2k}(A \cup B) \leq T_k^{1/2k}(A) + T_k^{1/2k}(B) . \qquad (9)$$

Нам понадобится понятие диссоциативности в группе $\mathbf{F}_2^n$.

Определение 2.4 Пусть $R \subseteq \mathbb{F}_2^n$ — некоторое множество, $R = -R$ и $\{0\} \in R$. Множество $\Lambda = \{\lambda_1, \dots, \lambda_{|\Lambda|}\} \subseteq \mathbb{F}_2^n$ принадлежит семейству $\mathbf{\Lambda}_R(k)$, если из включения

$$\sum_{i=1}^{|\Lambda|} \varepsilon_i \lambda_i \in R , \qquad (10)$$

где $\varepsilon_i \in \{-1, 0, 1\}$ и $\sum_{i=1}^{|\Lambda|} |\varepsilon_i| \leq k$ вытекает, что все ε_i равны нулю. Если $R = \{0\}$, то множество Λ принадлежит семейству $\mathbf{\Lambda}(k)$.

Предложение 2.5 *Пусть k — натуральное число, $k \geq 2$ и $\Lambda \subseteq \mathbf{F}_2^n$ — произвольное множество из семейства $\mathbf{\Lambda}(2k)$. Тогда для всех натуральных p, $2 \leq p \leq k$ выполнено*

$$T_p(\Lambda) \leq p^p |\Lambda|^p . \qquad (11)$$

Доказательство. Пусть $m = |\Lambda|$. Рассмотрим уравнение

$$\lambda_1 + \dots + \lambda_{2p} = 0, \quad \lambda_i \in \Lambda, \quad i = 1, \dots, 2p . \qquad (12)$$

Рассмотрим также всевозможные разбиения $\mathcal{M} = \{M_1, \dots, M_p\}$ отрезка $[2p]$ на множества M_j, $|M_j| = 2$, $j = 1, \dots, p$. Легко видеть, что число таких разбиений равно $\frac{(2p)!}{2^p p!} \leq \frac{(2p)^p}{2^p} = p^p$. Сопоставим, дополнительно, каждому множеству M_j некоторый элемент $\lambda^{(j)}$ из множества Λ. Тогда число полученных *отмеченных* разбиений не

превосходит $p^p m^p$. Поскольку множество Λ принадлежит семейству $\mathbf{\Lambda}(2k)$, то в произвольном решении уравнения (12) любое λ_i, $i \in [2p]$ встречается четное число раз. Каждому решению $(\lambda_1, \dots, \lambda_{2p})$ уравнения (12) можно сопоставить отмеченное разбиение $\mathcal{M}' = \{(M_1, \lambda^{(1)}), \dots, (M_p, \lambda^{(p)})\}$. Действительно, построим отмеченное разбиение $\mathcal{M}' = \{(M_1, \lambda^{(1)}), \dots, (M_p, \lambda^{(p)})\}$ так чтобы для каждого $M_j = \{\alpha, \beta\}$, $j = 1, \dots, p$ было выполнено $\lambda_\alpha = \lambda_\beta = \lambda^{(j)}$. Ясно, что различным решениям уравнения (12) соответствуют различные отмеченные разбиения. Отсюда общее число решений (12) не превосходит $p^p m^p$. Предложение доказано.

Замечание 2.6 Теорема Рудина (см. [21, 22]) утверждает, что для произвольной функции $f : G \to \mathbb{C}$, $\operatorname{supp} \widehat{f} \subseteq \Lambda$, Λ — диссоциативное выполнено $\|f\|_k \le C\sqrt{k}\|f\|_2$, где $C > 0$ — некоторая абсолютная константа и $k \ge 2$. Иными словами, для любых чисел a_λ выполнено

$$\frac{1}{N}\sum_x \left|\sum_{\lambda\in\Lambda} a_\lambda e(-\lambda\cdot x)\right| \le C^k k^{k/2}\left(\sum_{\lambda\in\Lambda}|a_\lambda|^2\right)^{k/2}. \qquad (13)$$

Безусловно, из неравенства (13) вытекает предложение 2.5 : достаточно взять $k = 2p$ и положить $a_\lambda = 1$. С другой стороны, для доказательства (13) можно применить чуть модифицированные рассуждения из предложения 2.5. Действительно, чтобы убедиться в справедливости (13) нам необходимо найти число решений уравнения (12), причем каждое решение берется с весом $a_{\lambda_1}\dots a_{\lambda_{2p}}$. Поскольку множество Λ принадлежит семейству $\mathbf{\Lambda}(2k)$, то в произвольном решении уравнения (12) любое λ_i, $i \in [2p]$ встречается четное число раз. Следовательно, при фиксированном разбиении $\mathcal{M} = \{M_1, \dots, M_p\}$ отрезка $[2p]$ на множества M_j, $|M_j| = 2$, $j = 1, \dots, p$ мы получим вес $\left(\sum_{\lambda\in\Lambda}|a_\lambda|^2\right)^p$. Так как количество разбиений $\mathcal{M}$ не превосходит p^p, то мы доказали (13) в случае когда $k = 2p$. Применяя обычные рассуждения (см., например, [10], лемма 19), мы устанавливаем (13) для всех остальных $k \ge 2$.

Мы докажем аналог предложения 2.5 для подмножеств сумм диссоциативных множеств. Именно это утверждение и поможет нам получить теорему 2.9.

Предложение 2.7 *Пусть k, d — натуральные числа, $k \ge 2$ и $\Lambda \subseteq \mathbf{F}_2^n$ — произвольное множество из семейства $\mathbf{\Lambda}(2dk)$ такое, что $|\Lambda| \ge 4d^2$. Пусть также Q — некоторое подмножество $d\dot{\Lambda}$. Тогда для всех натуральных p, $2 \le p \le k$ выполнено*

$$T_p(Q) \le 2^{8dp} p^{dp} |Q|^p . \qquad (14)$$

Доказательство. Мы доказываем предложение 2.7 по индукции. Если $d = 1$, то оценка величины $T_p(Q)$ была получена в предложении 2.5. Пусть $d \ge 2$ и пусть $m = |Q|$. Положим $c_d := 8d$, $d \ge 1$.

Пусть $a = [|\Lambda|/2d]$. По условию $|\Lambda| \ge 4d^2$. Отсюда $|\Lambda|/a \le 4d$. Кроме того

$$\binom{|\Lambda|-d}{a-1}^{-1}\binom{|\Lambda|}{a} = \frac{|\Lambda|(|\Lambda|-1)\dots(|\Lambda|-d+1)}{a(|\Lambda|-a)(|\Lambda|-a-1)\dots(|\Lambda|-a-d+2)} \le$$

$$\le 4d\cdot e^{\frac{1}{|\Lambda|}\left(\sum_{i=1}^{d-1} i + 2\sum_{i=0}^{d-2}(a+i)\right)} \le 2^4 d . \qquad (15)$$

Пусть для произвольного множества E символ E^c означает $\Lambda \setminus E$. Пользуясь диссоциативностью множества Λ и определением операции $\dot{+}$, получаем

$$Q(x) = d^{-1}\binom{|\Lambda|-d}{a-1}^{-1} \sum_{\Lambda_0\subseteq\Lambda,\,|\Lambda_0|=a} \left(Q\bigcap(\Lambda_0 + (d-1)\dot{\Lambda}_0^c\right)(x) .$$

Применяя неравенство Гельдера, находим

$$T_p(Q) \le d^{-2p}\binom{|\Lambda|-d}{a-1}^{-2p}\binom{|\Lambda|}{a}^{2p-1}\sum_{\Lambda_0\subseteq\Lambda,\,|\Lambda_0|=a} T_p(Q\bigcap(\Lambda_0+(d-1)\dot\Lambda_0^c)\,. \qquad (16)$$

Если мы докажем, что для любого $\Lambda_0 \subseteq \Lambda$ выполнено

$$T_p(Q\bigcap(\Lambda_0+(d-1)\dot\Lambda_0^c) \le 2^{c_{d-1}p}p^{dp}|Q\bigcap(\Lambda_0+(d-1)\dot\Lambda_0^c|^p\,,$$

то подставляя это неравенство в (16) и используя (15), мы получим

$$T_p(Q) \le d^{-2p}\binom{|\Lambda|-d}{a-1}^{-2p}\binom{|\Lambda|}{a}^{2p}2^{c_{d-1}p}p^{pd}m^p \le 2^{(c_{d-1}+8)p}p^{pd}m^p = 2^{c_dp}p^{pd}m^p$$

и предложение 2.7 будет доказано.

Пусть $\Lambda_1 = \tilde\Lambda$, $\Lambda_2 = \Lambda \setminus \tilde\Lambda$ и $Q' \subseteq \Lambda_1 + (d-1)\dot\Lambda_2$. Требуется доказать, что $T_p(Q') \le 2^{c_{d-1}p}p^{pd}|Q'|^p$. Пусть λ — произвольный элемент из Λ_1. Рассмотрим множества

$$D_\lambda = D(\lambda) = \{\ \lambda'\ :\ \lambda \dotplus \lambda' \in Q',\ \lambda' \in (d-1)\dot\Lambda_2\ \}\,,$$

$$Q_\lambda = Q(\lambda) = \{\ q \in Q'\ :\ q = \lambda \dotplus \lambda_2' \dotplus \dots \dotplus \lambda_d',\quad \lambda_i' \in \Lambda,\ i = 2,\dots,d\ \}\,,$$

Ясно, что $Q(\lambda) = D(\lambda)+\lambda$. Пусть s_1 — число непустых множеств D_λ. Пусть это множества $D_{\lambda_1},\dots,D_{\lambda_{s_1}}$. Иногда, для краткости, мы будем писать D_j вместо D_{λ_j}. Пусть также $s_2 = |\Lambda_2|$. Ясно, что $Q \subseteq \{\lambda_1,\dots,\lambda_s\} + (d-1)\dot\Lambda_2$

Рассмотрим уравнение

$$q_1 + \dots + q_p = q_{p+1} + \dots + q_{2p}\,, \qquad (17)$$

где $q_i \in Q'$, $i = 1,\dots,2p$. Обозначим через σ число решений уравнения (17). Так как $Q' \subseteq \Lambda_1 + (d-1)\dot\Lambda_2$, то для всех $q \in Q'$ выполнено $q = \lambda + \mu$, где $\lambda \in \Lambda_1$, $\mu \in (d-1)\dot\Lambda_2$.

Пусть $i_1,\dots,i_{2p} \in [s_1]$ — произвольные числа. Обозначим через $\sigma_{\vec i}$, $\vec i = (i_1, i_2, \dots, i_{2p})$ — множество решений уравнения (17) таких, что для всех $j \in [2p]$ имеет место ограничение $q_j \in D(\lambda_{i_j})$, $\lambda_{i_j} \in \Lambda_1$. По условию множества Λ_1 и Λ_2 принадлежат семейству $\mathbf{\Lambda}(2dk)$ и не пересекаются. Отсюда следует, что если $q_1,\dots,q_{2p}$ — решение уравнения (17), принадлежащее множеству $\sigma_{\vec i}$, то любой компонент вектора $\vec i$ встречается в этом векторе четное число раз. Имеем

$$\sigma \le \sum_{\mathcal{M},\,\mathcal{M}=\{M_1,\dots,M_r\},\,[2p]=M_1\bigsqcup\dots\bigsqcup M_p}\ \sum_{\vec i\in\mathcal{M}} |\sigma_{\vec i}|\,. \qquad (18)$$

Суммирование в правой части (18) проходит по семействам множеств $\mathcal{M}, \mathcal{M} = \{M_1,\dots,M_p\}$, $[2p] = M_1\bigsqcup\dots\bigsqcup M_p$ так, что для всех $j = 1,\dots,p$ выполнено $|M_j| = 2$. Пусть $M_j = \{\alpha_1^{(j)}, \alpha_2^{(j)}\}$, $j = 1,\dots,p$. По определению $\vec i \in \mathcal{M}$, если для всех $j \in [p]$ выполнено $i_{\alpha_1^{(j)}} = i_{\alpha_2^{(j)}}$.

Применяя лемму 2.2 и индукционное предположение, находим

$$|\sigma_{\vec i}| \le 2^{c_{d-1}}p^{d(p-1)}\prod_{j=1}^{2p}|D(\lambda_{i_j})|^{1/2}\,.$$

Отсюда

$$\sigma \le 2^{c_{d-1}} p^{d(p-1)} \sum_{\mathcal{M}} \sum_{\vec{i}\in\mathcal{M}} \prod_{j=1}^{2p} |D(\lambda_{i_j})|^{1/2} . \qquad (19)$$

Пусть $m' = |Q'|$ и пусть q — произвольный элемент множества Q'. Используя условие $\Lambda_1 \bigcap \Lambda_2 = \emptyset$ и диссоциативность множества Λ, легко видеть, что множества $Q(\lambda)$ не пересекаются. Отсюда

$$\sum_{\lambda\in\Lambda_1} |D(\lambda)| = \sum_{\lambda\in\Lambda_1} |Q(\lambda)| = m' . \qquad (20)$$

Для любого $\lambda \in \Lambda_1$ имеем $|D_\lambda| \le m'$. Пусть $x \ge 1$ — любое число. Используя равенство (20), получаем

$$\sum_{\lambda\in\Lambda_1} |D(\lambda)|^x = \sum_{\lambda\in\Lambda_1} |Q(\lambda)|^x \le (m')_2^{x-1} \sum_{\lambda\in\Lambda_1} |Q(\lambda)| = (m')^x . \qquad (21)$$

Число разбиений $\mathcal{M}$ в неравенстве (19) не превосходит p^p. Так как любой компонент вектора $\vec{i}$ встречается в этом векторе четное число раз, то объединяя неравенство (19) и оценку (21), находим $\sigma \le 2^{c_{d-1}} p^{dp} (m')^p$. Предложение доказано.

Легко видеть, что если не обращать внимание на константы, то предложение выше — не улучшаемо.

