УДК 517.5

С. В. Конягин (Мат. ин-т РАН, Москва, Россия),
И. Д. Шкредов (Моск. ун-т им. М. В. Ломоносова, Россия)

ОБ ОДНОМ РЕЗУЛЬТАТЕ Ж. БУРГЕНА*

In a linear space of dimension n over the field $\mathbb{F}_2$, we construct a set A of a given density such that the Fourier transform of A is large on a large set and the intersection of A with any subspace of small dimension is small. The results obtained show, in a certain sense, the sharpness of one theorem of J. Bourgain.

У лінійному просторі розмірності n над полем $\mathbb{F}_2$ побудовано множину A заданої щільності, в якої перетворення Фур'є є великим на великій множині і таким, що перетин A з будь-яким підпростором невеликої розмірності є малим. Одержані результати показують у певному сенсі точність однієї теореми Ж. Бургена.

1. Введение. Пусть N, $k \geq 3$ — натуральные числа. Пусть также

$$a_k(N) = \frac{1}{N} \max \Big\{ |A| \colon A \subseteq \{1, 2, \ldots, N\},$$

$$A \text{ не содержит арифметических прогрессий длины } k \Big\},$$

где $|A|$ — мощность множества A. Поведение величины $a_k(N)$ при фиксированном k и $N \to \infty$ изучалось в работах различных авторов (см. [1 – 7, 9 – 12, 14, 15, 25, 26, 31, 34, 35]). На сегодняшний день наилучший результат об оценке сверху функции $a_3(N)$ принадлежит Ж. Бургену [35]. Он доказал, что

$$a_3(N) \ll \frac{(\log \log N)^3}{(\log N)^{2/3}}. \tag{1}$$

В своей работе Бурген применил оригинальный подход, связанный с использованием множеств Бора (см. работы [34, 35], а также [20, 25, 33]). Напомним определение множества Бора. Пусть G — конечная абелева группа с аддитивной групповой операцией $+$. Обозначим через $\widehat{G}$ двойственную группу для G. Иными словами, пусть $\widehat{G}$ — группа гомоморфизмов ξ из G в $\mathbb{R}/\mathbb{Z}$, $\xi \colon x \to \xi \cdot x$. Известно, что группа $\widehat{G}$ изоморфна G.

Определение 1.1. *Пусть S — некоторое подмножество группы $\widehat{G}$ и $\varepsilon > 0$ — действительное число. Множеством Бора $B = B(S, \varepsilon)$ называется множество*

$$B(S, \varepsilon) = \big\{ n \in G \colon \|\xi \cdot n\| < \varepsilon \text{ для всех } \xi \in S \big\},$$

где $\| \cdot \|$ — расстояние до нуля на торе $\mathbb{R}/\mathbb{Z}$.

Множество Бора $B(S, \varepsilon)$ называется *регулярным* (см. [30, 34]), если для всех $\eta \leq 2^{-4}|S|^{-1}$ выполнено

$$1 - 2^4|S|\eta \leq \frac{|B(S, (1+\eta)\varepsilon)|}{|B(S, \varepsilon)|} \leq 1 + 2^4|S|\eta.$$

Кроме множеств Бора в своей работе Бурген получил несколько новых результатов о множествах больших тригонометрических сумм (результаты по этой

* Первый автор поддержан фондом Освальда Веблена (Oswald Veblen Fund), второй — грантом Российского фонда фундаментальных исследований № 06-01-00383, грантом Президента РФ МК-1959.2009.1, грантом им. П. Делиня (фонд Бальзана 2004) и грантом НШ-691.2008.1.

тематике могут быть найдены, например, в работах [16, 21, 30, 35, 43 – 45]). Напомним основные определения. Пусть f — некоторая функция из G в $\mathbb{C}$. Обозначим через $\widehat{f}(\xi)$ преобразование Фурье функции f

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

где $e(x) = e^{2\pi i x}$. Пусть δ, α — действительные числа, $0 < \alpha \le \delta \le 1$, и A — некоторое подмножество G мощности $\delta|G|$. Будем обозначать той же буквой A характеристическую функцию этого множества. Рассмотрим множество $\mathcal{R}_\alpha$ больших тригонометрических сумм A

$$\mathcal{R}_\alpha = \mathcal{R}_\alpha(A) = \big\{ r \in \widehat{G} \colon |\widehat{A}(r)| \ge \alpha |G| \big\}. \tag{2}$$

Вопрос о строении таких множеств относится к проблематике обратных задач аддитивной теории чисел (см. [13, 32]). Ясно, что можно также определить аналог множества $\mathcal{R}_\alpha(f)$ для произвольной функции $f \colon \mathbb{C} \to G$.

При рассмотрении множества больших тригонометрических сумм оказывается полезным понятие диссоциативности (см. [16, 21, 30, 35, 44, 45]). Пусть $R \subseteq G$ — некоторое множество, $R = -R$ и $\{0\} \in R$. Множество $\Lambda = \{\lambda_1, \ldots, \lambda_{|\Lambda|}\} \subseteq G$ называется *R-диссоциативным*, если из включения

$$\sum_{i=1}^{|\Lambda|} \varepsilon_i \lambda_i \in R, \tag{3}$$

где $\varepsilon_i \in \{-1, 0, 1\}$, следует, что все ε_i равны нулю. Если $R = \{0\}$, то множество Λ называется *диссоциативным*. Как упоминалось выше, Бурген в работе [35] использовал подход, связанный с множествами Бора, а также с множествами больших тригонометрических сумм. С помощью своего метода он доказал следующий результат (мы приведем формулировку из работы [30]).

Теорема 1.1. *Пусть S — некоторое подмножество $\widehat{G}$, ε, δ, α — положительные числа, $\alpha \le \delta$, $B = B(S, \varepsilon)$ — регулярное множество Бора и $A \subseteq B(S, \varepsilon)$ — любое множество, $|A| = \delta |B(S, \varepsilon)|$. Пусть также $B' = B(S, \varepsilon')$ — множество Бора,*

$$2 \left(\frac{\alpha}{2(1 + |S|)} \right)^{64} \varepsilon \le \varepsilon' \le 4 \left(\frac{\alpha}{2(1 + |S|)} \right)^{64} \varepsilon,$$

$R = \big\{ r \colon |\widehat{B'}(r)| \ge |B'|/3 \big\}$, Λ — R-диссоциативное подмножество множества $\big\{ r \colon |\widehat{A}(r)| \ge \alpha |B| \big\}$ и $|\Lambda| \ge 2^7 \dfrac{\delta(1 + \log(1/\delta))}{\alpha}$. Тогда найдутся множество $I \subseteq \Lambda$, $|I| \le \dfrac{\alpha |\Lambda|}{2^4 \delta (1 + \log(1/\delta))}$, и множество Бора $B'' = B(S \cup I, \varepsilon'')$, $\varepsilon'' \ge (\delta/(2(1 + |S|)))^{64} \varepsilon$, такие, что для некоторого $x \in G$ выполнено

$$\big| A \cap (B'' + x) \big| \ge \big(\delta + 2^{-12} \alpha |I| \big) |B''|. \tag{4}$$

Кроме работы [35] теорема 1.1 имеет несколько приложений (см., например, [30]). В настоящей работе мы покажем, что теорема 1.1 является, в некотором смысле, неулучшаемой.

Вначале переформулируем результат Бургена в группе $\mathbb{F}_2^n$ (обсуждение плодотворности изучения задач аддитивной теории чисел в группах $\mathbb{F}_q^n$ (q — простое число) см. в обзоре [24]).

Пусть n и N — натуральные числа, $N = 2^n$. Рассмотрим конечную абелеву группу $\mathbb{F}_2^n = (\mathbb{Z}/2\mathbb{Z})^n$, $|\mathbb{F}_p^n| = N$. Группа $\mathbb{F}_2^n$ является векторным пространством со скалярным произведением

$$x \cdot y = \vec{x} \cdot \vec{y} = \langle \vec{x}, \vec{y} \rangle = x_1 y_1 + \ldots + x_n y_n \pmod 2.$$

Преобразование Фурье функции $f\colon \mathbb{F}_2^n \to \mathbb{C}$ задается формулой

$$\widehat{f}(r) = \sum_{x \in \mathbb{F}_p^n} f(x)(-1)^{\langle r,x \rangle}.$$

В группе $\mathbb{F}_2^n$ понятию множества Бора соответствует *аффинное подпространство*. Пусть $\vec{v}_1, \ldots, \vec{v}_k$ — некоторые линейно независимые векторы и $\varepsilon_1, \ldots, \varepsilon_k$ — произвольные элементы $\mathbb{F}_2$. Аффинным подпространством коразмерности k называется множество

$$P = P_{\varepsilon_1,\ldots,\varepsilon_k}(\vec{v}_1, \ldots, \vec{v}_k) = \left\{\vec{x} \in \mathbb{F}_2^n \colon \langle \vec{x}, \vec{v}_1 \rangle = \varepsilon_1, \ldots, \langle \vec{x}, \vec{v}_k \rangle = \varepsilon_k \right\}.$$

Если все ε_i равны нулю, то иногда будем писать $P(\vec{v}_1, \ldots, \vec{v}_k)$ вместо $P_{0,\ldots,0}(\vec{v}_1, \ldots \ldots, \vec{v}_k)$. Для множества $W = (w_1, \ldots, w_{|W|})$ пусть $P(W)$ обозначает $P(w_1, \ldots \ldots, w_{|W|})$. Коэффициенты Фурье множества $P = P(W)$ вычисляются чрезвычайно просто. Пусть L — линейное пространство размерности k, натянутое на векторы $\vec{v}_1, \ldots, \vec{v}_k$, и $\vec{r} \in \mathbb{F}_2^n$ — произвольный вектор. Ясно, что $L = P^\perp := \left\{\vec{x} \colon \langle \vec{x}, \vec{p} \rangle = 0 \ \forall \vec{p} \in P\right\}$ и для любого $r \in L$ выполнено $\widehat{P}(r) = |P|$. Далее, из равенства Парсеваля

$$\sum_{r \in \mathbb{F}_2^n} |\widehat{P}(r)|^2 = |P|N$$

следует, что $\widehat{P}(r) = 0$ для любого $r \notin L$. Иными словами,

$$\widehat{P}(r) = L(r)|P|. \tag{5}$$

Таким образом, $|\widehat{P}(r)|$ равен либо нулю, либо $|P|$.

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

Определение 1.2. *Пусть $R \subseteq \mathbb{F}_2^n$ — некоторое множество, $\{0\} \in R$. Множество $\Lambda = \{\lambda_1, \ldots, \lambda_{|\Lambda|}\} \subseteq \mathbb{F}_2^n$ принадлежит семейству $\mathbf{\Lambda}_R(k)$, если из включения*

$$\sum_{i=1}^{|\Lambda|} \varepsilon_i \lambda_i \in R, \tag{6}$$

где $\varepsilon_i \in \{0, 1\}$, а число ненулевых ε_i не превышает k, следует, что все ε_i равны нулю. Если $R = \{0\}$, то множество Λ принадлежит семейству $\mathbf{\Lambda}(k)$.

Будем обозначать через $M_1, M_2, \ldots$ абсолютные положительные константы.

Теорема 1.2 (Бурген, группа $\mathbb{F}_2^n$)**.** *Пусть δ, α — действительные числа, $0 < < \alpha \le \delta$, $P_0 = P_0(\vec{v}_1, \ldots, \vec{v}_h) \subseteq \mathbb{F}_2^n$ — подпространство, L_0 — линейная оболочка векторов $\vec{v}_1, \ldots, \vec{v}_h$ и $A \subseteq P_0$ — некоторое множество, $|A| = \delta|P_0|$. Пусть также*

Λ — L_0-диссоциативное подмножество $\{r\colon |\widehat{A}| \geq \alpha|P_0|\}$ и $|\Lambda| \geq M_1 \dfrac{\delta \log(1/\delta)}{\alpha}$. Тогда найдутся множество $I \subseteq \Lambda$,

$$M_2 \frac{\alpha|\Lambda|}{2\delta \log(1/\delta)} \leq |I| \leq M_2 \frac{\alpha|\Lambda|}{\delta \log(1/\delta)}, \tag{7}$$

подпространство $P = P(I)$ и вектор $x \in \mathbb{F}_2^n$ такие, что

$$|A \cap (P + x)| \geq (\delta + M_3 \alpha |I|)\, |P|. \tag{8}$$

Сформулируем наш результат.

Теорема 1.3. *Пусть δ, α, ε — действительные числа, $0 < \alpha \leq 2^{-1000/(1-\varepsilon)^2}\delta$, $\delta \leq 2^{-4}$, $\alpha \geq 40N^{-1/2}$, $\varepsilon \in (0,1)$, и*

$$\frac{\delta}{\alpha} \log\left(\frac{\delta}{\alpha}\right) \leq 2^{-10} n. \tag{9}$$

Тогда найдется множество $A \subseteq \mathbb{F}_2^n$, $|A| = \delta_0 N$, $\delta \leq \delta_0 \leq 4\delta$, такое, что

$$\big|\mathcal{R}_\alpha(A)\big| \geq 2^{-600} \left(\frac{\delta}{\alpha}\right)^2 \log\left(\frac{1}{\delta}\right). \tag{10}$$

Далее, пусть Λ — максимальное диссоциативное подмножество $\mathcal{R}_\alpha(A)$ из семейства $\mathbf{\Lambda}\big(4[\delta\alpha^{-1}]\big)$. Тогда

$$2^{-600} \left(\frac{\delta}{\alpha}\right)^{(31+\varepsilon)/16} \log\left(\frac{1}{\delta}\right) \leq |\Lambda| \leq \left(\frac{\delta}{\alpha}\right)^{(31+\varepsilon)/16} \log\left(\frac{1}{\delta}\right). \tag{11}$$

Кроме того, для любого множества $I \subseteq \mathcal{R}_\alpha(A)$ такого, что

$$|I| \leq 2^{-600} \left(\frac{\delta}{\alpha}\right)^{(31+\varepsilon)/32}, \tag{12}$$

и произвольного $x \in \mathbb{F}_2^n$ выполнено

$$\big|A \cap (P(I) + x)\big| \leq \big(\delta_0 + 2^{1000}\alpha|I|\big)\, |P(I)|. \tag{13}$$

Легко видеть, что при определенных условиях на параметры δ и α ограничения на величину $|I|$ из (12) гораздо шире, чем неравенства (7). Таким образом, теорема 1.3 показывает, что теорема Бургена 1.2 не может быть улучшена.

***Замечание* 1.1.** Более аккуратный анализ нашего доказательства показывает, что условия на мощность множества I в теореме 1.3 могут быть заменены еще более слабыми. Кроме того, справедлив аналог приведенного результата, в котором множество Λ является диссоциативным, а не просто принадлежащим семейству $\mathbf{\Lambda}\big(4[\delta\alpha^{-1}]\big)$.

***Замечание* 1.2.** Если отказаться от выполнения неравенства (11), то, используя технику так называемых „множеств уровня” И. Ружи (см. работы [21, 29]), можно легко построить множество A, для которого выполняется (13). Действительно, в соответствующем примере Ружи $\mathcal{R}_\alpha(A) = \{0\} \bigsqcup \Lambda \bigsqcup (-\Lambda)$, где Λ — диссоциативное множество (см. [45]). Поэтому если $I \subseteq \mathcal{R}_\alpha(A)$, то легко видеть, что мощность

пересечения линейной оболочки I и $\mathcal{R}_\alpha(A)$ не превышает по порядку мощности I. Тем не менее в работе [35] Бурген использовал аналог теоремы 1.2 в случае, когда $|\Lambda| = o\big(|\mathcal{R}_\alpha(A)|\big)$ (точнее, когда мощность $\mathcal{R}_\alpha(A)$ близка к своему экстремальному значению δ/α^2). Одна из главных целей настоящей статьи — показать, что и в этом случае результат Бургена не может быть усилен.

Коротко остановимся на доказательстве основного результата статьи.

Опишем сначала множество $\mathcal{R}_\alpha(A)$ из теоремы 1.3. Пусть Λ_1, Λ_2 — некоторые непересекающиеся множества такие, что их объединение является диссоциативным множеством. Выберем случайным образом множество Q из $\Lambda_1 + \Lambda_2$, равномерно и независимо: любой элемент принадлежит Q с некоторой вероятностью q. Мы хотим добиться того, чтобы $\mathcal{R}_\alpha(A)$ было равно $\{0\} \bigsqcup Q$ (на самом деле в теореме 1.3 используется немного другая конструкция). Далее, используя случайные свойства множества Q, доказываем, что для любого подпространства Y не очень большой размерности ρ мощность его пересечения с Q по порядку равна ρ (см. следствие 4.1). Иными словами, в пересечении Y с Q не содержится слишком много „лишних” точек. Грубо говоря, из этого факта и следует неравенство (13).

Чтобы построить множество A с $\mathcal{R}_\alpha(A) = \{0\} \bigsqcup Q$, мы используем модернизированную технику множеств уровня И. Ружи, развитую Б. Грином. Напомним, что оригинальное множество уровня Ружи $S(s_1, \ldots, s_m)$, $s_1, \ldots, s_m \in (\mathbb{Z}/N\mathbb{Z}) \setminus \{0\}$, определяется следующим образом:

$$S(s_1, \ldots, s_m) = \left\{ x \in \mathbb{Z}/N\mathbb{Z} \colon \sum_{j=1}^{m} \cos(a_j x) > \eta\sqrt{m} \right\} =$$

$$= \left\{ x \colon g\left(\sum_{j=1}^{m} \cos(a_j x) \right) = 1 \right\}, \qquad (14)$$

где $\eta > 0$ — некоторое число и функция $g(x)$ такая, что $g(x) = 1$, если $x > \eta\sqrt{m}$, и $g(x) = 0$, если $x \le \eta\sqrt{m}$. В работе [21] (см. также [22, 23]) Б. Грин аппроксимирует функцию $g(x)$ полиномом $p_{d,S}(x)$ степени d, по порядку равной $|S|$, а затем рассматривает функцию $f(x) = p_{d,S}\left(\sum_{j=1}^{m} \cos(a_j x)\right)$. После этого он доказывает, что $\mathcal{R}_\alpha(f) = \{0\} \bigsqcup S$, и использует в качестве характеристической функции искомого множества A функцию, которая, в некотором смысле, приближает $f(x)$ (см. лемму 2.1).