Предложение 2.8 *Пусть k, d — натуральные числа и $\Lambda \subseteq \mathbf{F}_2^n$ принадлежит семейству $\mathbf{\Lambda}(2d)$. Пусть также Λ_1 — произвольное подмножество Λ и $Q = d\dot{\Lambda}_1 \subseteq d\dot{\Lambda}$. Тогда для всех $k \le |\Lambda_1|/(2d)$ и всех $2 \le p \le k$ выполнено $T_p(Q) \ge 2^{-3pd} p^{pd} |Q|^p$.*

Доказательство. Рассмотрим уравнение

$$q_1 + \cdots + q_p = q_{p+1} + \cdots + q_{2p} , \qquad (22)$$

где $q_i \in Q$, $i = 1, \ldots, 2p$. Докажем, что уравнение (22) имеет не менее $2^{-3pd} p^{pd} |Q|^p$ решений. Так как $q_i \in Q$, то $q_i = \sum_{j=1}^d \lambda_j^{(i)}$, $i = 1, \ldots, 2p$. Рассмотрим наборы $(q_1, \ldots, q_p)$ такие, что *все* $\lambda_j^{(i)}$ в разложении этих q_i — различны. Ясно, что существует ровно $\binom{|\Lambda_1|}{pd} \frac{(pd)!}{(d!)^p}$ таких наборов. Для каждого набора $(q_1, \ldots, q_p)$ существует не менее $\frac{(pd)!}{(d!)^p}$ решений уравнения (22). Действительно, число способов разбить множество $\{\lambda_1^{(1)}, \ldots, \lambda_d^{(1)}, \ldots, \lambda_1^{(p)}, \ldots, \lambda_d^{(p)}\} = \{\lambda_1, \ldots, \lambda_{pd}\}$ на p множеств $M_1, \ldots, M_p$ равной мощности равно $\frac{(pd)!}{(d!)^p}$. Полагая $q_i = \sum_{j\in M_i} \lambda_j$, $i = p+1, \ldots, 2p$, получаем набор $(q_{p+1}, \ldots, q_{2p}) \in Q^p$ такой, что $q_1 + \cdots + q_p = q_{p+1} + \cdots + q_{2p}$. По диссоциативности Λ каждому набору множеств $M_1, \ldots, M_p$ однозначным образом соответствует набор $(q_{p+1}, \ldots, q_{2p})$. Отсюда $T_p(Q) \ge \binom{|\Lambda_1|}{pd} \frac{(pd)!}{(d!)^p} \cdot \frac{(pd)!}{(d!)^p}$. Так как $\Lambda \in \mathbf{\Lambda}(2d)$, то $|Q| = \binom{|\Lambda_1|}{d}$. Применяя неравенство $2kd \le |\Lambda_1|$, находим

$$T_p(Q) \ge \binom{|\Lambda_1|}{pd} \frac{(pd)!}{(d!)^p} \cdot \frac{(pd)!}{(d!)^p} \ge 2^{-pd} \frac{(pd)!}{(d!)^p} |Q|^p \ge 2^{-3pd} p^{pd} |Q|^p .$$

Предложение доказано.

В завершении этого параграфа мы покажем, что если не обращать внимания на константы, то в случае $G = \mathbf{F}_2^n$ теорема 1.2 вытекает из теоремы 1.3 (точнее ее аналога — теоремы 5.1 из добавления) и предложения 2.7.

Теорема 2.9 *Пусть δ, α — действительные числа, $0 < \alpha \le \delta \le 1/4$, d — натуральное число, $d \le \log(1/\delta)/4$, A — произвольное подмножество $\mathbf{F}_2^n$ мощности δN и множество $\mathcal{R}_\alpha$ определено равенством (3). Пусть также множество $\Lambda \subseteq \mathbf{F}_2^n$ принадлежит семейству $\mathbf{\Lambda}(2\log(1/\delta))$. Тогда для всех $1 \le d \le \log(1/\delta)/4$ выполнено*

$$|d\dot{\Lambda} \bigcap \mathcal{R}_\alpha| \le \left(\frac{\delta}{\alpha}\right)^2 \left(\frac{2^{12}\log(1/\delta)}{d}\right)^d . \tag{23}$$

Доказательство. Пусть $k = [\ln(1/\delta)/d] \ge 2$, $Q = d\dot{\Lambda} \bigcap \mathcal{R}_\alpha$ и $m = |Q|$. Требуется доказать, что $m \le (\delta/\alpha)^2 (\frac{2^{12}\log(1/\delta)}{d})^d$. Применяя теорему 5.1, получаем

$$T_k(Q) \ge \frac{\delta\alpha^{2k}}{\delta^{2k}} m^{2k} . \tag{24}$$

С другой стороны, из предложения 2.7 вытекает, что $T_k(Q) \le 2^{8kd} k^{kd} m^k$. Объединяя последнее неравенство и оценку (24), находим $m \le (\delta/\alpha)^2 (\frac{2^{12}\log(1/\delta)}{d})^d$. Теорема доказана.

В теореме 2.9 доказана верхняя оценка для величины $|d\dot{\Lambda} \bigcap \mathcal{R}_\alpha|$. Следующее простое предложение дает нижнюю оценку этой величины. Оказывается, что эта нижняя оценка почти совпадает с верхней.

Предложение 2.10 *Пусть δ — действительное число, $1/N \le \delta \le 1/16$ и $\alpha = 2^{-12}\delta/\sqrt{n}$, $n \ge 32$. Существует множество $A \subseteq \mathbf{F}_2^n$, $\delta N \le |A| \le 8\delta N$ и диссоциативное множество $\Lambda \subseteq \mathcal{R}_\alpha(A)$ такие, что для всех целых $d \ge 1$ выполнено*

$$|d\dot{\Lambda} \bigcap \mathcal{R}_\alpha| \ge 2^{-30} \left(\frac{\delta}{\alpha}\right)^2 \left(\frac{\log(1/\delta)}{16d}\right)^{d-1} . \tag{25}$$

Доказательство. Пусть $\vec{e}_1 = (1, 0, \dots, 0), \dots, \vec{e}_n = (0, \dots, 0, 1)$ — стандартный базис в $\mathbf{F}_2^n$. Пусть также $k = [\log 1/(4\delta)]$ и $H, H^\perp$ — подпространства, натянутые на вектора $\vec{e}_1, \dots, \vec{e}_{n-k}$ и $\vec{e}_{n-k+1}, \dots, \vec{e}_n$, соответственно. Пусть $A \subseteq H$ — множество тех $\vec{x} = (x_1, \dots, x_n)$ из H, для которых число $x_i = 1$, $i = 1, \dots, n-k$ не меньше $(n-k)/2$. Ясно, что $|A| \ge 2^{n-k-2} \ge \delta N$ и $|A| \le |H| \le 2^{n-k} \le 8\delta N$. Пусть H' — пространство, натянутое на вектора длины $n-k$, а именно, $(1, 0, \dots, 0), \dots, (0, \dots, 0, 1)$. Пусть также $n' = n-k$ и $A' \subseteq H'$ — ограничение множества A на H'. Найдем коэффициенты Фурье множества A'. Имеем

$$\widehat{A'}(r) = \sum_x A'(x)(-1)^{<r,x>} = |A' \bigcap H_r^{(0)}| - |A' \bigcap H_r^{(1)}| = 2|A' \bigcap H_r^{(0)}| - |A'| , \tag{26}$$

где $H_r^{(0)} = \{x \in H' \ : < r, x >= 0\}$ и $H_r^{(1)} = \{x \in H' \ : < r, x >= 1\}$. Пусть $l \ge 0$ — целое число. Рассмотрим множества

$$\mathcal{H}_l = \{x = (x_1, \dots, x_{n'}) \ : \ \#x_i = 1 \text{ в точности равно } l\} .$$

Пусть $r \in \mathcal{H}_1$. Полагая $\binom{x}{y} = 0$, для $y > x$, применяя формулу Стирлинга, а также формулу (26), получаем

$$|\widehat{A'}(r)| = \left| \sum_{s=\lceil n'/2 \rceil}^{n'} \left(2\binom{n'-1}{s} - \binom{n'}{s}\right) \right| = \sum_{s=\lceil n'/2 \rceil}^{n'} \left(\frac{2s-n'}{n'}\right) \binom{n'}{s} \ge$$

$$\geq \sum_{s=\lceil n'/2+\sqrt{n'}/2\rceil}^{\lceil n'/2+\sqrt{n'}\rceil} \binom{2s-n'}{n'}\binom{n'}{s} \geq e^{-8}\frac{1}{2\sqrt{\pi}}\frac{2^{n'}}{\sqrt{n'}} \geq 2^{-14}\,\frac{2^{n'}}{\sqrt{n'}} \geq 2^{-12}\,\frac{\delta N}{\sqrt{n}}\,. \qquad (27)$$

Легко видеть, что для всякого $r \in H'$ и любого $h^\perp \in H^\perp$ выполнено $\widehat{A}(r+h^\perp) = \widehat{A'}(r)$. Отсюда $\mathcal{H}_1 + H^\perp \subseteq \mathcal{R}_\alpha(A)$ с $\alpha = 2^{-12}\delta/\sqrt{n}$ и $|\mathcal{R}_\alpha(A)| \geq n'2^k \geq n/(16\delta) \geq 2^{-28}\cdot\delta/\alpha^2$. Таким образом, нижняя оценка на мощность множества $\mathcal{R}_\alpha(A)$, по–порядку, близка к оценке сверху — δ/α^2. Пользуясь инвариантностью множества A' относительно перестановок координат, можно, имея некоторые ограничения на параметры, показать, что не только выполнено включение $(\{0\}\sqcup\mathcal{H}_1)+H^\perp \subseteq \mathcal{R}_\alpha(A)$, но и, более того, $\mathcal{R}_\alpha(A) = (\{0\}\sqcup\mathcal{H}_1)+H^\perp$. В дальнейшем нам не понадобится этот факт.

Пусть $\Lambda = \{\vec{e}_1,\dots,\vec{e}_n\} \subseteq \mathcal{R}_\alpha(A)$ и $\Lambda^* = \{\vec{e}_{n-k+1},\dots,\vec{e}_n\}$. Ясно, что $\bigsqcup_{h_1\in\mathcal{H}_1}(h_1 + (d-1)\dot{\Lambda}^*) \subseteq \mathcal{R}_\alpha(A)\bigcap d\dot{\Lambda}$. Отсюда

$$|\mathcal{R}_\alpha(A)\bigcap d\dot{\Lambda}| \geq n'\binom{k}{d-1} \geq \frac{n}{4}\cdot\frac{k^{d-1}}{d^{d-1}e^{d-1}} \geq 2^{-30}\left(\frac{\delta}{\alpha}\right)^2\left(\frac{\log(1/\delta)}{16d}\right)^{d-1}\,.$$

Предложение доказано.

Замечание 2.11 Безусловно, значение параметра α в предложении 2.10 можно несколько изменить. Например, если рассмотреть в этом предложении множества $\mathcal{H}_2$ вместо $\mathcal{H}_1$, то параметр α можно выбрать меньше, чем $2^{-12}\delta/\sqrt{n}$.

3. О связных подмножествах $d\dot{\Lambda}$.

Пусть G — абелева группа и $A \subseteq G$ — произвольное конечное множество. В работе [30] изучались множества A обладающие так называемым свойством "связности" (см. также статью [8]). Приведем одно определение из [30].

Определение 3.1 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 (β_1,β_2)*–связным порядка* k, если найдется такая абсолютная константа $C \in (0,1]$, что для всякого множества $B \subseteq A$, $\beta_1|A| \leq |B| \leq \beta_2|A|$ выполнено

$$T_k(B) \geq C^{2k}\left(\frac{|B|}{|A|}\right)^{2k} T_k(A)\,. \qquad (28)$$

Через $\zeta_k(A)$ обозначим величину $\zeta_k(A) := \frac{\log T_k(A)}{\log|A|}$. В работе [30] (см. также [16]) была доказана следующая теорема.

Теорема 3.2 *Пусть $A \subseteq G$ — произвольное конечное множество, $|A| = m \geq 2$. Пусть также $\beta_1,\beta_2 \in (0,1)$ — действительные числа, $\beta_1 \leq \beta_2$. Тогда найдется множество $A' \subseteq A$ такое, что*

1) *A' является (β_1,β_2)–связным порядка k множеством, причем в качестве константы C в неравенстве (28) можно взять любое число не превосходящее* $1/32$.

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

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

В этом параграфе мы получим аналог теоремы 3.2 для подмножеств сумм диссоциативных множеств.

Пусть $\Lambda \subseteq \mathbf{F}_2^n$ — произвольное множество из семейства $\mathbf{\Lambda}(2dk)$ и $A \subseteq d\dot{\Lambda}$. Определим величину $D_k(A)$ по формуле

$$D_k(A) = \log\left(\frac{T_k(A)}{k^k|A|^k}\right). \tag{29}$$

Иными словами $T_k(A) = 2^{D_k(A)}k^k|A|^k$. Поскольку для всех множеств A с достаточно большой мощностью всегда выполнено $T_k(A) \geq \binom{|A|}{k}(k!)^2 \geq e^{-2k}k^k|A|^k$, то величина $D_k(A)$ не меньше $-2k\log e$. С другой стороны, из предложения 2.7 вытекает, что $D_k(A) \leq 8d\log d + k(d-1)\log k$.

Теорема 3.3 *Пусть $K > 0$ — действительное число, k, d — натуральные числа, $k, d \geq 2$. Пусть $\Lambda \subseteq \mathbf{F}_2^n$ — произвольное множество из семейства $\mathbf{\Lambda}(2dk)$, а Q — некоторое подмножество $d\dot{\Lambda}$ такое, что $T_k(Q) \geq \frac{k^{dk}|Q|^k}{K^k}$. Пусть также $\beta_1, \beta_2 \in (0,1)$ — действительные числа, $\beta_1 \leq \beta_2$. Тогда найдется множество $Q' \subseteq Q$ такое, что*
1) *Q' является (β_1, β_2)–связным порядка k множеством, причем в качестве константы C в неравенстве (28) можно взять любое число не превосходящее $1/8$.*
2) $|Q'| \geq |Q| \cdot 2^{\frac{8d\log d + k(d-1)\log k - D_k(Q)}{k\log(1+\beta_1(1-4C))}\log(1-\beta_2)}$.
3) $T_k(Q') \geq \frac{k^{dk}|Q'|^k}{K^k}$.