Этот метод работает, если точки $s_1, \ldots, s_m$ выбраны специальным образом, например если множество $S = \{s_1, \ldots, s_m\}$ является диссоциативным. Внимательный анализ доказательства из статьи [21] показывает, что, грубо говоря, достаточно потребовать выполнения неравенств вида

$$T_p(S) := \big|\{z_1 + \ldots + z_{2p} = 0 \colon z_i \in S\}\big| \le C^p p^p |S|^p, \quad p = 1, \ldots, d, \qquad (15)$$

где C — некоторая абсолютная константа. Для диссоциативных множеств оценка (15), разумеется, выполнена, что следует из классического неравенства Рудина [27, 28]. Мы хотим использовать в качестве $\{s_1, \ldots, s_m\}$ множество $Q \subseteq \Lambda_1 + \Lambda_2$, которое, конечно, не является диссоциативным. Тем не менее, используя технику из работы [46] и тот факт, что множество Q случайно, мы доказываем справедли-

вость неравенства (15) для всех p, не превышающих по порядку $\sqrt{m}$. Безусловно, это еще не позволяет построить множество A, поскольку, как отмечалось выше, степень полинома $p_{d,S}(x)$ есть величина $d \gg m$. Чтобы избежать последнего жесткого условия, мы выбираем в качестве $p_{d,S}(x)$ многочлен Чебышева $T_l(x)$ (а точнее, функцию $1/2 + 1/2 \cdot T_l(x)$), где степень l не превышает $\sqrt{m}$. Это позволяет построить функцию $f(x)$, и, следовательно, искомое множество A.

В пункте 2, используя многочлены Чебышева, мы строим множество A с $\mathcal{R}_\alpha(A) = \{0\} \bigsqcup Q$. В пункте 3 доказываем более сильную версию оценки (15) для случая специальных подмножеств Q сумм двух диссоциативных множеств. Основной результат здесь — это лемма 3.5. Наконец, в последней части статьи нам лишь остается убедиться в том, что случайные подмножества сумм диссоциативных множеств обладают всеми свойствами, которые требуются в утверждениях двух предыдущих пунктов.

То же самое множество A, что и в теореме 1.3, дает ответ на один вопрос Т. Сандерса о множествах больших тригонометрических сумм. В пункте 4 мы доказывем следующую теорему.

Теорема 1.4. *Пусть δ, α, ε_1, ε_2 — действительные числа, $0 < \alpha \leq \leq 2^{-1000/(1-\varepsilon_1)^2}\delta$, $\delta \leq 2^{-4}$, $\varepsilon_1 \in (0,1)$, $\varepsilon_2 \in (0, 2^{-8})$, $\alpha \geq 40N^{-1/2}$ и*

$$\frac{\delta}{\alpha} \log\left(\frac{\delta}{\alpha}\right) \leq 2^{-10} n. \tag{16}$$

Тогда найдется множество $A \subseteq \mathbb{F}_2^n$, $\delta N \leq |A| \leq 4\delta N$, такое, что

$$\big|\mathcal{R}_\alpha(A)\big| \geq 2^{-1000} \left(\frac{\delta}{\alpha}\right)^2 \log\left(\frac{1}{\delta}\right). \tag{17}$$

Далее, пусть Λ — максимальное диссоциативное подмножество $\mathcal{R}_\alpha(A)$ из семейства $\mathbf{\Lambda}\big(4[\delta\alpha^{-1}]\big)$. Тогда

$$2^{-1000} \left(\frac{\delta}{\alpha}\right)^{(31+\varepsilon_1)/16} \log(1/\delta) \leq |\Lambda| \leq \left(\frac{\delta}{\alpha}\right)^{(31+\varepsilon_1)/16} \log\left(\frac{1}{\delta}\right) \tag{18}$$

и для произвольного подмножества $I \subseteq \mathcal{R}_\alpha(A)$, $|I| \leq (\delta/\alpha)^{(15+\varepsilon_1-\varepsilon_2)/8}$, выполнено

$$\big|\mathcal{R}_\alpha(A) \cap \operatorname{Span}(I)\big| \leq \frac{2^{10}|I|}{\varepsilon_2}. \tag{19}$$

Таким образом, теорема 1.4 показывает, что можно построить множество больших тригонометрических сумм, которое не обладает свойством „непрерывности”. В нашем примере все $\mathcal{R}_\alpha(A)$ порождено некоторым множеством Λ, но оболочка любого множества мощности меньше чем $|\Lambda|^{1-\xi}$, где $\xi > 0$ — некоторая константа, $\xi = \xi(\varepsilon_1, \varepsilon_2)$, практически не пересекается с $\mathcal{R}_\alpha(A)$.

Мы выражаем благодарность Т. Сандерсу за неоднократные и чрезвычайно полезные обсуждения рассматриваемых вопросов. Авторы благодарны Институту высших исследований (Принстон, США) за гостеприимство и создание прекрасных условий для работы.

2. Множества больших тригонометрических сумм со специальными свойствами. Пусть p — натуральное число. Через $[p]$ обозначим отрезок натурального

ряда $[p] = \{1, 2, \ldots, p\}$. Напомним, что мы пишем $[u]$ также для целой части действительного числа u. Надеемся, это не вызовет затруднений у читателя. Обозначим через $A_1 \dot{+} A_2 \dot{+} \ldots \dot{+} A_d$ множество, образованное суммой различных элементов из множеств $A_1, \ldots, A_d$. Множество, состоящее из суммы d различных элементов множества A, обозначим через $d^{\wedge}A$.

Напомним определения свертки и линейной оболочки множества.

Определение 2.1. *Пусть $f, g\colon \mathbb{F}_2^n \to \mathbb{C}$ — произвольные функции. Обозначим через $(f * g)(x)$ функцию*

$$(f * g)(x) = \sum_s f(s)g(x+s). \tag{20}$$

Далее, определим по индукции операцию $*_k$, где k — натуральное число, $*_k = *(*_{k-1})$. Положим функцию $f *_0 f$ равной $f(x)$.

Определение 2.2. *Пусть $I \subseteq \mathbb{F}_2^n$ — произвольное множество. Обозначим через $\mathrm{Span}\,(I)$ линейную оболочку множества I. Другими словами, $\mathrm{Span}\,(I)$ — это множество всевозможных линейных комбинаций элементов I.*

Для построения множеств со специально устроенным $\mathcal{R}_\alpha$ нам потребуется следующая лемма (см. [21, 36]).

Лемма 2.1. *Пусть G — абелева группа, $|G| = N$ и $f\colon G \to [0,1]$ — произвольная функция. Тогда найдется множество $E \subseteq G$ с $|E| = \left[\sum_{x\in G} f(x)\right]$ такое, что для всех $r \in G \setminus \{0\}$ выполнено $|\widehat{E}(r) - \widehat{f}(r)| \le 20\sqrt{N}$.*

Пусть d, t — натуральные числа, $n = td$ и $e_1, \ldots, e_n$ — стандартный базис $\mathbb{F}_2^n$. Обозначим через $\mathcal{L}_w$ подпространство, натянутое на векторы $e_{(w-1)d+1}, \ldots$ $\ldots, e_{(w-1)d+d}$, $w = 1, \ldots, t$. Если $E \subseteq \mathbb{F}_2^d$ — некоторое множество, то обозначим через E_w копии этого множества в пространствах $\mathcal{L}_w$, $w = 1, \ldots, t$.

Пусть $Q \subseteq \mathbb{F}_2^n$ — произвольное множество, g — целое неотрицательное, а $p \ge 2$ — натуральное число. Пусть $q_1^*, \ldots, q_g^*$ — некоторые элементы множества Q. Обозначим через $\bar{N}_p(Q; q_1^*, \ldots, q_g^*)$ число решений уравнения

$$q_1 + \ldots + q_p = q_1^* + \ldots + q_g^*, \tag{21}$$

где $q_i \in Q$, $i \in [p]$. Если g равно нулю, то будем считать, что вместо суммы $q_1^* + \ldots + q_g^*$ в правой части (21) стоит нуль. В этом случае будем обозначать величину $\bar{N}_p(Q)$ через $N_p(Q)$.

Сформулируем основной результат этого пункта.