Доказательство. Пусть $m = |Q|$ и $C \leq 1/8$ — некоторое число. Доказательство теоремы 3.3 представляет собой алгоритм. Если множество Q является (β_1, β_2)–связным множеством порядка k, так что неравенство (28) выполнено с константой C, то доказывать нечего. Пусть теперь множество Q не является (β_1, β_2)–связным порядка k множеством с константой C. Тогда найдется множество $B \subseteq Q$, $\beta_1|Q| \leq |B| \leq \beta_2|Q|$ такое, что неравенство (28) не выполнено. Пусть $\overline{B} = Q \setminus B$ и $c_B = |B|/|Q|$. Имеем $\beta_1 \leq c_B \leq \beta_2$. Применяя следствие 2.3, находим

$$T_k(\overline{B}) > T_k(A)(1 - Cc_B)^{2k}. \tag{30}$$

Пусть $b = |B|$ и $\overline{b} = |\overline{B}| = m - b$, $D = D_k(Q)$, $\overline{D} = D_k(\overline{B})$. Логарифмируя неравенство (30), получаем

$$\overline{D} > D + k\log m - k\log\overline{b} + 2k\log(1 - Cc_B) = D + k\left(\log(\frac{m}{m-b}(1 - Cc_B)^2)\right) \geq$$

$$\geq D + k\log((1 + c_B)(1 - 2Cc_B)) \geq D + k\log(1 + \beta_1(1 - 4C)). \tag{31}$$

Из определения (β_1, β_2)–связности порядка k вытекает неравенство

$$|\overline{B}| \geq (1 - \beta_2)m = (1 - \beta_2)|Q|. \tag{32}$$

Таким образом, если множество не является (β_1, β_2)–связным порядка k, то найдется множество $\overline{B} \subseteq Q$ для которого выполнены неравенства (31), (32). Положим $Q_1 = \overline{B}$ и применим изложенные выше рассуждения к множеству Q_1. И так далее. Мы получим множества $Q_0 = Q, Q_1, Q_2, \ldots, Q_s$. Ясно, что для любого Q_i справедливо неравенство $D_k(Q_i) \leq 8d\log d + k(d-1)\log k$. Отсюда и неравенства (31) вытекает, что наш процесс закончится менее, чем через $\frac{8d\log d + k(d-1)\log k - D_k(Q)}{k\log(1+\beta_1(1-4C))}$ шагов. На последнем шаге алгоритма мы найдем множество $Q' = Q_s \subseteq Q$, которое будет (β_1, β_2)–связным порядка k и, при этом, $D_k(Q') \geq D_k(Q)$. Таким образом неравенства 1) и 3) теоремы 3.3 для множества Q' выполнены. Докажем 2). Применяя неравенство (32), получаем

$$|A'| \geq (1 - \beta_2)^s m \geq m \cdot 2^{\frac{8d\log d + k(d-1)\log k - D_k(Q)}{k\log(1+\beta_1(1-4C))}\log(1-\beta_2)}.$$

Теорема доказана.

Теорема 3.3 нам понадобится в следующем параграфе.

4. О больших подмножествах суммы двух диссоциативных множеств.

Пусть $G = (g_{ij})$ — матрица $x \times y$, $x \le y$ Обозначим через $\operatorname{per} G$ перманент матрицы G. Напомним, что

$$\operatorname{per} G = \sum_{\sigma} g_{1\sigma(1)} \dots g_{x\sigma(x)}\,, \tag{33}$$

где суммирование в формуле (33) проходит по всех инъективным отображениям $\sigma : [x] \to [y]$. Нам понадобится известная теорема Фробениуса–Кенига о неотрицательных матрицах (см. [25]).

Теорема 4.1 *Пусть p и r — натуральные числа, $r \le p$ и пусть H — неотрицательная матрица размера $p \times r$. Тогда перманент матрицы H равен нулю в том и только в том случае, когда H содержит нулевую матрицу размера $p - s + 1 \times s$.*

Используя теорему 4.1 мы докажем лемму.

Лемма 4.2 *Пусть p и r — натуральные числа и пусть $H = (h_{ij})$ — матрица размера $p \times r$, составленная из целых неотрицательных чисел. Пусть также*
1) *Для всех $i \in [p]$ выполнено $\sum_{j=1}^{r} h_{ij} \ge 2$.*
2) *Для всех $j \in [r]$ выполнено $\sum_{i=1}^{p} h_{ij} \ge 1$ и, наконец,*
3) *$\sum_{i=1}^{p} \sum_{j=1}^{r} h_{ij} = 2p$.*

Выкинув из матрицы H все столбцы с $\sum_{i=1}^{p} h_{ij} = 1$ мы получим матрицу H_0. Тогда перманент этой матрицы не равен нулю.

Доказательство. Пусть существует ровно e значений j таких, что $\sum_{i=1}^{p} h_{ij} = 1$. Не ограничивая общности будем считать, что матрица H_0 получена из матрицы H вычеркиванием последних e столбцов. Пусть $H_0 = (h^0_{ij})$, $i = 1, \dots, p$, $j = 1, \dots, r - e = r_0$. Из условия 3) леммы вытекает, что $\sum_{i=1}^{p} \sum_{j=1}^{r_0} h^0_{ij} = 2p - e$. Отсюда и условия 2) получаем неравенство $r_0 \le p$. Предположим, что лемма не верна. Если перманент матрицы H_0 равен нулю, то по теореме Фробениуса–Кенига H_0 содержит нулевую подматрицу размера $s \times t$, $s + t = p + 1$. Делая перестановку строк и столбцов можно добиться того, чтобы матрица H_0 имела вид

$$H_0 = \begin{pmatrix} \mathbf{X} & \mathbf{Z} \\ \mathbf{0} & \mathbf{Y} \end{pmatrix},$$

где нулевая матрица $\mathbf{0}$ имеет размер $s \times t$, $s + t = p + 1$. Обозначим через s_1 — число тех $i \in \{p - s + 1, \dots, p\}$, что $\sum_{j=1}^{r_0} h^0_{ij} = 1$, а через s_2 — число тех $i \in \{p - s + 1, \dots, p\}$, что $\sum_{j=1}^{r_0} h^0_{ij} \ge 2$. Очевидно $s_1 \le e$. Из условия 2) вытекает, что $s = s_1 + s_2$. Применяя условие 1) леммы, находим

$$2p - e = \sum_{i=1}^{p} \sum_{j=1}^{r_0} h^0_{ij} \ge \sum_{j=1}^{t} \sum_{i=1}^{p} h^0_{ij} + \sum_{i=p-s+1}^{p} \sum_{j=1}^{r_0} h^0_{ij} \ge 2t + s_1 + 2s_2 = 2t + 2s - s_1 = 2p + 2 - s_1\,.$$

Из последнего неравенства вытекает оценка $s_1 \ge e + 2$, что противоречит неравенству $s_1 \le e$. Лемма доказана.

Пусть p — натуральное число, $\Lambda \subseteq \mathbf{F}_2^n$ — произвольное множество из семейства $\mathbf{\Lambda}(2p)$ и $\mathcal{E} = \{E_1, \dots, E_{2p}\}$ — набор подмножеств Λ. В процессе доказательства предложения 2.7 возникала необходимость оценивать число решений уравнения

$$\lambda_1 + \dots + \lambda_{2p} = 0, \qquad \text{где} \qquad \lambda_i \in E_i, \quad i = 1, \dots, 2p\,. \tag{34}$$

Для подсчета числа решений таких уравнений мы использовали лемму 2.2 — простое следствие неравенства Гельдера. Для доказательства теоремы 4.10 — основного результата этого параграфа, нам понадобится более тонкий результат о числе решений уравнения (34).

Лемма 4.3 *Пусть p — натуральное число, $\Lambda \subseteq \mathbf{F}_2^n$ — произвольное множество из семейства $\mathbf{\Lambda}(2p)$ и $\mathcal{E} = \{E_1, \dots, E_{2p}\}$ — набор подмножеств Λ. Предположим, что отрезок $[2p]$ разбит на r классов $\mathcal{C}_1, \dots, \mathcal{C}_r$. Пусть $S^* \subseteq [2p]$ — произвольное множество и $\bar{S}^* = [2p] \setminus S$. Пусть также $M(S^*) = (m_{ij})$ — матрица размера $p \times p$, $m_{ij} = |E_i \bigcap E_j|$, $i \in S$, $j \in \bar{S}^*$. Тогда число решений уравнения*

$$\lambda_1 + \dots + \lambda_{2p} = 0, \qquad \text{где} \qquad \lambda_i \in E_i, \quad i = 1, \dots, 2p \tag{35}$$

не превосходит величины

$$\sum_{S^* \subseteq [2p],\, |S^*| = p} \operatorname{per} M(S^*)\,, \tag{36}$$

причем суммирование в формуле (36) проходит по таким S^*, что S^* содержит по одному представителю из каждого класса $\mathcal{C}_i$ с условием $|\mathcal{C}_i| \geq 2$.

Доказательство. Обозначим число решений уравнения (35) через Z. Поскольку множество Λ принадлежит семейству $\mathbf{\Lambda}(2p)$, то в произвольном решении уравнения (35) любое λ_i, $i \in [2p]$ встречается четное число раз. Рассуждая, как при доказательстве предложения 2.5, получаем

$$Z \leq \sum_{\mathcal{K},\, \mathcal{K} = \{K_1, \dots, K_p\},\, [2p] = K_1 \bigsqcup \dots \bigsqcup K_p} \prod_{j=1}^{p} \left| \bigcap_{\alpha \in K_j} E_\alpha \right| = Z_1\,. \tag{37}$$

Суммирование в (37) проходит по семействам множеств $\mathcal{K}$, $\mathcal{K} = \{K_1, \dots, K_p\}$, $[2p] = K_1 \bigsqcup \dots \bigsqcup K_p$ так, что для любого $j \in [p]$ выполнено $|K_j| = 2$. Докажем, что

$$Z_1 \leq \sum_{S^* \subseteq [2p],\, |S^*| = p} \operatorname{per} M(S^*) \tag{38}$$

причем суммирование в (38) проходит по таким S^*, что S^* содержит по одному элементу из каждого класса $\mathcal{C}_i$ с условием $|\mathcal{C}_i| \geq 2$. Если опустить последнюю оговорку, то неравенство (38) становится очевидным. Другими словами, всегда

$$\sum_{\mathcal{K},\, \mathcal{K} = \{K_1, \dots, K_p\},\, [2p] = K_1 \bigsqcup \dots \bigsqcup K_p} \prod_{j=1}^{p} \left| \bigcap_{\alpha \in K_j} E_\alpha \right| \leq \sum_{S^* \subseteq [2p],\, |S^*| = p} \operatorname{per} M(S^*) \tag{39}$$

Чтобы убедиться в справедливости последнего неравенства заметим, что любое слагаемое x, отвечающее некоторому разбиению $\mathcal{K}$ из левой части (39), присутствует и в правой части. Действительно, возьмем в качестве S^* первые элементы множеств K_j, $j = 1, \dots, p$. Пусть α — любой такой элемент, $\alpha \in K_j$. Тогда в правой части (39) присутствует величина $|E_\alpha \bigcap E_\beta|$ с $\beta \in K_j$. Перемножая все такие величины получаем x. Наоборот, если y — произвольное слагаемое из правой части (39) и то, как легко видеть, мы однозначно построим по этому y некоторое разбиение $\mathcal{K}$.

Таким образом, чтобы доказать неравенство (38) достаточно по каждому слагаемому x из левой части (38), отвечающему некоторому разбиению $\mathcal{K}$, найти множество S^* такое,

что для всех $j \in [p]$ выполнено $|K_j \bigcap S^*| = 1$ и такое, что S^* содержит по одному представителю из каждого класса $\mathcal{C}_i$ с условием $|\mathcal{C}_i| \geq 2$. Пусть $H = (h_{\gamma\delta})$ — неотрицательная матрица $p \times r$ такая, что элемент $h_{\gamma\delta}$ матрицы H равен $|K_\gamma \bigcap \mathcal{C}_\delta|$. Ясно, что для всех $\gamma \in [p]$ выполнено $\sum_\delta h_{\gamma\delta} = |K_\gamma| = 2$ и $\sum_{\gamma,\delta} h_{\gamma\delta} = \sum_\gamma |K_\gamma| = 2p$. Так как множества $\mathcal{C}_1, \ldots, \mathcal{C}_r$ разбивают отрезок $[2p]$, то для всех $\delta \in [r]$ справедливо неравенство $\sum_\gamma h_{\gamma\delta} = |\mathcal{C}_\delta| \geq 1$. Применяя лемму 4.2, получаем, что перманент матрицы H_0, полученной из H вычеркиванием всех столбцов с $\sum_\gamma h_{\gamma\delta} = 1$, не равен нулю. Следовательно, в H_0 есть диагональ из ненулевых элементов. Пусть H_0 имеет размеры $p \times r_0$. Не ограничивая общности будем считать, что матрица H_0 занимает первые r_0 столбцов в матрице H. Тогда ненулевая диагональ в H_0 имеет вид — $(\gamma_1, 1), \ldots, (\gamma_{r_0}, r_0)$. Из построения матрицы H вытекает, что для любого $i \in [r]$ найдется число $\alpha_i \in K_{\gamma_i}$ такое, что $\alpha_i \in \mathcal{C}_i$ и $|\mathcal{C}_i| \geq 2$. Поместим элементы $\alpha_1, \ldots, \alpha_r$ в множество S^*. Кроме того, добавим в S^* первые элементы из всех K_γ, $\gamma \neq \gamma_1, \ldots, \gamma_r$. Легко видеть, что S^* содержит по одному представителю из каждого класса $\mathcal{C}_i$ с условием $|\mathcal{C}_i| \geq 2$. Лемма доказана.

Замечание 4.4 Лемма 4.3 дает оценку величины $T_p(E_1, \ldots, E_{2p})$ по–порядку не хуже, чем оценка $p^p \prod_{\alpha=1}^{2p} |E_\alpha|^{1/2}$, вытекающая из леммы 2.2. Действительно, для любых множеств A и B выполнено

$$|A \bigcap B| \leq \min\{|A|, |B|\} \leq |A|^{1/2} |B|^{1/2}. \tag{40}$$

Поэтому каждое слагаемое в разложении $\operatorname{per} M(S^*)$ не превосходит $\prod_{\alpha=1}^{2p} |E_\alpha|^{1/2}$. Поскольку существует ровно $p!$ таких слагаемых, мы получаем по лемме 4.3, что $T_p(E_1, \ldots, E_{2p}) \leq 2^{2p} p! \prod_{\alpha=1}^{2p} |E_\alpha|^{1/2}$.