Предложение 2.1. *Пусть δ, α, C_1 — действительные числа, $C_1 \ge 1$, $\delta \le$ $\le 1/16$, $\delta \ge 1/N$, $\alpha \ge 80N^{-1/4}$, $0 < \alpha \le 2^{-1000}\delta$, $t = [\log(1/2\delta)]$, $n = td$, $K \ge 2^5 C_1$, $c = 2^7$ — параметры и*

$$\frac{\delta}{\alpha}\log\left(\frac{\delta}{\alpha}\right) \le 2^{-10}n. \tag{22}$$

Пусть Q — некоторое подмножество $\mathbb{F}_2^n$, $2^6K^{-4}\delta^2\alpha^{-2}c^{-4} \le |Q| \le 2^{-6}K^{-4}\delta^2 \times$ $\times\alpha^{-2}c^{-2}$, $|Q| \ge 16c^2K^2$, такое, что для всех натуральных p, $2 \le p \le \sqrt{|Q|}$, любого натурального g и произвольных $q_1^*, \ldots, q_g^* \in Q$, $q_1^* + \ldots + q_g^* \ne 0$, выполнено

$$\bar{N}_p(Q; q_1^*, \ldots, q_g^*) \le C_1^p p^{p/2+1}|Q|^{(p-1)/2}, \tag{23}$$

а для всех нечетных p величина $N_p(Q)$ равна нулю. Тогда существует множество $A \subseteq \mathbb{F}_2^n$, $\delta N \le |A| \le 4\delta N$, для которого

1) $|\mathcal{R}_\alpha(A)| \ge (cK)^{-4} \left(\dfrac{\delta}{\alpha}\right)^2 \log(1/\delta)$,

2) $\mathcal{R}_\alpha(A) = \{0\} \bigsqcup \left(\bigsqcup_{w=1}^{t} Q_w \right)$, *где Q_w — копии множества Q в пространствах $\mathcal{L}_w$, $w = 1, \ldots, t$.*

Пусть ρ — натуральное число, M, K' — действительные числа, $M \ge 1$, $K' \ge$ $\ge 2^5 MK$, $2^6 (K')^{-4} \delta^2 \alpha^{-2} c^{-4} \le |Q| \le 2^{-6} (K')^{-4} \delta^2 \alpha^{-2} c^{-2}$, $|Q| \ge 16 c^2 K'^2$, $|Q| \ge$ $\ge 8M$ и $\rho \le 2^{-10} \sqrt{|Q|}/M^3$. Пусть также I — некоторое множество, $I \subseteq \mathcal{R}_\alpha(A)$, $Y = \operatorname{Span}(I)$, $\dim Y = \rho$ такие, что для всех $p \le \sqrt{|Q|}$ выполнено

$$\sum_{x \in \mathbb{F}_2^n} (Q *_{p-1} Q)(x) Y(x) \le M^p \rho p^{(p-1)/2} m^{(p-1)/2}. \tag{24}$$

Тогда существует множество $A \subseteq \mathbb{F}_2^n$, $\delta N \le |A| \le 4\delta N$, для которого кроме пунктов 1, 2 *выполнено следующее неравенство: для произвольного $z \in \mathbb{F}_2^n$ имеем*

$$\big|A \cap (P(I) + z)\big| \le \big(\delta_0 + 2^{20} c^2 K' M^3 \alpha \rho\big) |P(I)|, \tag{25}$$

где $\delta_0 := |A|/N$, $\delta \le \delta_0 \le 4\delta$.

Доказательство. Пусть $m = |Q|$, $j_0 = \big[\sqrt{m}/(4cK)\big]$, $l = 2j_0 + 1 =$ $= 2\big[\sqrt{m}/(4cK)\big] + 1$. Ясно, что $j_0 = [l/2]$ и $l = 2j_0 + 1$ — нечетное число. Пусть также $T_l(y) = \cos(l \arccos y)$ — многочлен Чебышева. Имеем (см. [37] или [38, с. 4], § 1.1, формула (1.10))

$$T_l(y) = \frac{l}{2} \sum_{j=0}^{[l/2]} (-1)^j \frac{(l-j-1)!}{j!(l-2j)!} 2^{l-2j} y^{l-2j}.$$

Будем считать, что в каждом пространстве $\mathcal{L}_w$ находятся копии множества $Q =$ $= \{q_1, \ldots, q_m\}$. Обозначим копии множества Q через Q_w, $w = 1, \ldots, t$. Пусть также

$$f_w(x) = \frac{1}{2} + \frac{1}{2} T_l \left(\frac{1}{Km} \sum_{i=1}^{m} (-1)^{\langle x, q_i \rangle} \right), \quad x \in \mathcal{L}_w, \quad w = 1, \ldots, t.$$

Пусть функции f_w продолжены на все пространство $\mathbb{F}_2^n$ формулой $f_w(x + x^\perp) :=$ $:= f_w(x)$, где $x \in \mathcal{L}_w$, $x^\perp \in \mathcal{L}_w^\perp$. Тогда для всех $w \in [t]$ и любого $x \in \mathbb{F}_2^n$ выполнено $0 \le f_w(x) \le 1$. Далее, пусть

$$f(x) = \prod_{w=1}^{t} f_w(x). \tag{26}$$

Очевидно, что $f(x) \in [0, 1]$, $x \in \mathbb{F}_2^n$. Кроме того,

$$\widehat{f}(r) = \prod_{w=1}^{t} \widehat{f}_w(r), \quad r \in \mathbb{F}_2^n, \tag{27}$$

где функции f_w снова рассматриваются как заданные на пространствах $\mathcal{L}_w$. Из формулы (27) видно, что для того, чтобы найти все коэффициенты Фурье функции

f, достаточно определить коэффициенты Фурье функций f_w. Для всех $w \in [t]$ имеем

$$f_w(x) = \frac{1}{2} + \frac{l}{4} \sum_{j=0}^{[l/2]} \frac{(-1)^j}{(Km)^{l-2j}} \frac{(l-j-1)!}{j!(l-2j)!} 2^{l-2j} \left(\sum_{i=1}^{m} (-1)^{\langle x, q_i \rangle} \right)^{l-2j}. \qquad (28)$$

Поскольку l — нечетное число и $N_v(Q) = 0$ для нечетных v, из формулы (28) следует, что $\widehat{f}(0) = \sum_x f(x) = 2^{-t}N \geq 2\delta N$. Найдем ненулевые коэффициенты Фурье функции $f(x)$. Как было упомянуто выше, для этого достаточно определить коэффициенты Фурье функций f_w. Зафиксируем w и будем считать, для простоты, что копии Q_w множества Q в пространствах $\mathcal{L}_w$ — это просто множество Q.

Пусть $N' = 2^d$, $\alpha' = \alpha 2^t$. Ясно, что если r не принадлежит множеству $h^{\wedge}Q$, $h \leq l$ — нечетное, то $\widehat{f_w}(r) = 0$. Покажем сначала, что $Q \subseteq \mathcal{R}_{\alpha'}(f_w)$. В сумме (28) рассмотрим слагаемое с $j = [l/2] = j_0$. Пусть

$$f_w^{(0)}(x) = \frac{l}{2Km} (-1)^{j_0} \sum_{i=1}^{m} (-1)^{\langle x, q_i \rangle}.$$

Тогда $\widehat{f}_w^{(0)}(r) = (-1)^{j_0} \dfrac{lN'}{2Km} Q(r)$. Отсюда для всех $q \in Q$ выполнено $\left|\widehat{f}_w^{(0)}(q)\right| = \dfrac{lN'}{2Km}$. Используя неравенство $|Q| \leq 2^{-6}(K')^{-4}\delta^2\alpha^{-2}c^{-2}$ и учитывая, что $t = \left[\log(1/2\delta)\right]$, получаем оценку

$$\left|\widehat{f}_w^{(0)}(q)\right| = \frac{lN'}{2Km} \geq \frac{\sqrt{m}N'}{8cK^2m} = \frac{N'}{8cK^2\sqrt{m}} \geq \frac{\alpha N'}{\delta} \geq 2\alpha 2^t N' = 2\alpha' N'.$$

Пусть $f_w^{(1)}(x) = f_w(x) - f_w^{(0)}(x)$. Если мы покажем, что для всех $q \in Q$ выполняется неравенство $\left|\widehat{f}_w^{(1)}(q)\right| \leq \alpha' N'$, то включение $Q \subseteq \mathcal{R}_{\alpha'}(f_w)$ будет доказано. Пусть $q^* \in h^{\wedge}Q$, $q^* \neq 0$. Оценим модуль коэффициента Фурье $\widehat{f}_w^{(1)}(q^*)$. Имеем

$$\widehat{f}_w^{(1)}(q^*) = \frac{lN'}{4} \sum_{j=0}^{j_0-1} \frac{(-1)^j}{(Km)^{l-2j}} \frac{(l-j-1)!}{j!(l-2j)!} 2^{l-2j} \bar{N}_{l-2j}(Q; q^*). \qquad (29)$$

Так как $l = 2j_0 + 1$, для всех $j \leq j_0 - 1$ выполнено $-l/2 + j \leq -3/2$. Используя последнее замечание, оценки $l \leq \sqrt{m}/2$, $K \geq 2^5 C_1$, формулу Стирлинга и неравенство (23), находим

$$\left|\widehat{f}_w^{(1)}(q^*)\right| \leq$$

$$\leq \frac{lN'}{4} \sum_{j=0}^{j_0-1} \frac{1}{(Km)^{l-2j}} \frac{(l-j-1)!}{j!(l-2j)!} (2C_1)^{l-2j} m^{(l-2j-1)/2} (l-2j)^{(l-2j+2)/2} \leq$$

$$\leq \frac{lN'}{4} \sum_{j=0}^{j_0-1} \left(\frac{2C_1}{K}\right)^{l-2j} l^{l-2j-1} \frac{(l-2j)^{(l-2j+2)/2}}{(l-2j)!} m^{-l/2+j-1/2} \leq$$

$$\leq \frac{lN'}{4} \sum_{j=0}^{j_0-1} \left(\frac{2C_1 e}{K}\right)^{l-2j} l^{l-2j-1} (l-2j)^{-l/2+j+1} m^{-l/2+j-1/2} \leq$$

$$\le \frac{lN'}{8}\sum_{j=0}^{j_0-1} l^{l-2j-1}(l-2j)^{-l/2+j+1}m^{-l/2+j-1/2} \le$$

$$\le \frac{N'}{8\sqrt{m}}\sum_{j=0}^{j_0-1}\left(\frac{l}{\sqrt{m}}\right)^{l-2j} \le \frac{l^3}{2m^2}N'. \tag{30}$$

По условию $l = 2\big[\sqrt{m}/(4cK)\big] + 1 \le \sqrt{m}/(cK)$ и $m \ge 2^6K^{-4}\delta^2\alpha^{-2}c^{-4} \ge$ $\ge 2^6K^{-6}\delta^2\alpha^{-2}c^{-6}$, так как $K, c > 1$. Кроме того, $\alpha' = \alpha 2^t$, где $t = \big[\log(1/2\delta)\big]$. Значит, $\alpha' \ge 2^{-2}\alpha\delta^{-1}$ и

$$\frac{l^3}{2m^2} \le \frac{1}{2(cK)^3\sqrt{m}} \le \frac{\alpha}{16\delta} \le \frac{\alpha'}{4}.$$

Применяя последнюю оценку и неравенство (30), имеем

$$\big|\widehat{f}_w^{(1)}(q^*)\big| \le \frac{\alpha' N'}{4}. \tag{31}$$

Отсюда $Q \subseteq \mathcal{R}_{\alpha'}(f_w)$. Если $q^* \in h^{\wedge}Q$, $q^* \ne 0$, $q^* \notin Q$, то $\widehat{f}_w^{(0)}(q^*) = 0$. Следовательно, из неравенства (31) вытекает равенство $\mathcal{R}_{\alpha'}(f_w) = \{0\}\bigsqcup Q$. Используя формулу (27), получаем, что для всех $r \in \bigsqcup_{w=1}^t Q_w$, $r \ne 0$, выполнено

$$\big|\widehat{f}(r)\big| \ge 2^{-(t-1)}\frac{3}{2}\alpha' N \ge 2\alpha N.$$

Применяя теперь лемму 2.1 к функции $f(x)$ и используя оценку $\alpha \ge 80N^{-1/4}$, находим множество A такое, что для множества $\mathcal{R}_\alpha(A)$ справедливо включение $\{0\}\bigsqcup\Big(\bigsqcup_{w=1}^t Q_w\Big) \subseteq \mathcal{R}_\alpha(A)$. Если $r \notin \{0\}\bigsqcup\Big(\bigsqcup_{w=1}^t Q_w\Big)$, то согласно формуле (31) для некоторого $w \in [t]$ выполнено $|\widehat{f}_w(r)| \le \dfrac{\alpha' N'}{4}$. Используя тождество (27), получаем $\big|\widehat{f}(r)\big| \le \left(\dfrac{1}{2}\right)^{t-1}\dfrac{\alpha' N}{4} = \dfrac{\alpha N}{2}$. Снова применяя лемму 2.1 и оценку $\alpha \ge 80N^{-1/4}$, находим $\big|\widehat{A}(r)\big| \le \dfrac{3\alpha N}{4} < \alpha N$. Значит, $\mathcal{R}_\alpha(A) =$ $= \{0\}\bigsqcup\Big(\bigsqcup_{w=1}^t Q_w\Big)$. Отсюда и из неравенства $|Q| \ge 2^6K^{-4}\delta^2\alpha^{-2}c^{-4}$ получаем оценку из пункта 1.

Нам осталось убедиться в выполнении неравенства (25). Возьмем $K' \ge 2^5KM$ и используем все рассуждения, приведенные выше. Пусть $P = P(I)$ и $z = z_1 + \ldots$ $\ldots + z_t$, $z_w \in \mathcal{L}_w$, $w \in [t]$. Имеем

$$\big|A \cap (P+z)\big| = \frac{1}{N}\sum_{r\in\mathbb{F}_2^n}\widehat{A}(r)\widehat{P}(r)(-1)^{\langle r,z\rangle}.$$

Для подсчета коэффициентов Фурье множества P применим формулу (5). Тогда

$$\big|A \cap (P+z)\big| = \sum_x f(x)P(x+z) + \sigma_0 = \sigma' + \sigma_0, \tag{32}$$

где

$$|\sigma_0| \le 20\sqrt{N}\frac{1}{N}\sum_r |\widehat{P}(r)| \le 20\sqrt{N}\frac{1}{N}|P|\,|P^{\perp}| \le 20\sqrt{N} \le 20\alpha\rho|P|. \tag{33}$$

Последнее неравенство в (33) следует из формулы $|P(I)| = N2^{-\rho}$, условия (22), неравенств $80N^{-1/4} \le \alpha \le 2^{-1000}\delta$ и оценки $\rho \le \sqrt{|Q|} \le 2^{-3}(K')^{-2}c^{-1}\dfrac{\delta}{\alpha} \le \dfrac{\delta}{\alpha}$, так как

$$20\alpha\rho|P| \ge 20\alpha 2^{-\rho}N \ge 20\cdot 2^{-\delta/\alpha}N^{3/4} = 20\cdot 2^{3n/4-\delta/\alpha} \ge 20\cdot 2^{n/2} = 20\sqrt{N}.$$

По условию $I \subseteq \mathcal{R}_\alpha(A)$, а согласно пункту 2 имеем $\mathcal{R}_\alpha(A) = \{0\} \bigsqcup \left(\bigsqcup_{w=1}^t Q_w\right)$. Пусть Y_w — аффинное подпространство, натянутое на векторы из $I \cap \mathcal{L}_w$, $w \in [t]$. Ясно, что каждая характеристическая функция множества Y_w зависит только от переменных $x_{(w-1)d+1}, \ldots, x_{(w-1)d+d}$. Имеем $Y = Y_1 * Y_2 * \ldots * Y_t$ и $\widehat{P}(r) = |P|Y(r)$. Используя две последние формулы и тождество (26), получаем

$$\sigma' = \frac{|P|}{N}\prod_{w=1}^t\left(\sum_x f_w(x+z_w)\widehat{Y}_w(x)\right) = \frac{|P|}{N}\prod_{w=1}^t \sigma_w. \tag{34}$$

Пусть $\rho_w = \dim Y_w$, $w \in [t]$. Очевидно, что

$$\sum_{w=1}^t \rho_w = \rho. \tag{35}$$

Зафиксируем $w \in [t]$ и найдем σ_w. Легко видеть, что

$$\sum_x \widehat{Y}_w(x) = Y_w(0)2^d = 2^d. \tag{36}$$

Применяя тождество (36) и формулу (28), находим

$$\sigma_w = \frac{2^d}{2} + \frac{l}{4}\sum_{j=0}^{[l/2]}\frac{(-1)^j}{(K'm)^{l-2j}}\frac{(l-j-1)!}{j!(l-2j)!}\times$$

$$\times 2^{l-2j}\sum_x\sum_{i_1,\ldots,i_{l-2j}}\widehat{Y}_w(x)(-1)^{\langle x+z_w, q_{i_1}+\ldots+q_{i_{l-2j}}\rangle} =$$

$$= \frac{2^d}{2} + \frac{2^d l}{4}\sum_{j=0}^{[l/2]}\frac{(-1)^j}{(K'm)^{l-2j}}\frac{(l-j-1)!}{j!(l-2j)!}\times$$

$$\times 2^{l-2j}\sum_{i_1,\ldots,i_{l-2j}} Y_w(q_{i_1}+\ldots+q_{i_{l-2j}})(-1)^{\langle z_w, q_{i_1}+\ldots+q_{i_{l-2j}}\rangle}.$$

Докажем неравенство

$$|\sigma_w| \le 2^d\left(\frac{1}{2} + \frac{M\rho_w l}{2K'm} + \frac{\rho_w}{\sqrt{m}}\left(\frac{2eM}{K'}\right)^3\right). \tag{37}$$

Будем действовать, как и выше. Ясно, что

$$|\sigma_w| \le \frac{2^d}{2} + \frac{2^d l}{4}\sum_{j=0}^{[l/2]}\frac{1}{(K'm)^{l-2j}}\frac{(l-j-1)!}{j!(l-2j)!}2^{l-2j}\sum_x (Q_w *_{l-2j-1} Q_w)(x)Y_w(x). \tag{38}$$