Лемма 4.5 *Пусть $\delta_0 > 0$ — действительное число, r, p — натуральные числа, $p \geq 2\delta_0 + 3$, $r \geq p - \delta_0$. Пусть $t_1, \ldots, t_r$ — последовательность натуральных чисел таких, что $t_j \geq 2$, $j = 1, \ldots, r$ и $\sum_{j=1}^r t_j = 2p$. Пусть также $T = \max_{j \in [r]} t_j$ и $\alpha_j = |\{j \in [r] \ : \ t_j \geq T - i\}|$, $i = 0, 1, \ldots, T-2$. Пусть неотрицательное число z определяется соотношениями $\sum_{i=0}^{z-1} \alpha_i \leq p < \sum_{i=0}^{z} \alpha_i$ и $q_z = p - \sum_{i=0}^{z-1} \alpha_i$. Тогда величина*

$$\pi(t_1, \ldots, t_r) := T^{\alpha_0} (T-1)^{\alpha_1} \ldots (T - (z-1))^{\alpha_{z-1}} (T-z)^{q_z}$$

не превосходит $2^{3p} \max\{\, \delta_0^{4\delta_0}, 1 \,\}$.

Доказательство. Предположим сначала, что $\delta_0 \geq 1$. Легко видеть, что последовательность $\alpha_0, \alpha_1, \ldots, \alpha_{T-2}$ — неубывающая и $\sum_{i=0}^{T-2} \alpha_i = \sum_{j=1}^r t_j = 2p$. Еще раз применяя условие $\sum_{j=1}^r t_j = 2p$, а также неравенства $r \geq p - \delta_0$, $t_j \geq 2$, $j \in [r]$, получаем $T + 2(r-1) \leq 2p$ и $T \leq 2\delta_0 + 2 \leq 4\delta_0$. Предположим, что $\alpha_0 = \cdots = \alpha_{z-1} = q_z = 1$. Тогда $p = \sum_{i=0}^{z-1} \alpha_i + q = z + 1$. С другой стороны, имеется ровно $T - 1$ чисел α_i. Следовательно, величина z не превосходит $T - 1$ и мы получаем неравенство $p \leq T \leq 2\delta_0 + 2$, что противоречит условию. Значит, либо $\alpha_{z-1} \geq 2$, либо $q_z \geq 2$.

Пусть π^* — максимальное значение функции $\pi(t_1, \ldots, t_r)$ при условиях

$$t_1 + \cdots + t_r = 2p, \quad t_j \geq 2, \quad r \geq p - \delta_0. \tag{41}$$

Наборы $t_1, \ldots, t_r$, удоветворяющие условию (41) будем называть *допустимыми*. Пусть $\pi^* = \pi(t_1^0, \ldots, t_r^0)$. Без ограничения общности можно считать, что $t_1^0 \geq t_2^0 \geq \cdots \geq t_r^0$. Из рассуждений выше вытекает, что либо $\alpha_{z-1} \geq 2$, либо $q_z \geq 2$. Если $t_2^0 \geq 3$, то рассмотрим допустимый набор $\tilde{t}_1 = t_1^0 + 1$, $\tilde{t}_2 = t_1^0 - 1$, $\tilde{t}_3 = t_3^0, \ldots, \tilde{t}_r = t_r^0$. Нетрудно убедится в том, что $\pi^* = \pi(t_1^0, \ldots, t_r^0) < \pi(\tilde{t}_1, \ldots, \tilde{t}_r)$. Следовательно, $t_2^0 = 2$ и $\pi^* \leq T^T 2^p \leq 2^{3p} \delta_0^{4\delta_0}$.

Нам осталось рассмотреть ситуацию, когда $\delta_0 < 1$. В этом случае $T \le 4$. Применяя тривиальную оценку $\pi(t_1,\dots,t_r) \le T^p \le 2^{2p}$ получаем требуемый результат. Лемма доказана.

Пусть k — натуральное число, $k \ge 2$ и $\Lambda_1, \Lambda_2 \subseteq \mathbf{F}_2^n$ — произвольные *непересекающиеся* множества так, что $\Lambda_1 \bigsqcup \Lambda_2$ принадлежит семейству $\mathbf{\Lambda}(4k)$. Пусть также Q — некоторое подмножество множества $\Lambda_1 \dot{+} \Lambda_2 = \Lambda_1 + \Lambda_2$. Определим множества $D(\lambda) = D_\lambda$ и $Q(\lambda) = Q_\lambda$, $\lambda \in \Lambda_1$ (см. доказательство предложения 2.7). Пусть $\lambda \in \Lambda_1$ и

$$D(\lambda) = \{\ \lambda' \ :\ \lambda + \lambda' \in Q,\ \lambda' \in \Lambda_2\ \}\,,$$

$$Q(\lambda) = \{\ q \in Q \ :\ q = \lambda + \lambda',\ \lambda' \in \Lambda_2\ \}\,.$$

Ясно, что $Q(\lambda) = D(\lambda) + \lambda$. Пусть s_1 — число непустых множеств D_λ. Пусть это множества $D_{\lambda_1},\dots,D_{\lambda_{s_1}}$. Иногда, для краткости, мы будем писать D_j вместо D_{λ_j}. Пусть также $s_2 = |\Lambda_2|$. Ясно, что $Q \subseteq \{\lambda_1,\dots,\lambda_s\} + \Lambda_2$.

Предложение 4.6 *Пусть $M > 0$ — вещественное число, p — натуральное число, $p \ge 5$ и $\Lambda_1, \Lambda_2 \subseteq \mathbf{F}_2^n$ — произвольные непересекающиеся множества из семейства $\mathbf{\Lambda}(4p)$. Пусть также Q — некоторое подмножество $\Lambda_1 + \Lambda_2$, $|Q| \ge \max\{2s_2p, 2^8 s_2 p M^8\}$, $\delta_0 = \max\{(p\log(2eM))/\log(|Q|/(s_2p)), 1\}$ и $X = \max\{\ \delta_0^{4\delta_0}, 1\ \}$. Тогда*

$$T_p(Q) \le 2^{5p} X p^{3p} s_2^p \cdot \sum_{r=p-\lceil\delta_0\rceil}^{p} \left(\frac{1}{ps_2}\right)^r \cdot \left(\sum_{S\subseteq[s_1],\,|S|=r}\ \prod_{\alpha\in S}\left(\sum_{\beta\in S}|D_\alpha \bigcap D_\beta|\right)\right) + \frac{p^{2p}|Q|^p}{2M^p}\,. \quad (42)$$

Доказательство. Пусть $m = |Q|$. Рассмотрим уравнение

$$q_1 + \dots + q_{2p} = 0\,, \quad (43)$$

где $q_i \in Q$, $i = 1,\dots,2p$. Обозначим через σ число решений уравнения (43). Так как $Q \subseteq \Lambda_1 + \Lambda_2$, то для всех $q \in Q$ выполнено $q = \lambda_1 + \lambda_2$, где $\lambda_1 \in \Lambda_1$, $\lambda_2 \in \Lambda_2$.

Пусть $i_1,\dots,i_{2p} \in [s_1]$ — произвольные числа. Обозначим через $\sigma_{\vec{i}}$, $\vec{i} = (i_1, i_2, \dots, i_{2p})$ — множество решений уравнения (43) таких, что для всех $j \in [2p]$ имеет место ограничение $q_j \in D(\lambda_{i_j})$, $\lambda_{i_j} \in \Lambda_1$. По условию множество $\Lambda_1 \bigsqcup \Lambda_2$ принадлежит семейству $\mathbf{\Lambda}(4k)$ и $\Lambda_1 \bigcap \Lambda_2 = \emptyset$. Отсюда следует, что если $q_1,\dots,q_{2p}$ — решение уравнения (43), принадлежащее множеству $\sigma_{\vec{i}}$, то любой компонент вектора $\vec{i}$ встречается в этом векторе четное число раз. Имеем

$$\sigma \le \sum_{\mathcal{N},\,\mathcal{N}=\{N_1,\dots,N_r\},\ [2p]=N_1\bigsqcup\dots\bigsqcup N_r}\ \sum_{\vec{i}\in\mathcal{N}} |\sigma_{\vec{i}}|\,. \quad (44)$$

Суммирование в правой части (44) проходит по семействам множеств $\mathcal{N}, \mathcal{N} = \{N_1,\dots,N_r\}$, $[2p] = N_1 \bigsqcup \dots \bigsqcup N_r$ так, что для всех $j = 1,\dots,r$ величина $|N_j|$ — четная и $|N_j| \ge 2$. Пусть $N_j = \{\alpha_1^{(j)},\dots,\alpha_{|N_j|}^{(j)}\}$, $j = 1,\dots,r$. По определению $\vec{i} \in \mathcal{N}$, если для всех $j \in [r]$ выполнено $i_{\alpha_1^{(j)}} = \dots = i_{\alpha_{|N_j|}^{(j)}}$ и для различных множеств N_{j_1}, N_{j_2} из разбиения $\mathcal{N}$ выполнено $i_\alpha \ne i_\beta$, где α — произвольный элемент из N_{j_1}, а β — из N_{j_2}.

Обозначим число множеств N_j в разбиении $\mathcal{N}$ через $r = r(\mathcal{N})$. Имеем

$$\sigma = \sum_{r=0}^{p-\lceil\delta_0\rceil}\ \sum_{\mathcal{N},\,r(\mathcal{N})=r}\ \sum_{\vec{i}\in\mathcal{N}} |\sigma_{\vec{i}}| + \sum_{r=p-\lceil\delta_0\rceil+1}^{p}\ \sum_{\mathcal{N},\,r(\mathcal{N})=r}\ \sum_{\vec{i}\in\mathcal{N}} |\sigma_{\vec{i}}| = \sigma_1 + \sigma_2\,. \quad (45)$$

Оценим сумму σ_1. Пусть q — произвольный элемент множества Q. Используя условие $\Lambda_1 \bigcap \Lambda_2 = \emptyset$ и диссоциативность множества Λ, легко видеть, что множества $Q(\lambda)$ не пересекаются. Отсюда

$$\sum_{\lambda\in\Lambda_1} |D(\lambda)| = \sum_{\lambda\in\Lambda_1} |Q(\lambda)| = m\,. \tag{46}$$

Для любого $\lambda \in \Lambda_1$ имеем $|D_\lambda| \le s_2$. Пусть $x \ge 1$ — любое число. Используя равенство (46), получаем

$$\sum_{\lambda\in\Lambda_1} |D(\lambda)|^x = \sum_{\lambda\in\Lambda_1} |Q(\lambda)|^x \le s_2^{x-1} \sum_{\lambda\in\Lambda_1} |Q(\lambda)| = s_2^{x-1} m\,. \tag{47}$$

Пусть $S_{\vec{i}} = \{i_j\}_{j\in[2p]}$. Пользуясь леммой 2.2 и неравенством (47), получаем

$$\sigma_1 \le \sum_{r=0}^{p-\lceil\delta_0\rceil} \sum_{\mathcal{N},\, r(\mathcal{N})=r} \sum_{\vec{i}\in\mathcal{N}} \prod_{\alpha\in[2p]} |D_{i_\alpha}|^{1/2} \le p^p \sum_{r=0}^{p-\lceil\delta_0\rceil} \sum_{\mathcal{N},\, r(\mathcal{N})=r} s_2^{p-r} \sum_{\vec{i}\in\mathcal{N}} \prod_{\alpha\in S_{\vec{i}}} |D_\alpha|\,.$$

Заметим, что если зафиксированы длины множеств N_j, то от их перестановки множество $S_{\vec{i}}$ не меняется. Пусть $t_j = |N_j|$, $j = 1, \dots, r$. Используя неравенство $m \ge 2s_2 p$, определение величины δ_0 и тождество (46), находим

$$\sigma_1 \le p^p \sum_{r=0}^{p-\lceil\delta_0\rceil} \sum_{t_1+\dots+t_r=2p} \frac{(2p)!}{t_1!\dots t_r!}\,\frac{1}{r!}\,s_2^{p-r}\,m^r \le e^p p^p s_2^p \sum_{r=0}^{p-\lceil\delta_0\rceil} \left(\frac{m}{s_2}\right)^r r^{2p-r} \le$$

$$\le 2e^p p^{3p} s_2^p \left(\frac{m}{ps_2}\right)^{p-\delta_0} = 2e^p p^{2p} m^p \left(\frac{s_2 p}{m}\right)^{\delta_0} \le \frac{p^{2p} m^p}{2M^p}\,. \tag{48}$$

Как видно из формулы (48), разбиения $\mathcal{N}$ с малым значением $r(\mathcal{N})$ дают малый вклад в величину $T_p(Q)$. В оставшейся части доказательства мы рассмотрим разбиения $\mathcal{N}$ с большим числом множеств N_j.

Оценим сумму σ_2. Рассмотрим множества $D_{i_1}, \dots, D_{i_{2p}}$. Пусть $\mathcal{C}_j = N_j$ — множества, разбивающие отрезок $[2p]$. Применяя лемму 4.3, получаем

$$\sigma_2 \le \sum_{r=p-\lceil\delta_0\rceil}^{p} \sum_{\mathcal{N},\, r(\mathcal{N})=r} \sum_{\vec{i}\in\mathcal{N}} \left(\sum_{S^*\subseteq[2p],\, |S^*|=p} \operatorname{per} M_{\vec{i}}(S^*) \right)\,. \tag{49}$$

Согласно лемме 4.3 суммирование в формуле (49) проходит по таким S^*, что S^* содержит по одному представителю из каждого множества N_j. При этом $M_{\vec{i}}(S^*) = (m_{\alpha\beta})$ — матрица размера $p \times p$, $m_{\alpha\beta} = |D_{i_\alpha} \bigcap D_{i_\beta}|$, $\alpha \in S^*$, $\beta \in \bar{S}^*$. Пусть $M'_{\vec{i}}$ — матрица $r \times 2p$, $M'_{\vec{i}} = (|D_\alpha \bigcap D_{i_\beta}|)_{\alpha\in S_{\vec{i}}, \beta\in[2p]}$. Из формулы (33) вытекает неравенство

$$\operatorname{per} M_{\vec{i}}(S^*) \le \prod_{\alpha\in[2p],\, i_\alpha\notin S_{\vec{i}}} \left(\sum_{\beta\in\bar{S}^*} |D_{i_\alpha} \bigcap D_{i_\beta}| \right) \cdot \operatorname{per} M'_{\vec{i}}\,. \tag{50}$$

Используя только что доказанное неравенство и очевидную оценку $|D_\lambda| \le s_2$, $\lambda \in \Lambda_1$, находим

$$\operatorname{per} M_{\vec{i}}(S^*) \le \prod_{\alpha\in[2p],\, i_\alpha\notin S_{\vec{i}}} \left(\sum_{x\in\Lambda_2} D_{i_\alpha}(x) \sum_{\beta\in\bar{S}^*} D_{i_\beta}(x) \right) \cdot \operatorname{per} M'_{\vec{i}} \le p^{p-r} s_2^{p-r} \operatorname{per} M'_{\vec{i}}\,. \tag{51}$$

Пользуясь формулой для вычисления перманента (33), легко видеть, что

$$\operatorname{per} M'_{\vec{i}} \le \pi(t_1,\dots,t_r)\prod_{\alpha\in S_{\vec{i}}}\left(\sum_{\beta\in S_{\vec{i}}}|D_\alpha\bigcap D_\beta|\right),$$

где величина $\pi(t_1,\dots,t_r)$ определена в лемме 4.5. Используя оценку для $\pi(t_1,\dots,t_r)$ из этой леммы и неравенства (49), (51), получаем

$$\sigma_2 \le 2^{5p}\max\{\,\delta_0^{4\delta_0},1\,\}\cdot\sum_{r=p-\lceil\delta_0\rceil}^{p}p^{p-r}s_2^{p-r}\sum_{\mathcal{N},r(\mathcal{N})=r}\sum_{\vec{i}\in\mathcal{N}}\prod_{\alpha\in S_{\vec{i}}}\left(\sum_{\beta\in S_{\vec{i}}}|D_\alpha\bigcap D_\beta|\right).$$

Множество $S_{\vec{i}}$ не изменится, если переставить различные компоненты вектора $\vec{i}$ по различным частям N_j разбиения $\mathcal{N}$. Кроме того, если зафиксированы длины множеств N_j, то от их перестановки множество $S_{\vec{i}}$ также не меняется. Отсюда

$$\sigma_2 \le 2^{5p}\max\{\,\delta_0^{4\delta_0},1\,\}\cdot\sum_{r=p-\lceil\delta_0\rceil}^{p}p^{p-r}s_2^{p-r}\sum_{t_1+\dots+t_r=2p}\frac{(2p)!}{t_1!\dots t_r!}\frac{1}{r!}\,r!\cdot$$

$$\cdot\left(\sum_{S\subseteq[s_1],\,|S|=r}\prod_{\alpha\in S}\left(\sum_{\beta\in S}|D_\alpha\bigcap D_\beta|\right)\right)\le 2^{5p}\max\{\,\delta_0^{4\delta_0},1\,\}p^{3p}s_2^p\cdot$$

$$\cdot\sum_{r=p-\lceil\delta_0\rceil}^{p}\left(\frac{1}{ps_2}\right)^r\cdot\left(\sum_{S\subseteq[s_1],\,|S|=r}\prod_{\alpha\in S}\left(\sum_{\beta\in S}|D_\alpha\bigcap D_\beta|\right)\right). \qquad (52)$$

Объединяя оценки (48), (52) и формулу (45), получаем неравенство (42). Предложение доказано.

Для доказательства теоремы 4.10 нам понадобится одна комбинаторная лемма и известная лемма Е. Бомбьери (см., например, [27]).

Пусть p — натуральное число и $A_1,\dots,A_p$ — последовательность множеств таких, что любые два множества A_i и A_j этой последовательности либо не пересекаются, либо совпадают. Обозначим через ρ — количество различных множеств среди $A_1,\dots,A_p$. Пусть множество A_1^* встречается в последовательности $A_1,\dots,A_p$ ровно l_1 раз, A_2^* — ровно l_2 раза, $\dots$, A_ρ^* — ровно l_ρ раз.

Лемма 4.7 *Пусть w — натуральное число, $2\le p\le a$, $\zeta\in(0,1]$ — действительное число и $S_1,\dots,S_q$ — некоторые множества, не равные между собой, $|S_i|=p$, $S_i=\{s_i^{(1)},\dots,s_i^{(p)}\}$, $i=1,\dots,q$. Пусть также для всех $i\in[q]$ и всех множеств S_i выполнено $s_i^{(j)}\in A_j$, $j=1,\dots,p$. Предположим, что*

$$q\ge 2\sum_{\omega=\lceil\zeta p\rceil}^{p}\frac{(pw)^\omega}{\omega!}\sum_{n_1+\dots+n_\rho=p-\omega,\,n_i\le l_i}\frac{|A_1^*|^{n_1}\dots|A_\rho^*|^{n_\rho}}{n_1!\dots n_\rho!}.$$

Тогда найдутся множества $S_{n_1},\dots,S_{n_w}$ из набора $S_1,\dots,S_q$ такие, что для всех $l=2,\dots,w$ выполнено $|(\bigcup_{i=1}^{l-1}S_{n_i})\bigcap S_{n_l}|\le\zeta p$.

Доказательство. Будем последовательно строить множества $S_{n_1},\dots,S_{n_w}$. Пусть $S_{n_1}=$

S_1. Предположим, что множества $S_{n_1},\dots,S_{n_{l-1}}$ уже построены. Найдем множество S_{n_l}. Пусть $C_l=\bigcup_{i=1}^{l-1}S_{n_i}$. Ясно, что $|C_l|\le wp$. Пусть $C_l=C_1^*\bigsqcup\dots\bigsqcup C_\rho^*$, где $C_i^*\subseteq A_i^*$, $i=1,\dots,\rho$. Пусть также $a_i=|A_i^*|$, $c_i=|C_i^*|$, $i=1,\dots,\rho$. Число множеств мощности p из объединения $A_1^*\bigsqcup\dots\bigsqcup A_\rho^*$, пересекающих C_l по более чем ζp элементам не превосходит

$$\sigma:=\sum_{\omega=\lceil\zeta p\rceil}^{p}\sum_{m_1+\dots+m_\rho=\omega,\,m_i\le c_i}\ \sum_{n_1+\dots+n_\rho=p-\omega,\,n_i\le\min\{a_i-c_i,l_i\}}\binom{c_1}{m_1}\dots\binom{c_\rho}{m_\rho}\times$$

$$\times\binom{a_1-c_1}{n_1}\dots\binom{a_\rho-c_\rho}{n_\rho}\le\sum_{\omega=\lceil\zeta p\rceil}^{p}\sum_{m_1+\dots+m_\rho=\omega}\ \sum_{n_1+\dots+n_\rho=p-\omega,\,n_i\le l_i}\frac{c_1^{m_1}\dots c_\rho^{m_\rho}}{m_1!\dots m_\rho!}\cdot\frac{a_1^{n_1}\dots a_\rho^{n_\rho}}{n_1!\dots n_\rho!}\le$$

$$\le\sum_{\omega=\lceil\zeta p\rceil}^{p}\frac{(c_1+\dots+c_\rho)^\omega}{\omega!}\cdot\sum_{n_1+\dots+n_\rho=p-\omega,\,n_i\le l_i}\frac{a_1^{n_1}\dots a_\rho^{n_\rho}}{n_1!\dots n_\rho!}\le$$

$$\le\sum_{\omega=\lceil\zeta p\rceil}^{p}\frac{(pw)^\omega}{\omega!}\cdot\sum_{n_1+\dots+n_\rho=p-\omega,\,n_i\le l_i}\frac{a_1^{n_1}\dots a_\rho^{n_\rho}}{n_1!\dots n_\rho!}=\sigma^*\,.$$

По условию $q\ge 2\sigma^*$. Отсюда $q\ge w$ и, следовательно, $q-(l-1)>q-w\ge\sigma^*$. Значит, среди множеств $S_1,\dots,S_q$ можно выбрать множество S_{n_l}, не совпадающее с множествами $S_{n_1},\dots,S_{n_{l-1}}$ так, что $|(\bigcup_{i=1}^{l-1}S_{n_i})\bigcap S_{n_l}|\le\zeta p$. Лемма доказана.

Лемма 4.8 (Бомбьери) *Пусть q — натуральное число, $\lambda>0$ — действительное число, B — конечное множество, $B_1,\dots,B_q$ — его подмножества такие, что $|B_i|\ge\lambda|B|$. Тогда для всех $t\le\lambda q$ найдутся различные натуральные числа $j_1,\dots,j_t\in[q]$ для которых*

$$|B_{j_1}\bigcap\dots\bigcap B_{j_t}|\ge\left(\lambda-\frac{t}{q}\right)\binom{q}{t}^{-1}|B|\,.$$

Теорема 4.9 *Пусть $K,\eta>0$ — вещественные числа, $\eta\in(0,1/2]$, p — натуральное число и $\Lambda\subseteq\mathbf{F}_2^n$ — произвольное множество из семейства $\mathbf{\Lambda}(4p)$. Пусть также Q — некоторое подмножество $\Lambda\dotplus\Lambda$, $K^*:=\max\{1,K\}$, $p\ge 2^{30}K^*/\eta$ и*

$$T_p(Q)\ge\frac{p^{2p}|Q|^p}{K^p}\,. \tag{53}$$

Предположим, что $p\le\log|\Lambda|/\log\log|\Lambda|$ и

$$|Q|\ge 2^{60+\frac{2}{\eta}}(K^*)^{17}p^3|\Lambda|\cdot\max\left\{(2^{30}(K^*)^{11}p)^{\eta p}|\Lambda|^\eta\log|\Lambda|,\exp\left(\frac{\log(2^{30}(K^*)^{20})\log(\frac{p\log K^*}{\log p})}{\log(\frac{2^{-25}\eta p}{K^*})}\right)\right\}$$

Тогда найдутся множества $\mathcal{L}_1,\mathcal{L}_1',\dots,\mathcal{L}_h,\mathcal{L}_h'$ из Λ такие, что $\mathcal{L}_i\bigcap\mathcal{L}_j'=\emptyset$, $\mathcal{L}_i+\mathcal{L}_i'\subseteq Q$, $i=1,\dots,h$, $j=1,\dots,h$,

$$|\mathcal{L}_i|\ge\frac{\log(\frac{|Q|}{16(K^*)^9|\Lambda|})}{2^{10}\log(2^{20}K^*)},\quad |\mathcal{L}_i'|\ge\frac{1}{2^{10}p^2}\left(\frac{|Q|}{(K^*)^9|\Lambda|}\right)^\eta, \tag{54}$$

$(\mathcal{L}_i+\mathcal{L}_i')\bigcap(\mathcal{L}_j+\mathcal{L}_j')=\emptyset$, $i,j=1,\dots,h$, $i\ne j$ *и*

$$\left|Q\bigcap\Big((\mathcal{L}_1+\mathcal{L}_1')\bigsqcup\dots\bigsqcup(\mathcal{L}_h+\mathcal{L}_h')\Big)\right|\ge\frac{|Q|}{16(K^*)^9}\,. \tag{55}$$

Если же p — произвольное и

$$\log\left(\frac{|Q|}{16(K^*)^9 p|\Lambda|}\right) \geq 2^{20}\log(2^{10}K^*)\log p\,, \tag{56}$$

то найдутся множества $\mathcal{L}_1, \mathcal{L}'_1, \ldots, \mathcal{L}_h, \mathcal{L}'_h$ из Λ, удовлетворяющие всем условиям выше, за исключением неравенства (54), которое должно быть заменено на следующее

$$|\mathcal{L}_i| \geq \min\{2^{-18}\frac{p}{K^*}, 2^{-5}\log\left(\frac{|Q|}{16(K^*)^9 p}\right)\}, \quad |\mathcal{L}'_i| \geq \frac{1}{32p^2}\left(\frac{|Q|}{(K^*)^9|\Lambda|}\right)^{1/2}. \tag{57}$$

Замечание 4.10 Если $K = O(1)$, например $K \leq 1$, то для справедливости неравенств (55), (57) достаточно, чтобы выполнялось более слабое неравенство, чем (56), а именно $|Q| \geq 2^{60+\frac{2}{\eta}}(K^*)^{17}p^3|\Lambda|$.

Доказательство теоремы. Пусть $m = |Q|$, $\beta_1 = 1/4$, $\beta_2 = 1/2$. Пусть также

$$\mathbf{M} = 2^{52+\frac{2}{\eta}}(K^*)^{17}p^3|\Lambda|\cdot\max\left\{(2^{27}(K^*)^{11}p)^{\eta p}|\Lambda|^{\eta}\log|\Lambda|, \exp\left(\frac{\log(2^{24}(K^*)^{20})\log(\frac{p\log K^*}{\log p})}{\log(\frac{2^{-22}\eta p}{K^*})}\right)\right\}.$$

Так как $T_p(Q) \geq p^{2p}|Q|^p/K^p$, то $D_p(Q) \geq p\log(p/K)$. Применяя теорему 3.3 с параметрами $d = 2$ и $C = 1/8$, находим (β_1, β_2)–связное порядка p множество $Q_1 \subseteq Q$ такое, что $m_1 := |Q_1| \geq m/(2K^9)$ и $T_p(Q_1) \geq p^{2p}m_1^p/K^p$. Пусть $a = \lceil|\Lambda|/2\rceil$. Имеем

$$\sum_{\tilde\Lambda\subseteq\Lambda,\,|\tilde\Lambda|=a}\ \sum_{\lambda_1\in\tilde\Lambda,\,\lambda_2\in\Lambda\setminus\tilde\Lambda} Q_1(\lambda_1+\lambda_2) = 2\binom{|\Lambda|-2}{a-1}|Q_1|\,. \tag{58}$$

Из формулы (58) вытекает, что найдется множество $\tilde\Lambda \subseteq \Lambda$, $|\tilde\Lambda| = a$ такое, что $|Q_1\bigcap(\tilde\Lambda + (\Lambda\setminus\tilde\Lambda))| \geq 2m_1\binom{|\Lambda|-2}{a-1}\binom{|\Lambda|}{a}^{-1} = 2m_1\frac{a(|\Lambda|-a)}{|\Lambda|(|\Lambda|-1)} \geq m_1/2$. Положим $\Lambda_1 = \tilde\Lambda$, $\Lambda_2 = \Lambda\setminus\tilde\Lambda$ и $Q_2 = Q_1\bigcap(\Lambda_1+\Lambda_2)$. Выкидывая, если это необходимо, несколько элементов из Q_2, получаем множество $Q_3 \subseteq Q_2$ такое, что $Q_3 = \lceil m_1/2\rceil$. Пусть $m_3 = |Q_3|$. Так как множество Q_1 является (β_1, β_2)–связным порядка p с константой $C = 1/8$, то

$$T_p(Q_3) \geq 2^{-6p}\left(\frac{m_3}{m_1}\right)^{2p}T_p(Q_1) \geq \frac{p^{2p}m_3^p}{(2^7K)^p}\,.$$