Применяя формулу (24) с $p = 1$, получаем, что член с $j = j_0$ во втором слагаемом формулы (38) не превышает по модулю $2^d \cdot \dfrac{M\rho_w l}{2K'm}$. Пусть сумма остальных слагаемых в (38), кроме члена $\dfrac{2^d}{2}$, равна σ''_w. Используя оценку (24) и формулу Стирлинга, получаем

$$|\sigma''_w| \le \frac{2^d l\rho_w}{4} \sum_{j=0}^{j_0-1} \frac{1}{(K'm)^{l-2j}} \frac{(l-j-1)!}{j!(l-2j)!} \times$$

$$\times 2^{l-2j} M^{l-2j} (l-2j)^{(l-2j-1)/2} m^{(l-2j-1)/2} \le$$

$$\le \frac{2^d l\rho_w}{4} \sum_{j=0}^{j_0-1} l^{l-2j-1} (l-2j)^{-l/2+j-1/2} m^{-l/2+j-1/2} \left(\frac{2eM}{K'}\right)^{l-2j} \le$$

$$\le \frac{2^d \rho_w}{4\sqrt{m}} \sum_{j=0}^{j_0-1} \left(\frac{2eM}{K'} \frac{l}{\sqrt{m}}\right)^{l-2j} \le 2^d \frac{\rho_w}{\sqrt{m}} \left(\frac{2eM}{K'}\right)^3. \tag{39}$$

Отсюда следует неравенство (37). По условию $\rho \le 2^{-10} M^{-3} \sqrt{m}$. Кроме того, $l = 2\big[\sqrt{m}/(4cK')\big] + 1 \le \sqrt{m}/(cK')$. Следовательно,

$$\sum_{w=1}^{t} \left(\frac{M\rho_w l}{2K'm} + \frac{\rho_w}{\sqrt{m}} \left(\frac{2eM}{K'}\right)^3\right) \le \frac{M\rho l}{2K'm} + \frac{\rho}{\sqrt{m}} \left(\frac{2eM}{K'}\right)^3 \le$$

$$\le 2^{-11} M^{-2} c^{-1} (K')^{-2} + 2^{-7} e^3 (K')^{-3} \le \frac{1}{4}. \tag{40}$$

Аналогично, используя оценку $2^6 (K')^{-4} \delta^2 \alpha^{-2} c^{-4} \le m$, находим

$$\sum_{w=1}^{t} \left(\frac{M\rho_w l}{2K'm} + \frac{\rho_w}{\sqrt{m}} \left(\frac{2eM}{K'}\right)^3\right) \le \frac{M\rho l}{2K'm} + \frac{\rho}{\sqrt{m}} \left(\frac{2eM}{K'}\right)^3 \le$$

$$\le \rho \left(\frac{M}{2c(K')^2\sqrt{m}} + \frac{8e^3M^3}{(K')^3\sqrt{m}}\right) \le$$

$$\le cM\alpha\delta^{-1}\rho + 2^8 c^2 M^3 \alpha\delta^{-1}\rho \le 2^9 c^2 K' M^3 \alpha\delta^{-1}\rho. \tag{41}$$

Имеем $\alpha \ge 80N^{-1/4}$ и $|A| = \delta_0 N = \Big[\sum_x f(x)\Big] = [2^{-t}N] > 2^{-t}N - 1$. Отсюда $2^{-t} \le \delta_0 + 1/N \le \delta_0 + \alpha$. Кроме того, $e^x \le 1 + 2x$, если $x \in [0, 1/2]$. Применяя эти оценки, неравенство (40), тождество (35) и формулы (34) и (37), получаем

$$\sigma' \le \frac{|P|}{N} N \prod_{w=1}^{t} \left(\frac{1}{2} + \frac{M\rho_w l}{2K'm} + \frac{\rho_w}{\sqrt{m}} \left(\frac{2eM}{K'}\right)^3\right) \le$$

$$\le 2^{-t}|P| \left(1 + \sum_{w=1}^{t} \left(\frac{2M\rho_w l}{K'm} + \frac{4\rho_w}{\sqrt{m}} \left(\frac{2eM}{K'}\right)^3\right)\right) \le$$

$$\le \delta_0|P| + \alpha|P| + 2\delta_0|P| \sum_{w=1}^{t} \left(\frac{2M\rho_w l}{K'm} + \frac{4\rho_w}{\sqrt{m}} \left(\frac{2eM}{K'}\right)^3\right) \le$$

$$\le \delta_0|P| + \alpha|P| + \delta_0|P|\frac{4M\rho l}{K'm} + \delta_0|P|\frac{8\rho}{\sqrt{m}}\left(\frac{2eM}{K'}\right)^3.$$

Используя теперь формулу (41) и оценку $\delta_0 \le 4\delta$, находим

$$\sigma' \le \delta_0|P| + 2^{15}c^2K'M^3\alpha\rho|P|.$$

Из последнего неравенства и формул (32), (33) следует (25).

Предложение доказано.

***Замечание* 2.1.** Главное отличие предложения 2.1 от аналогичных утверждений из [21, 45] (см. также [29]) заключается в ограничении $p \le \sqrt{|Q|}$, накладываемом на параметр p. Как отмечалось во введении, в предшествовавших работах приходилось проверять справедливость оценки (23) для всех $p \ll |Q|$.

Достаточные условия для выполнения свойства (23) будут обсуждаться в следующем пункте.

3. О числе решений одного уравнения. Настоящий пункт посвящен изучению величины $T_p(S)$ (см. определение (15)) и ее обобщений. Нам понадобятся несколько лемм.

Лемма 3.1. *Пусть p и r — натуральные числа, $r \le p$. Тогда число разбиений отрезка $[p]$ на r частей не превышает $r^p/r! \le e^p r^{p-r}$.*

Пусть $f\colon \mathbb{F}_2^n \to \mathbb{C}$ — произвольная функция. Обозначим через $T_k(f)$ величину $T_k(f) = \sum\limits_x |(f *_{k-1} f)(x)|^2$. Простое применение неравенства Гельдера дает нам следующую лемму (см., например, [46]).

Лемма 3.2. *Пусть s — натуральное число, $s \ge 2$, и $f_1, \ldots, f_s\colon \mathbb{F}_2^n \to \mathbb{R}$ — некоторые функции. Тогда для любого $\lambda \in \mathbb{F}_2^n$ выполнено*

$$\left|(f_1 * \ldots * f_s)(\lambda)\right| \le (T_s(f_1))^{1/2s} \ldots (T_s(f_s))^{1/2s}. \tag{42}$$

Доказательство. Имеем $\widehat{(f * g)}(r) = \widehat{f}(r)\widehat{g}(r)$. Используя формулу обращения, находим

$$\sigma := (f_1 * \ldots * f_s)(\lambda) = \frac{1}{N}\sum_r \widehat{f}_1(r) \ldots \widehat{f}_s(r)(-1)^{\langle r,\lambda\rangle}.$$

Применяя несколько раз неравенство Гельдера, получаем

$$\sigma \le \left(\frac{1}{N}\sum_r \left|\widehat{f}_1(r)\right|^{2s}\right)^{1/2s} \ldots \left(\frac{1}{N}\sum_r \left|\widehat{f}_s(r)\right|^{2s}\right)^{1/2s} =$$

$$= (T_s(f_1))^{1/2s} \ldots (T_s(f_s))^{1/2s}.$$

Лемма доказана.

Если $A_1, \ldots, A_p \subseteq \mathbb{F}_2^n$ — некоторые множества, то через $T_p(A_1, \ldots, A_p)$ обозначим число решений уравнения

$$T_p(A_1, \ldots, A_p) := \left|\left\{a_1 + \ldots + a_p = 0\colon a_i \in A_i,\ i = 1, \ldots, p\right\}\right|.$$

Тогда $T_p(A, \ldots, A) = T_p(A)$. В работе [46] получен результат об оценке величины $T_p(\Lambda)$ для диссоциативных множеств Λ.

Предложение 3.1. *Пусть k — натуральное число, $k \geq 2$ и $\Lambda \subseteq \mathbb{F}_2^n$ — произвольное множество из семейства $\mathbf{\Lambda}(2k)$. Тогда для всех натуральных p, $2 \leq p \leq k$, выполнено*

$$T_p(\Lambda) \leq p^p |\Lambda|^p. \tag{43}$$

Кроме того, в той же работе был доказан аналог предыдущего предложения для сумм диссоциативных множеств.

Предложение 3.2. *Пусть k, d — натуральные числа, $k \geq 2$, и $\Lambda \subseteq \mathbb{F}_2^n$ — произвольное множество из семейства $\mathbf{\Lambda}(2dk)$ такое, что $|\Lambda| \geq 4d^2$. Пусть также Q — некоторое подмножество $d^{\wedge}\Lambda$. Тогда для всех натуральных p, $2 \leq p \leq k$, выполнено*

$$T_p(Q) \leq 2^{8dp} p^{dp} |Q|^p. \tag{44}$$

К сожалению, непосредственное применение предложения 3.2 недостаточно для целей настоящей работы. Кроме неравенства (44) нам понадобятся более тонкие результаты об оценках аналогов величины $T_p(Q)$, где Q — подмножество сумм *двух* диссоциативных множеств.

Пусть Λ_1, $\Lambda_2 \subseteq \mathbb{F}_2^n$ — произвольные множества, Q — некоторое подмножество множества $\Lambda_1 + \Lambda_2$. Пусть

$$D_\lambda = \{\mu \in \Lambda_2 \colon \lambda + \mu \in Q\}, \quad \lambda \in \Lambda_1,$$

$$\tilde{D}_\mu = \{\lambda \in \Lambda_1 \colon \lambda + \mu \in Q\}, \quad \mu \in \Lambda_2,$$

и

$$Q_\lambda = \big\{q \in Q \colon q = \lambda + \mu, \ \ \mu \in \Lambda_2\big\}, \quad \lambda \in \Lambda_1.$$

Ясно, что $Q_\lambda = D_\lambda + \lambda$. Отсюда $|Q_\lambda| = |D_\lambda|$. Пусть также $|\Lambda_1| = |\Lambda_2| = s$.

Пусть t — натуральное число, $t \geq 2$, h_1, h_2 — целые неотрицательные числа, а $\mu_1^{(1)}, \ldots, \mu_{h_1}^{(1)} \in \Lambda_1$, $\mu_1^{(2)}, \ldots, \mu_{h_2}^{(2)} \in \Lambda_2$ — различные элементы. Обозначим через $N_t(Q; \mu_1^{(1)}, \ldots, \mu_{h_1}^{(1)}; \mu_1^{(2)}, \ldots, \mu_{h_2}^{(2)})$ число решений уравнения

$$q_1 + \ldots + q_t = \mu_1^{(1)} + \ldots + \mu_{h_1}^{(1)} + \mu_1^{(2)} + \ldots + \mu_{h_2}^{(2)}, \tag{45}$$

где $q_1, \ldots, q_t \in Q$. Если $h_1 = 0$, $h_2 \neq 0$ или $h_2 = 0$, $h_1 \neq 0$, то будем использовать обозначения $N_t(Q; \mu_1^{(2)}, \ldots, \mu_{h_2}^{(2)})$ и $N_t(Q; \mu_1^{(1)}, \ldots, \mu_{h_1}^{(1)})$ соответственно. Если, наконец, $h_1 = h_2 = 0$, то будем считать, что вместо суммы $\mu_1^{(1)} + \ldots + \mu_{h_1}^{(1)} + \mu_1^{(2)} + \ldots + \mu_{h_2}^{(2)}$ в правой части (45) стоит нуль. В этом случае для числа решений уравнения (45) будем использовать обозначение $N_t(Q)$. Через $N_t^*\big(Q; \mu_1^{(1)}, \ldots, \mu_{h_1}^{(1)}; \mu_1^{(2)}, \ldots, \mu_{h_2}^{(2)}\big)$ обозначим число решений уравнений (45) с *различными* $q_1, \ldots, q_t$.

Если $\vec{v} = (v_1, \ldots, v_t)$ — некоторый вектор, то через $\langle \vec{v} \rangle$ обозначим сумму $v_1 + \ldots + v_t$.

Лемма 3.3. *Пусть k — натуральное число, p — четное, $2 \leq p \leq k$, Λ_1, $\Lambda_2 \subseteq \mathbb{F}_2^n$ — произвольные непересекающиеся множества такие, что $\Lambda_1 \bigsqcup \Lambda_2$ принадлежит семейству $\mathbf{\Lambda}(4k)$. Пусть также Q — некоторое подмножество $\Lambda_1 + \Lambda_2$. Тогда*

$$N_p(Q) \leq p^{p/2} \sum_{\langle \lambda^{(1)} \rangle + \langle \lambda^{(2)} \rangle = 0} \left(\prod_{j=1}^{p/2} \left| D_{\lambda_j^{(1)}} \cap D_{\lambda_j^{(2)}} \right| \right), \tag{46}$$

где $\lambda^{(1)} = \bigl(\lambda_1^{(1)}, \ldots, \lambda_{p/2}^{(1)}\bigr)$, $\lambda^{(2)} = \bigl(\lambda_1^{(2)}, \ldots, \lambda_{p/2}^{(2)}\bigr)$ — *произвольные векторы из* $\Lambda_1^{p/2}$.

Далее, пусть $\mu_1^{(1)}, \ldots, \mu_{h_1}^{(1)}$ — *произвольные различные элементы из множества* Λ_1, $h_1 \le 2k$ *и*

$$E = \bigl\{\lambda + \mu \colon D_\lambda \cap D_\mu \ne \varnothing\bigr\} \subseteq \Lambda_1 + \Lambda_1. \tag{47}$$

Тогда

$$N_p\bigl(Q; \mu_1^{(1)}, \ldots, \mu_{h_1}^{(1)}\bigr) \le$$

$$\le 2^p p^{p/2} \Bigl(\max_{\lambda,\mu\in\Lambda_1} |D_\lambda \cap D_\mu|\Bigr)^{p/2} N_{p/2}\bigl(E; \mu_1^{(1)}, \ldots, \mu_{h_1}^{(1)}\bigr). \tag{48}$$

Доказательство. Сначала установим неравенство (46). Рассмотрим уравнение

$$q_1 + \ldots + q_p = 0, \tag{49}$$

где $q_i \in Q$, $q_i = \lambda_i + \lambda_i'$, $\lambda_i \in \Lambda_1$, $\lambda_i' \in \Lambda_2$, $i \in [p]$. Ясно, что p — четное, иначе уравнение (49) не имеет решений. Поскольку множества Λ_1, Λ_2 не пересекаются и их объединение принадлежит множеству $\mathbf{\Lambda}(4k)$, для любого решения уравнения (49) выполнено $\sum_{i=1}^p \lambda_i = \sum_{i=1}^p \lambda_i' = 0$. Более того, любое λ_i' встречается в векторе $(\lambda_1', \ldots, \lambda_p')$ четное число раз. Ясно, что для любого $i \in [p]$ выполнено $\lambda_i' \in D_{\lambda_i}$. Следовательно, произвольному решению уравнения (49) $q_i = \lambda_i + \lambda_i'$, $i \in [p]$, соответствует вектор $(x_1, \ldots, x_{p/2})$, все x_i из множества $\{\lambda_1', \ldots, \lambda_p'\}$, каждый x_i принадлежит некоторому множеству $D_{\lambda_i} \cap D_{\lambda_s}$, $s = s(i)$. Для любого x_i выбор числа $s(i)$ осуществляется не более чем p способами. Отсюда получаем формулу (46).

Прежде чем доказывать неравенство (48), сделаем несколько замечаний. Ясно, что для любых векторов $\lambda^{(1)} = \bigl(\lambda_1^{(1)}, \ldots, \lambda_{p/2}^{(1)}\bigr)$, $\lambda^{(2)} = \bigl(\lambda_1^{(2)}, \ldots, \lambda_{p/2}^{(2)}\bigr)$ из $\Lambda_1^{p/2}$ выполнено

$$\prod_{j=1}^{p/2} \Bigl|D_{\lambda_j^{(1)}} \cap D_{\lambda_j^{(2)}}\Bigr| \le \Bigl(\max_{\lambda,\mu\in\Lambda_1} |D_\lambda \cap D_\mu|\Bigr)^{p/2}.$$

Далее, в формуле (46) суммирование ведется по всем векторам $\lambda^{(1)}$, $\lambda^{(2)}$ таким, что $\langle\lambda^{(1)}\rangle + \langle\lambda^{(2)}\rangle = 0$ и для всех $j \in [p/2]$ выполнено $\lambda_j^{(1)} + \lambda_j^{(2)} \in E$. Теперь, чтобы получить (48), достаточно заметить, что среди компонент векторов $\lambda^{(1)}$, $\lambda^{(2)}$ должны быть элементы $\mu_1^{(1)}, \ldots, \mu_{h_1}^{(1)}$, так как множество $\Lambda_1 \bigsqcup \Lambda_2$ принадлежит семейству $\mathbf{\Lambda}(4k)$. Наконец, каждое $q_j \in E$ есть $q_j = \lambda_j^{(1)} + \lambda_j^{(2)} = \lambda_j^{(2)} + \lambda_j^{(1)}$, $j \in [p/2]$. Отсюда в формуле (48) получаем множитель $2^{p/2} \le 2^p$.

Лемма доказана.

***Замечание* 3.1.** Легко видеть, что для оценки величины $N_p^*(Q)$ справедлив аналог формулы (46), а для оценки величины $N_p^*(Q; \mu_1^{(1)}, \ldots, \mu_{h_1}^{(1)})$ — аналог формулы (48). В первом случае произведение в (46) берется только по тем j, для которых $\lambda_j^{(1)} \ne \lambda_j^{(2)}$, а во втором максимум в (48) достаточно брать лишь по $\lambda \ne \mu$. Заметим еще, что в последнем случае множество E из (47) принадлежит $\Lambda_1 \dotplus \Lambda_1$.