Сохраняя все обозначения предложения 4.6, полагая значение параметра M равным $M = 2^7K$ и применяя это предложение к множеству $Q_3 \subseteq \Lambda_1 + \Lambda_2$, находим

$$2^{5p}Xp^{3p}s_2^p\cdot\sum_{r=p-\lceil\delta_0\rceil}^{p}\left(\frac{1}{ps_2}\right)^r\cdot\left(\sum_{S\subseteq[s_1],\,|S|=r}\ \prod_{\alpha\in S}\left(\sum_{\beta\in S}|D_\alpha\bigcap D_\beta|\right)\right) \geq \frac{p^{2p}m_3^p}{2(2^7K)^p}\,. \tag{59}$$

Напомним, что в формуле (59) величина δ_0 равна $\delta_0 = \max\{(p\log(2eM))/\log(|Q_3|/(s_2p)), 1\}$, а число X есть $\max\{\delta_0^{4\delta_0}, 1\}$. Если $m \geq \mathbf{M}$ или m удовлетворяет условию (56), то $\delta_0 \leq \max\{(p\log(2^{10}K))/(2\log p), 1\} \leq p/2$ и $X^{1/p} \leq 2^8K$. Пусть $K_1 = 2^{13}KX^{1/p} \leq 2^{21}K^2$ и пусть либо $m \geq \mathbf{M}$, либо m удовлетворяет

условию (56). Тогда $m_3 \ge 2K_1 p|\Lambda|$. Применяя последнее неравенство и (59) получаем, что найдется натуральное число $p_1 \in [p - \lceil \delta_0 \rceil, p]$ для которого

$$\sum_{S\subseteq[s_1],\,|S|=p_1} \prod_{\alpha\in S} \left(\sum_{\beta\in S} |D_\alpha \bigcap D_\beta| \right) \ge \frac{m_3^{p_1}}{K_1^{p_1}} \,. \tag{60}$$

Пусть $S \subseteq [s_1]$, $|S| = p_1$ — некоторое множество и $\alpha \in S$ — произвольный элемент множества S. Пусть также $\varepsilon = 1/(16K_1)$. Если $M \le 1/2$, то $X = 1$ и используя оценку $p \ge 2^{30}K^*/\eta$ получаем, что $\varepsilon \ge 1/p_1$. Предположим теперь, что $M > 1/2$ и либо $m \ge \mathbf{M}$, либо m удовлетворяет условию (56). В этой ситуации неравенство $\varepsilon \ge 1/p_1$ вытекает из оценки $p \ge 2^{30}K^*/\eta$. Более точный подсчет показывает, что в обоих случаях $\varepsilon \ge 16/(\eta p)$. Определим множества

$$G_{S,\alpha} = \{\ x \in D_\alpha\ :\ \sum_{\beta\in S} D_\beta(x) \ge \varepsilon p_1\ \} \,.$$

Иными словами, $G_{S,\alpha}$ — это множество x из D_α таких, что x принадлежит не менее εp_1 множествам D_β, $\beta \in S$. Имеем

$$\sum_{\beta\in S} |D_\alpha \bigcap D_\beta| = \sum_{x\in\Lambda_2} D_\alpha(x) \sum_{\beta\in S} D_\beta(x) =$$

$$= \sum_{x\in G_{S,\alpha}} D_\alpha(x) \sum_{\beta\in S} D_\beta(x) + \sum_{x\notin G_{S,\alpha}} D_\alpha(x) \sum_{\beta\in S} D_\beta(x) \le p_1|G_{S,\alpha}| + \varepsilon p_1 |D_\alpha| \,. \tag{61}$$

Пусть $\mathcal{S}$ — семейство множеств S, $S \subseteq [s_1]$, $|S| = p_1$ таких, что для всякого $S \in \mathcal{S}$ найдется $\alpha \in S$ для которого одновременно выполнено $|G_{S,\alpha}| \ge \varepsilon |D_\alpha|$ и $|D_\alpha| \ge \varepsilon m_3/s_2$. Пусть также $\bar{\mathcal{S}}$ — семейство множеств S, $S \subseteq [s_1]$, $|S| = p_1$, не принадлежащих семейству $\mathcal{S}$. Докажем, что

$$\sigma_1 := \sum_{S\in\bar{\mathcal{S}}} \prod_{\alpha\in S} \left(\sum_{\beta\in S} |D_\alpha \bigcap D_\beta| \right) \le \frac{m_3^{p_1}}{2K_1^{p_1}} \,. \tag{62}$$

Пусть $Y(S) = \{\alpha \in S\ :\ |G_{S,\alpha}| < \varepsilon |D_\alpha|\}$ и $\bar{Y}(S) = S \setminus Y(S)$. Пользуясь оценкой (61), находим

$$\sigma_1 = \sum_{S\in\bar{\mathcal{S}}} \prod_{\alpha\in\bar{Y}(S),\,|D_\alpha|<\varepsilon m_3/s_2} \left(\sum_{\beta\in S} |D_\alpha \bigcap D_\beta| \right) \cdot \prod_{\alpha\in Y(S)} \left(\sum_{\beta\in S} |D_\alpha \bigcap D_\beta| \right) \le$$

$$\le \sum_{l=0}^{p_1} \sum_{S\subseteq[s_1],\,|S|=p_1,\,|Y(S)|=p_1-l} \left(\frac{\varepsilon p_1 m_3}{s_2} \right)^{|\bar{Y}(S)|} \cdot \prod_{\alpha\in Y(S)} (2\varepsilon p_1 |D_\alpha|) \le$$

$$\le \sum_{l=0}^{p_1} \left(\frac{\varepsilon p_1 m_3}{s_2} \right)^{l} (2\varepsilon p_1)^{p_1-l} \binom{s_1 - (p_1 - l)}{l} \sum_{S'\subseteq[s_1],\,|S'|=p_1-l} \prod_{\alpha\in S'} |D_\alpha| \le$$

$$\le 2^{p_1}\varepsilon^{p_1} \sum_{l=0}^{p_1} \left(\frac{\varepsilon p_1 m_3}{s_2} \right)^{l} p_1^{p_1-l} \frac{s_1^l}{l!} \varepsilon^{-l} \frac{1}{(p_1-l)!} m_3^{p_1-l} \le 2(2e)^{p_1}\varepsilon^{p_1} m_3^{p_1} \sum_{l=0}^{p_1} \frac{p_1!}{l!(p_1-l)!} =$$

$$= 2(4e)^{p_1}\varepsilon^{p_1} m_3^{p_1} \le 2^{4p_1-1}\varepsilon^{p_1} m_3^{p_1} = \frac{m_3^{p_1}}{2K_1^{p_1}}$$

и неравенство (62) доказано. Отсюда

$$\sigma_2 = \sum_{S\in\mathcal{S}} \prod_{\alpha\in S} \left(\sum_{\beta\in S} |D_\alpha \bigcap D_\beta| \right) \ge \frac{m_3^{p_1}}{2K_1^{p_1}} \,. \tag{63}$$

Рассмотрим случай $p \le \log|\Lambda|/\log\log|\Lambda|$. Пусть $u_0 = [\log s_2]$ и $\Lambda^{(j)} = \{\alpha \in [s_1] \,:\, 2^{j-1} \le |D_\alpha| \le 2^j\}$, $j = 1, \dots, u_0$. Из неравенства $\sum_{\alpha\in\Lambda_1} |D_\alpha| \le m$ вытекает оценка $|\Lambda^{(j)}| \le 2m2^{-j}$. Пусть $(j_1, \dots, j_{p_1})$ — некоторый набор из $[u_0]^{p_1}$. Обозначим количество различных чисел в наборе $(j_1, \dots, j_{p_1})$ через $\rho = \rho(j_1, \dots, j_{p_1})$ и пусть элемент j_1^* встречается в этом наборе ровно l_1 раз, элемент j_2^* — ровно l_2 раза, $\dots$, элемент j_ρ^* — ровно l_ρ раз, при этом все элементы $j_1^*, j_2^*, \dots, j_\rho^*$ — различные. Имеем

$$\sigma_2 \le \sum_{S\in\mathcal{S}} p_1^{p_1} \prod_{\alpha\in S} |D_\alpha| = \frac{p_1^{p_1}}{p_1!} \sum_{S\in\mathcal{S}} \sum_{\alpha_1,\dots,\alpha_{p_1} — \text{ различные}} S(\alpha_1)\dots S(\alpha_{p_1})|D_{\alpha_1}|\dots|D_{\alpha_{p_1}}| =$$

$$= p_1^{p_1} \sum_{S\in\mathcal{S}} \sum_{j_1,\dots,j_{p_1}=1}^{u_0} \frac{1}{l_1!\dots l_\rho!} \times$$

$$\times \sum_{\alpha_1\in\Lambda^{(j_1)},\dots,\alpha_{p_1}\in\Lambda^{(j_{p_1})},\, \alpha_1,\dots,\alpha_{p_1} — \text{ различные}} S(\alpha_1)\dots S(\alpha_{p_1})|D_{\alpha_1}|\dots|D_{\alpha_{p_1}}| \,. \tag{64}$$

Из формулы (64) вытекает, что найдется набор $(j_1, \dots, j_{p_1})$ для которого

$$\sum_{S\in\mathcal{S},\, S=\{s^{(1)},\dots,s^{(p_1)}\},\, s^{(j)}\in\Lambda^{(j)}} \prod_{\alpha\in S} |D_\alpha| \ge \frac{l_1!\dots l_\rho!}{p_1^{p_1}u_0^{p_1}} \cdot \frac{m_3^{p_1}}{4K_1^{p_1}} \,.$$

Пользуясь определением множеств $\Lambda^{(j)}$, получаем, что

$$q_0 := |\{S\in\mathcal{S} \,:\, S = \{s^{(1)},\dots,s^{(p_1)}\},\, s^{(j)}\in\Lambda^{(j)}\}| \ge \frac{l_1!\dots l_\rho!}{p_1^{p_1}u_0^{p_1}2^{j_1+\dots+j_{p_1}}} \cdot \frac{m_3^{p_1}}{4K_1^{p_1}} \,.$$

Из принципа Дирихле вытекает, что найдется $\alpha \in [s_1]$ для которого выполнено

$$q := |\{S\in\mathcal{S} \,:\, S = \{s^{(1)},\dots,s^{(p_1)}\},\, s^{(j)}\in\Lambda^{(j)},\, \alpha\in S\}| \ge \frac{l_1!\dots l_\rho!}{p_1^{p_1}u_0^{p_1}2^{j_1+\dots+j_{p_1}}} \cdot \frac{m_3^{p_1}}{4s_1K_1^{p_1}} \,.$$

Пусть $A_i = \Lambda^{(j_i)}$, $i = 1, \dots, p_1$ и $A_i^* = \Lambda^{(j_i^*)}$, $i = 1, \dots, \rho$. Мы хотим применить лемму 4.7 с параметром $w = [\log(m_3/s_2)/(\varepsilon^2 p_1 \log(2^6/\varepsilon^2))]$ к множествам A_i, A_i^*. Так как $m \ge \mathbf{M}$ и $m_3 \ge m/(8K^9)$, то

$$q \ge \frac{l_1!\dots l_\rho!}{p_1^{p_1}u_0^{p_1}2^{j_1^*l_1+\dots+j_\rho^*l_\rho}} \cdot \frac{m_3^{p_1}}{4s_1K_1^{p_1}} \ge 2 \sum_{\omega=\lceil\zeta p_1\rceil}^{p_1} \frac{(p_1w)^\omega}{\omega!} \sum_{n_1+\dots+n_\rho=p_1-\omega,\, n_i\le l_i} \frac{|A_1^*|^{n_1}\dots|A_\rho^*|^{n_\rho}}{n_1!\dots n_\rho!} = 2\sigma^* \,. \tag{65}$$

Действительно, по условию $m \ge \mathbf{M} \ge p_1ws_2$. Отсюда

$$2^{j_1^*l_1+\dots+j_\rho^*l_\rho}\sigma^* \le 2^{p_1} \sum_{\omega=\lceil\zeta p_1\rceil}^{p_1} \frac{(p_1w)^\omega}{\omega!} \sum_{n_1+\dots+n_\rho=p_1-\omega,\, n_i\le l_i} \frac{s_2^\omega m^{p_1-\omega}}{n_1!\dots n_\rho!} \le$$

$$\le 2^{p_1} m^{p_1} \sum_{\omega=\lceil \zeta p_1 \rceil}^{p_1} \frac{(p_1 w)^\omega}{\omega!} \left(\frac{s_2}{m}\right)^\omega \frac{\rho^{p_1-\omega}}{(p_1-\omega)!} \le 2^{4p_1} \left(\frac{\rho}{p_1}\right)^{p_1(1-\zeta)} w^{\zeta p_1} m^{p_1(1-\zeta)} s_2^{\zeta p_1} \qquad (66)$$

(при выводе последней оценки формулы (66) мы пользовались тождеством $1/(\omega!(p-\omega)!) = \binom{p}{w}/p!$). Теперь чтобы убедиться в справедливости (65), достаточно проверить неравенство

$$m_3 \ge 2^7 u_0 K_1 w^\zeta p_1 m^{1-\zeta} s_1^{1/p_1} s_2^\zeta \ge 32 \left(\frac{\rho^{p_1(1-\zeta)} p_1^{\zeta p_1}}{l_1! \dots l_\rho!}\right)^{1/p_1} u_0 K_1 w^\zeta m^{1-\zeta} s_1^{1/p_1} s_2^\zeta \,, \qquad (67)$$

которое легко вытекает из оценок $\varepsilon \ge 16/(\eta p)$, $m_3 \ge m/(8K^9)$ и

$$m \ge \mathbf{M} \ge 2^{44} (K^*)^4 p |\Lambda|^{1+\eta} \log|\Lambda| (2^{27}(K^*)^{11} p)^{\eta p} \ge |\Lambda| w p \cdot (s^{1/p_1} \log|\Lambda|\, 2^{27} (K^*)^{11} p^2)^{1/\zeta} \,.$$

Применяя лемму 4.7 к A_i, A_i^*, находим множества $S_1^*, \dots, S_w^* \in \mathcal{S}$ такие, что для всех $l = 2, 3, \dots, w$ выполнено $|(\bigcup_{i=1}^{l-1} S_i^*) \bigcap S_l^*| \le \zeta p_1$. При этом $|G_{S_i^*,\alpha}| \ge \varepsilon |D_\alpha|$, $i = 1, \dots, w$ и $|D_\alpha| \ge \varepsilon m_3/s_2$. Применяя лемму Бомбьери к множествам $G_{S_1^*,\alpha}, \dots, G_{S_w^*,\alpha} \subseteq D_\alpha$ с параметром $t = [\varepsilon w/2]$, находим индексы $i_1 < \dots < i_t$ из $[w]$ такие, что для множества $G^* = G_{S_{i_1}^*,\alpha} \cap \dots \cap G_{S_{i_t}^*,\alpha}$ имеем $|G^*| \ge \varepsilon \binom{w}{t}^{-1} |D_\alpha|/2$. Пусть x — произвольный элемент D_α и $\Gamma_i(x) = \{\beta \in S_i^* \ : \ x \in D_\beta\}$. Ясно, что для всякого $x \in G_{S_i^*,\alpha}$ выполнено $|\Gamma_i(x)| \ge \varepsilon p_1$. Пусть $E = \bigcup_{i=1}^w S_i^*$ и $I = \{i_1, \dots, i_t\}$. Очевидно, $|E| \le w p_1$. Рассмотрим множество

$$Z = \{\ x \in D_\alpha \ : \ x \text{ принадлежит не менее } \frac{\varepsilon p_1 t}{2} \textit{ различным} \text{ множествам } D_\beta,\ \beta \in E \ \} \,.$$

Докажем, что $G^* \subseteq Z$. Пусть $x \in G^*$. Тогда x принадлежит множествам D_β, $\beta \in \bigcup_{i \in I} \Gamma_i(x)$. Оценим мощность $\bigcup_{i \in I} \Gamma_i(x)$. Имеем

$$|\bigcup_{i\in I} \Gamma_i(x)| = |\bigcup_{i \in I\setminus\{i_t\}} \Gamma_i(x)| + |\Gamma_{i_t}(x)| - |(\bigcup_{i \in I\setminus\{i_t\}} \Gamma_i(x)) \bigcap \Gamma_{i_t}(x)| \ge$$

$$\ge |\bigcup_{i \in I\setminus\{i_t\}} \Gamma_i(x)| + \varepsilon p_1 - |(\bigcup_{i \in I\setminus\{i_t\}} S_i^*) \bigcap S_{i_t}^*| \ge |\bigcup_{i \in I\setminus\{i_t\}} \Gamma_i(x)| + \varepsilon p_1 - \zeta p_1 \ge \dots \ge \frac{\varepsilon p_1 t}{2} \,.$$

Откуда $G^* \subseteq Z$ и, следовательно, $|Z| \ge |G^*| \ge \varepsilon \binom{w}{t}^{-1} |D_\alpha|/2$. Пусть $l = [\varepsilon p_1 t/4]$. Тогда

$$Z \subseteq \bigcup_{r_1,\dots,r_l \in E \text{ — различные}} \left(D_{r_1} \bigcap \dots \bigcap D_{r_l}\right) \,.$$

Значит, найдется набор индексов $r_1 < \dots < r_l$ из E для которого

$$|D_{r_1} \bigcap \dots \bigcap D_{r_l}| \ge \binom{p_1 w}{l}^{-1} |Z| \ge \binom{p_1 w}{l}^{-1} \binom{w}{t}^{-1} \frac{\varepsilon^2 m_3}{2 s_2} \ge \frac{1}{2^8 p^2} \left(\frac{m}{(K^*)^9 |\Lambda|}\right)^\eta \,.$$

Положим $\mathcal{L}_1 = \{\lambda_{r_1}, \dots, \lambda_{r_l}\}$ и $\mathcal{L}_1' = D_{r_1} \bigcap \dots \bigcap D_{r_l}$. Тогда $\mathcal{L}_1 \bigcap \mathcal{L}_1' = \emptyset$, $\mathcal{L}_1 + \mathcal{L}_1' \subseteq Q_3 \subseteq Q$ и

$$|\mathcal{L}_1| = l \ge \frac{\log(\frac{m_3}{s_2})}{32 \log(\frac{2^8}{\varepsilon^2})} \ge \frac{\log(\frac{m}{8(K^*)^9|\Lambda|})}{2^{10} \log(2^{20} K^*)} \,.$$

Дальнейшее доказательство представляет собой итеративную процедуру. Если $|\mathcal{L}_1+\mathcal{L}_1'| \geq |Q_3|/2$, то закончим нашу процедуру. В противном случае рассмотрим множество $Q_3' = Q_3 \setminus (\mathcal{L}_1+\mathcal{L}_1')$ и применим к нему рассуждения выше. Найдем множества $\mathcal{L}_2 \subseteq \Lambda_1$, $\mathcal{L}_2' \subseteq \Lambda_2$ такие, что $\mathcal{L}_2 \bigcap \mathcal{L}_2' = \emptyset$, $\mathcal{L}_2+\mathcal{L}_2' \subseteq Q_3' \subseteq Q$ и для мощностей множеств $\mathcal{L}_2$, $\mathcal{L}_2'$ справедливы оценки

$$|\mathcal{L}_2| \geq \frac{\log(\frac{|Q|}{16(K^*)^9|\Lambda|})}{2^8\log(2^{12}K^*)}, \quad |\mathcal{L}_2'| \geq \frac{1}{2^{10}p^2}\left(\frac{|Q|}{(K^*)^9|\Lambda|}\right)^{\eta}.$$

Из диссоциативности множества Λ и того факта, что $\Lambda_1 \bigcap \Lambda_2 = \emptyset$ получаем свойство $(\mathcal{L}_1+\mathcal{L}_1') \bigcap (\mathcal{L}_2+\mathcal{L}_2') = \emptyset$. Если $|\mathcal{L}_1+\mathcal{L}_1'|+|\mathcal{L}_2+\mathcal{L}_2'| \geq |Q_3|/2$, то заканчиваем наш алгоритм, иначе повторяем предыдущие рассуждения. В конце–концов мы построим множества $\mathcal{L}_1, \mathcal{L}_1', \ldots, \mathcal{L}_h, \mathcal{L}_h'$ для которых выполнено неравенство (55).

Нам осталось рассмотреть ситуацию когда справедливо неравенство (56), но либо оценка $p \leq \log|\Lambda|/\log\log|\Lambda|$ не выполнена, либо $m < \mathcal{M}$. Если справедливо неравенство (56), то величина X равна единице. Из неравенства (63) и простой оценки $|D_\alpha| \leq s_2$ вытекает, что количество множеств в семействе $\mathcal{S}$ не меньше $m_3^{p_1}/(2K_1^{p_1}p_1^{p_1}s_2^{p_1})$. Из условия (56) находим, что последняя величина не меньше единицы. Следовательно, существует множество S и $\alpha \in [s_1]$ для которых выполнено $|G_{S,\alpha}| \geq \varepsilon|D_\alpha|$ и $|D_\alpha| \geq \varepsilon m_3/s_2$. Пусть

$$Z = \{\ x \in D_\alpha\ :\ x \text{ принадлежит не менее } \varepsilon p_1 \textit{ различным} \text{ множествам } D_\beta,\ \beta \in S\ \}.$$

Тогда $G_{S,\alpha} \subseteq Z$. Имеем $[\varepsilon p_1/2] \geq 2^{-18}\frac{p}{K^*} \geq 1$. Положим $l = \min\{[\varepsilon p_1/2], [\log(m_3/s_2)/8]\}$. Имеем

$$Z \subseteq \bigcup_{r_1,\ldots,r_l \in S \text{ — различные}} \left(D_{r_1} \bigcap \cdots \bigcap D_{r_l}\right).$$

Значит, найдется набор индексов $r_1 < \cdots < r_l$ из S для которого

$$|D_{r_1} \bigcap \cdots \bigcap D_{r_l}| \geq \binom{\lceil \varepsilon p_1 \rceil}{l}^{-1} |G_{S,\alpha}| \geq \frac{\varepsilon^2}{16^l}\frac{m_3}{s_2} \geq \frac{1}{16p^2}\left(\frac{m}{(K^*)^9|\Lambda|}\right)^{1/2}.$$

Полагая $\mathcal{L}_1 = \{\lambda_{r_1}, \ldots, \lambda_{r_l}\}$ и $\mathcal{L}_1' = D_{r_1} \bigcap \cdots \bigcap D_{r_l}$ и действуя как выше, получаем требуемый результат. Теорема доказана.

Замечание 4.11 Легко видеть, что оценка для мощности множеств $\mathcal{L}_i$ из неравенства (54), вообще говоря, не может быть усилена. Приведем соответствующий пример и схему доказательства оптимальности последнего неравенства. Сохраним все обозначения предыдущей теоремы. Пусть $K > 1$ — фиксированная константа, $\Lambda_1, \Lambda_2 \subseteq \Lambda$, $\Lambda_1 \bigcap \Lambda_2 = \emptyset$, $Q \subseteq \Lambda_1+\Lambda_2$ — некоторое множество, свойства которого мы опишем ниже, $m := |Q|$. Пусть также $|\Lambda_1| := s$, $|\Lambda_2| = [mK/s]$. Предположим, что множества $D_\alpha \subseteq \Lambda_2$, $\alpha = 1, \ldots, s$ выбраны случайным образом так, что для любого $\alpha \in [s]$ каждый элемент из Λ_2, принадлежит множеству D_α с вероятностью $1/K$. Ясно, что с положительной вероятностью $|D_\alpha| \approx m/s$, $\alpha = 1, \ldots, s$ $|D_\alpha \bigcap D_\beta| \approx m/(sK)$, $\alpha \neq \beta$, $\alpha, \beta = 1, \ldots, s$, а также

$$T_p(Q) \gg p^{2p} \sum_{S \subseteq [s],\, |S|=p} \prod_{\alpha \in S} \left(\sum_{\beta \in S} |D_\alpha \bigcap D_\beta|\right) \gg \frac{p^{2p}m^p}{K^p}.$$

и неравенство (53) выполнено. Тем не менее, если $\mathcal{L} \subseteq \Lambda_2$, $|\mathcal{L}| = l > 0$, $\Lambda_1 + \mathcal{L} \subseteq Q$, то $|\mathcal{L}| \leq |D_{\alpha_1} \bigcap \cdots \bigcap D_{\alpha_l}| \ll m/(sK^l)$ откуда получаем оценку $l \ll \log(m/s)/\log K$.

Выведем простое следствие из теоремы 4.9.

Предложение 4.12 *Пусть $K, \eta > 0$ — вещественные числа, $\eta \in (0, 1/2]$, $K \geq 1$, p, d — натуральные числа, $d \geq 3$ и $\Lambda \subseteq \mathbf{F}_2^n$ — произвольное множество из семейства $\mathbf{\Lambda}(2dp)$. Пусть также Q — некоторое подмножество $d\dot{\Lambda}$, $|\Lambda| \geq 8d^2$, $p \geq 2^{50+8d}K^d/\eta$ и*

$$T_p(Q) \geq \frac{p^{dp}|Q|^p}{K^{(d-1)p}}\,. \tag{68}$$

Предположим, что $p \leq \log|\Lambda|/\log\log|\Lambda|$ и

$$|Q| \geq 2^{60+50d+\frac{2}{\eta}} M^{17} K^{2d} p^3 d^{-d} |\Lambda|^{d-1} \times$$

$$\times \max\left\{(2^{30}M^{11}p)^{\eta p}|\Lambda|^{\eta}\log|\Lambda|, \exp\left(\frac{\log(2^{30}M^{20})\log(\frac{p\log M}{\log p})}{\log(\frac{2^{-25}\eta p}{M})}\right)\right\},$$

где $M = 2^{13}(8K)^{d-1}$. Тогда найдутся множества $\mathcal{L}, \mathcal{L}' \subseteq \Lambda$ и элементы $\lambda_1 + \dots + \lambda_{d-2}$ из Λ такие, что $\mathcal{L}_i \bigcap \mathcal{L}'_j = \emptyset$, $\lambda_i \notin \mathcal{L}, \mathcal{L}'$,

$$|\mathcal{L}| \geq \frac{\log(\frac{|Q|d^d}{2^{140+80d}K^{3d}|\Lambda|^{d-1}})}{2^{10}\log(2^{40}8^dK^d)}, \quad |\mathcal{L}'| \geq \frac{1}{2^{10}p^2}\left(\frac{|Q|d^d}{2^{140+80d}K^{3d}|\Lambda|^{d-1}}\right)^{\eta}, \tag{69}$$

и

$$\lambda_1 + \dots + \lambda_{d-2} + \mathcal{L} + \mathcal{L}' \subseteq Q\,. \tag{70}$$

Доказательство. Пусть $m = |Q|$, $\beta_1 = 4^{-d}$, $\beta_2 = 4^{-d} + 1/\sqrt{m}$ и $a = \lceil|\Lambda|/d\rceil$. Так как $T_p(Q) \geq p^{dp}|Q|^p/K^{(d-1)p}$, то $D_p(Q) \geq (d-1)p\log(p/K)$. Применяя теорему 3.3 с параметрами d и $C = 2^{-6}$, находим (β_1, β_2)–связное порядка p множество $Q_1 \subseteq Q$ такое, что $m_1 := |Q_1| \geq m/(dK^{2(d-1)})$ и $T_p(Q_1) \geq p^{dp}m_1^p/K^{(d-1)p}$. Пусть также $a_i = a$, $i = 1, \dots, d-1$ и $a_d = |\Lambda| - \sum_{i=1}^{d-2} a_i$. Так как $|\Lambda| \geq 8d^2$, то $|\Lambda|/(2d) \leq a_d \leq |\Lambda|/d$. Легко видеть, что

$$Q(x) = \left(\frac{d!(|\Lambda|-d)!}{(a_1-1)!\dots(a_d-1)!}\right)^{-1} \sum_{S_1,\dots,S_d,\,|S_i|=a_i,\,\bigsqcup_{i=1}^d S_i = \Lambda} \left(Q\bigcap(S_1+\dots+S_d)\right)(x)\,. \tag{71}$$

Из формулы (71) вытекает, что найдется набор непересекающихся множеств $S_1, \dots, S_d \subseteq \Lambda$ таких, что

$$|Q_1\bigcap(S_1+\dots+S_d)| \geq m_1 d!\frac{(|\Lambda|-d)!}{(a_1-1)!\dots(a_d-1)!}\left(\frac{|\Lambda|!}{a_1!\dots a_d!}\right)^{-1} =$$

$$= m_1 d!\frac{a_1\dots a_d}{|\Lambda|(|\Lambda|-1)\dots(|\Lambda|-d+1)} \geq \frac{1}{2}e^{-d}m_1\,. \tag{72}$$

Положим $Q_2 = Q_1\bigcap(S_1+\dots+S_d)$.

Пусть d_1 — натуральное число, $d_1 \leq d$, $l_1, \dots, l_{d_1}$ — различные числа из $[d]$, $L = \{l_1, \dots, l_{d_1}\}$, $\overline{L} = [d] \setminus L$. Пусть также $w_{l_i} \in S_{l_i}$ — произвольные элементы, $i \in [d_1]$, $\vec{w} = (w_{l_1}, \dots, w_{l_{d_1}})$ — вектор и $W = \{w_{l_1}, \dots, w_{l_{d_1}}\}$. Определим множества $D(W)$, $Q(W)$

$$D(W) = \{\sum_{i\in\overline{L}}\lambda_i \ :\ \sum_{i\in\overline{L}}\lambda_i + \sum_{i\in L}w_i \in Q'\}, \quad Q(W) = \{q \in Q' \ :\ q = \sum_{i\in\overline{L}}\lambda_i + \sum_{i\in L}w_i\}$$

Ясно, что $D(W) = Q(W) + \sum_{i\in L}w_i$. Иногда мы будем писать $D(\vec{w})$, $Q(\vec{w})$ вместо $D(W)$, $Q(W)$. По условию множество Λ принадлежит семейству $\mathbf{\Lambda}(2dp)$. Отсюда легко видеть,

что множества $Q(W\bigcup\{l_1\})$ и $Q(W\bigcup\{l_2\})$, $\lambda_1 \neq \lambda_2$ — не пересекаются. Кроме того, $Q(W\bigcup\{l\}) \subseteq Q(W)$. Следовательно, для всех $x \geq 1$ выполнено

$$\sum_{\lambda} |Q(W\bigcup\{\lambda\})|^x \leq |Q(W)|^{x-1} \sum_{\lambda} |Q(W\bigcup\{\lambda\})| = |Q(W)|^x \,. \tag{73}$$

Пусть $x_1, x_2 \geq 1$ — произвольные числа. Применяя оценку (73) и неравенство Коши–Буняковского, находим

$$\sum_{\lambda} |Q(W_1\bigcup\{\lambda\})|^{x_1/2} |Q(W_2\bigcup\{\lambda\})|^{x_2/2} \leq |Q(W_1)|^{x_1/2} |Q(W_1)|^{x_2/2} \,. \tag{74}$$

Ясно, что справедлив аналог формулы (74) и для большего числа множеств $Q(W_i\bigcup\{\lambda\})$.

Обозначим через Q_2' объединение множеств $Q_2(\vec{a})$, $\vec{a} \in S_1 \times \ldots \times S_{d-2}$ таких, что $|Q_2(\vec{a})| \geq |Q_2|/(4|S_1|\ldots|S_{d-2}|)$. Тогда $|Q_2'| \geq |Q_2|/2$. Выкидывая, если это необходимо, несколько элементов из Q_2, получаем множество $Q' \subseteq Q_2$ такое, что $|Q'| = \lceil 4^{-d} m_1 \rceil$. Опишем процедуру выбрасывания точек из Q_2 более подробнее. Эта процедура состоит из двух этапов. Сначала мы выбрасываем множества $Q_2(\vec{a})$ целиком, до тех пор пока это возможно, то есть пор пока выкидывание нового $Q_2(\vec{a})$ не приведет к множеству мощности меньше, чем $\lceil 4^{-d} m_1 \rceil$. Затем необходимо выбросить по одному элементу из множеств $Q_2(\vec{a})$, каждый раз выкидывая точку у $Q_2(\vec{a})$ наибольшей мощности. Легко видеть, что при такой процедуре мощности всех оставшихся классов уменьшаться не более чем в четыре раза, кроме той ситуации, когда останется лишь один класс. При последнем варианте для единственного класса $Q_2(\vec{a})$ выполнено $|Q_2(\vec{a})| \geq 4^{-d} m_1 \geq |Q_2|/(16|S_1|\ldots|S_{d-2}|)$. Пусть $m' = |Q'|$. Так как множество Q_1 является (β_1, β_2)–связным порядка p с константой $C = 2^{-6}$, то

$$T_p(Q') \geq 2^{-12p} \left(\frac{m'}{m_1}\right)^{2p} T_p(Q_1) \geq \frac{p^{dp} m'^p}{2^{12p} 4^{dp} K^{(d-1)p}} \,. \tag{75}$$

Рассмотрим уравнение

$$q_1 + \cdots + q_{2p} = 0 \,, \tag{76}$$

где $q_i \in Q'$, $i = 1, \ldots, 2p$. Обозначим через σ' число решений уравнения (76). Пусть $\vec{a}_1, \ldots, \vec{a}_{d-2}$ — произвольные векторы из $S_1 \times \ldots \times S_{d-2}$ и пусть $\vec{v} = (\vec{a}_1, \ldots, \vec{a}_{2p})$. Обозначим через $\sigma(\vec{v}) = \sigma(\vec{a}_1, \ldots, \vec{a}_{2p})$ — множество решений уравнения (76) таких, что $q_i \in Q(\vec{a}_i)$, $i \in [2p]$. Далее, обозначим через $\mathcal{M}$ — семейство разбиений отрезка $[2p]$ на p множеств $\{C_1, \ldots, C_p\}$, $|C_j| = 2$, $j \in [p]$. Пусть также $\mathcal{V}$ — всевозможные наборы разбиений $\{\mathcal{M}_1, \ldots, \mathcal{M}_{d-2}\}$, $\mathcal{M}_i \in \mathcal{M}$, $i \in [d-2]$. Ясно, что количество различных ноборов в $\mathcal{V}$ не превосходит $p^{p(d-2)}$. По определению вектор $\vec{v} = (\vec{a}_1, \ldots, \vec{a}_{2p})$ принадлежит $\mathcal{V}$, если для любого $j = 1, \ldots, d-2$ и произвольного элемента C разбиения $\mathcal{M}_j$, $C = \{\alpha, \beta\}$ выполнено $\lambda_\alpha = \lambda_\beta$. Имеем

$$\sigma' \leq \sum_{\mathcal{V}} \sum_{(\vec{a}_1, \ldots, \vec{a}_{d-2}) \in \mathcal{V}} |\sigma((\vec{a}_1, \ldots, \vec{a}_{d-2}))| = \sum_{\mathcal{V}} \sum_{\vec{v} \in \mathcal{V}} |\sigma(\vec{v})| \,. \tag{77}$$

Применяя лемму 2.2, получаем

$$|\sigma(\vec{v})| \leq \left(\prod_{i=1}^{2p} T_p(\vec{a}_i)\right)^{1/2p} \,. \tag{78}$$

Предположим, что для всех векторов $\vec{a}$ из $S_1 \times \ldots \times S_{d-2}$ выполнено

$$T_p(\vec{a}) \le \frac{p^{2p}|Q(\vec{a})|^p}{M^p}\,, \qquad (79)$$

где $M = 2^{13}(8K)^{(d-1)}$. Тогда из последнего неравенства и неравенств (77), (78), находим

$$\sigma' \le \frac{p^{2p}}{M^p} \sum_{\mathcal{V}} \sum_{(\vec{a}_1,\ldots,\vec{a}_{d-2})\in\mathcal{V}} \prod_{i=1}^{2p} |Q(\vec{a}_i)|^{1/2}\,. \qquad (80)$$

Применяя несколько раз формулы (73), (74), получаем

$$\sigma' \le \frac{p^{2p}}{M^p} \sum_{\mathcal{V}} m^p \le \frac{p^{dp} m^p}{M^p}\,,$$

что противоречит неравенству (75). Следовательно, найдется вектор $\vec{a}$ из $S_1 \times \ldots \times S_{d-2}$ для которого неравенство (79) не выполнено и

$$|Q(\vec{a})| \ge \frac{|Q_2|}{4|S_1|\ldots|S_{d-2}|} \ge \frac{m}{64de^d(4K)^{2(d-1)}|S_1|\ldots|S_{d-2}|} \ge \frac{md^d}{2^{50d}K^{2d}|\Lambda|^{d-2}}\,.$$

Пусть $\vec{a} = (a_1, \ldots, a_{d-2})$. Положим $\lambda_i = a_i$, $i \in [d-2]$. Применяя теорему 4.9 к множеству $Q(\vec{a}) \subseteq S_{d-1} + S_d$, находим множества $\mathcal{L}$, $\mathcal{L}'$ для которых справедливы неравенства (69) и включение (70). Предложение доказано.

5. Добавление.

В этом параграфе мы докажем аналог теоремы 1.3 в произвольной абелевой группе G. Справедлива теорема.

Теорема 5.1 *Пусть δ, α — действительные числа, $0 < \alpha \le \delta$, A — произвольное подмножество G мощности $\delta|G|$, $k \ge 2$ — натуральное число и множество $\mathcal{R}_\alpha$ определено равенством (3). Пусть также $B \subseteq \mathcal{R}_\alpha$ — произвольное множество. Тогда*

$$T_k(B) \ge \frac{\delta\alpha^{2k}}{\delta^{2k}}|B|^{2k}\,.$$

Доказательство. Пусть $r \in \widehat{G}$. Определим величину $\theta(r) \in \mathbf{S}^1$ равенством $\widehat{A}(r) = |\widehat{A}(r)|\theta(r)$. По определению множества $\mathcal{R}_\alpha$ имеем

$$\alpha N|B| \le \sum_{r\in B} |\widehat{A}(r)| = \sum_x \sum_r B(r)\theta^{-1}(r)e(-r\cdot x)\,.$$

Применяя неравенство Гельдера, находим

$$(\alpha N|B|)^{2k} \le \sum_x \left|\sum_r B(r)\theta^{-1}(r)e(-r\cdot x)\right|^{2k} \cdot \left(\sum_x A(x)\right)^{2k-1} = NT_k(B\cdot\theta^{-1})(\delta N)^{2k-1}\,. \qquad (81)$$

Докажем простую лемму.

Лемма 5.2 *Пусть $f : G \to \mathbb{C}$ — произвольная функция и $k \ge 2$ — целое число. Тогда $T_k(f) \le T_k(|f|)$.*

Доказательство леммы. Применяя неравенство треугольника легко видеть, что для любых функций $g, h : G \to \mathbb{C}$ выполнено $|(g*h)(x)| \le (|g|*|h|)(x)$, $x \in G$. Отсюда и итеративного определения величины $T_k(f)$ вытекает утверждение леммы. Лемма доказана.

Применяя лемму, получаем из (81), что $T_k(B) \ge T_k(B\cdot\theta^{-1}) \ge \frac{\delta\alpha^{2k}}{\delta^{2k}}|B|^{2k}$. Теорема доказана.

Список литературы

[1] *Gowers W. T.* Rough structure and classification // Geom. Funct. Anal., Special Volume - GAFA2000 "Visions in Mathematics", Tel Aviv, (1999) Part I, 79–117.

[2] *Nathanson M.* Additive number theory. Inverse problems and the geometry of sumsets / Graduate Texts in Mathematics 165, Springer–Verlag, New York, 1996.

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

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

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

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

[7] *Green B.* Arithmetic Progressions in Sumsets // Geom. Funct. Anal., **12** (2002) no. 3, 584–597.

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

[10] *Green B.* Structure Theory of Set Addition // ICMS Instructional Conference in Combinatorial Aspects of Mathematical Analysis, Edinburgh March 25 — April 5 2002.

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

[12] *Sanders T.* An application of a local version of a Chang's theorem // http://www.arXiv:math.CA/0607668.

[13] *Sanders T.* Three terms arithmetic progressions in sumsets // http://www.arXiv:math.NT/0611304.

[14] *Sanders T.* The Littlewood–Gowers problem // http://www.arXiv:math.CA/0605522.

[15] *Sanders T.* Notes on Bourgain's refinement of Chang's quantitative version of Ruzsa's proof of Freiman's theorem // Preprint, 2007.

[16] *Sanders T.* Notes on a preprint of Shkredov's // Prepint, 2007.

[17] *Yudin A. A.* On the measure of large values of a trigonametric sum // Number Theory (under the edition of G.A. Freiman, A.M. Rubinov, E.V. Novosyolov), Kalinin State Univ., Moscow (1973), 163–174.

[18] *Besser A.* Sets of integers with large trigonometric sums // Astérisque **258** (1999), 35–76.

[19] *Lev V. F.* Linear Equations over $\mathbb{F}_p$ and Moments of Exponential Sums // Duke Mathematical Journal **107** (2001), 239–263.

[20] *Konyagin S. V., Lev V. F.* On the distribution of exponential sums // Integers: Electronic Journal of Combinatorial Number Theory **0** # A01, (2000).

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

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

[23] *Schoen T.* Linear equations in $\mathbb{Z}_p$ // LMS, submitted for publication.

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

[25] *Минк Х.* Перманенты / М.: "Наука", 1981.

[26] *Bourgain J.* Roth's Theorem on Progressions Revisited // Preprint, 2007.

[27] *Вон Р.* Метод Харди–Литтлвуда / М.: "Мир", 1985.

[28] *Shkredov I. D.* On sets of large exponential sums // Doklady of Russian Academy of Sciences, 411, N 4, 455–459, 2006.

[29] *Shkredov I. D.* On sets of large exponential sums // Izvestiya of Russian Academy of Sciences, 72, N 1, 2008.

[30] *Шкредов И. Д.* О множествах с малым удвоением // Математические заметки, представлено в печать.