Теперь мы докажем одну лемму об аналогах величины $N_p\bigl(Q; \mu_1^{(1)}, \ldots, \mu_{h_1}^{(1)}\bigr)$ для множеств Q, принадлежащих сумме двух копий *одного* диссоциативного мно-

жества Λ. Такие множества появились, например, в предыдущей лемме (см. определение множества E из формулы (47)).

Пусть k — натуральное число, $k \geq 2$, и $\Lambda \subseteq \mathbb{F}_2^n$ — произвольное множество из семейства $\mathbf{\Lambda}(2k)$. Пусть также $\mathcal{Q} \subseteq \Lambda \dotplus \Lambda$, и для любого $\lambda \in \Lambda$ определим аналог величин Q_λ, D_λ:

$$\mathcal{Q}_\lambda = \big\{q \in \mathcal{Q}\colon q = \lambda \dotplus \mu \in \mathcal{Q}\big\},$$

$$\mathcal{D}_\lambda = \big\{\mu \in \Lambda\colon \lambda \dotplus \mu \in \mathcal{Q}\big\}.$$

Аналогично определяются $N_t(\mathcal{Q})$ и $N_t(\mathcal{Q}; \mu_1, \ldots, \mu_h)$, где элементы $\mu_i \in \Lambda$, $i \in [h]$, различны. Пусть еще

$$\mathbf{\Omega} = \big\{(\lambda, \mu)\colon \mathcal{Q}_\lambda \cap \mathcal{Q}_\mu \neq \varnothing, \ \ \lambda \neq \mu\big\}.$$

Справедлива следующая лемма.

Лемма 3.4. *Пусть k, p — натуральные числа, $2 \leq p \leq k$, $\epsilon > 0$ — действительное число, $\Lambda \subseteq \mathbb{F}_2^n$ — произвольное множество из семейства $\mathbf{\Lambda}(2k)$, $|\Lambda| \geq 16$. Пусть также $\mathcal{Q} \subseteq \Lambda \dotplus \Lambda$ и для произвольных λ, $\mu \in \Lambda$, $\lambda \neq \mu$, выполняется неравенство*

$$|\mathcal{D}_\lambda \cap \mathcal{D}_\mu| \leq \frac{\epsilon |\mathcal{Q}|}{|\Lambda|}. \tag{50}$$

Тогда

$$N_p(\mathcal{Q}) \leq 2^{15p} p^p |\mathcal{Q}|^{p/2} \epsilon^{p/2} \sum_{t=0}^{[p/2]} \frac{1}{(\epsilon p)^t} \tag{51}$$

и

$$N_p(\mathcal{Q}) \leq 2^{15p} p^p |\mathcal{Q}|^{p/2} \epsilon^{p/2} \left(\frac{|\mathbf{\Omega}|}{|\Lambda|^2}\right)^{p/4} \sum_{t=0}^{p/2} \frac{|\Lambda|^t}{(\epsilon p \sqrt{|\mathbf{\Omega}|})^t}. \tag{52}$$

Доказательство. Ясно, что число p является четным, иначе $N_p(\mathcal{Q}) = 0$. Сначала убедимся в справедливости оценки (51). Пусть $a = \big[|\Lambda|/4\big]$. По условию $|\Lambda| \geq 16$. Отсюда $|\Lambda|/a \leq 8$. Кроме того,

$$\binom{|\Lambda| - 2}{a - 1}^{-1} \binom{|\Lambda|}{a} = \frac{|\Lambda|(|\Lambda| - 1)}{a(|\Lambda| - a)} \leq 32. \tag{53}$$

Пусть для произвольного множества E символ E^c означает $\Lambda \setminus E$. Используя диссоциативность множества Λ и определение операции $\dotplus$, получаем

$$\mathcal{Q}(x) = 2^{-1} \binom{|\Lambda| - 2}{a - 1}^{-1} \sum_{\Lambda_0 \subseteq \Lambda,\, |\Lambda_0| = a} \left(\mathcal{Q} \cap (\Lambda_0 + \Lambda_0^c)\right)(x).$$

Применяя неравенство Гельдера, находим

$$N_p(\mathcal{Q}) \leq 2^{-p} \binom{|\Lambda| - 2}{a - 1}^{-p} \binom{|\Lambda|}{a}^{p-1} \sum_{\Lambda_0 \subseteq \Lambda,\, |\Lambda_0| = a} N_p(\mathcal{Q} \cap (\Lambda_0 + \Lambda_0^c)). \tag{54}$$

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

$$N_p(\mathcal{Q}\cap(\Lambda_0+\Lambda_0^c))\le 2^{8p}p^p|\mathcal{Q}|^{p/2}\epsilon^{p/2}\sum_{t=0}^{[p/2]}\frac{1}{(\epsilon p)^t},$$

то, подставив это неравенство в (54) и использовав (53), получим

$$N_p(\mathcal{Q})\le 2^{-p}\binom{|\Lambda|-2}{a-1}^{-p}\binom{|\Lambda|}{a}^p 2^{8p}p^p|\mathcal{Q}|^{p/2}\epsilon^{p/2}\sum_{t=0}^{[p/2]}\frac{1}{(\epsilon p)^t}\le$$

$$\le 2^{15p}p^p|\mathcal{Q}|^{p/2}\epsilon^{p/2}\sum_{t=0}^{[p/2]}\frac{1}{(\epsilon p)^t},$$

и первое утверждение леммы 3.4 будет доказано.

Пусть $\Lambda_0\subseteq\Lambda$, $|\Lambda_0|=a$ — некоторое множество. Положим $\Lambda_1=\Lambda_0$, $\Lambda_2=\Lambda\setminus\Lambda_0$ и $\mathcal{Q}'=\mathcal{Q}\cap(\Lambda_1+\Lambda_2)$. Требуется доказать, что

$$N_p(\mathcal{Q}')\le 2^{6p}p^p|\mathcal{Q}|^{p/2}\epsilon^{p/2}\sum_{t=0}^{[p/2]}\frac{1}{(\epsilon p)^t}.$$

Разобьем все решения уравнения $q_1+\ldots+q_p=0$, $q_i\in\mathcal{Q}'$, $i\in[p]$, на группы. Пусть $t\le p/2$ — целое неотрицательное число. Тогда в одну группу попадают решения $(q_1,\ldots,q_p)$, имеющие ровно t пар элементов q_i, в каждой паре элементы одинаковы, и при этом все остальные q_i различны. Индексы этих различных q_i образуют некоторое множество W, при этом число таких множеств не превышает $\binom{p}{p-2t}\le 2^p$. Далее, любой элемент пары можно выбрать не более чем $|\mathcal{Q}'|\le|\mathcal{Q}|$ способами. Кроме того, сумма всех элементов, образующих пары, равна нулю. Суммируя вышеизложенное и используя лемму 3.1, находим

$$N_p(\mathcal{Q}')\le 2^p\sum_{t=0}^{p/2}N^*_{p-2t}(\mathcal{Q}')e^{2t}t^t|\mathcal{Q}|^t\le 8^p\sum_{t=0}^{p/2}N^*_{p-2t}(\mathcal{Q}')t^t|\mathcal{Q}|^t, \qquad (55)$$

где значение $N_0^*(\mathcal{Q}')$ полагаем равным 1. Для оценки величин $N^*_{p-2t}(\mathcal{Q}')$ применим лемму 3.3. Мы получим множество $E\subseteq\Lambda_1\dotplus\Lambda_1$, $E\subseteq\mathbf{\Omega}$, такое, что

$$N^*_{p-2t}(\mathcal{Q}')\le 2^p(p-2t)^{(p-2t)/2}\left(\frac{\epsilon|\mathcal{Q}|}{|\Lambda|}\right)^{p/2-t}N_{p/2-t}(E)\le$$

$$\le 2^p(p-2t)^{(p-2t)/2}\left(\frac{\epsilon|\mathcal{Q}|}{|\Lambda|}\right)^{p/2-t}N_{p/2-t}(\Lambda_1\dotplus\Lambda_1). \qquad (56)$$

Таким образом, если мы оценим $N_{p/2-t}(\Lambda_1\dotplus\Lambda_1)$ сверху, то величина $N^*_{p-2t}(\mathcal{Q}')$ также будет оценена. Ясно, что $|\Lambda_1\dotplus\Lambda_1|\le|\Lambda_1|^2\le|\Lambda|^2$. Используя теперь предложение 3.2, получаем

$$N_{p/2-t}(\Lambda_1\dotplus\Lambda_1)\le 2^{8(p/2-t)}\left(\frac{1}{2}\left(\frac{p}{2}-t\right)\right)^{p/2-t}|\Lambda|^{p/2-t}.$$

Объединяя последнюю формулу и неравенства (55), (56), находим

$$N_p(\mathcal{Q}') \le 2^{4p} \sum_{t=0}^{p/2} (p-2t)^{(p-2t)/2} \left(\frac{\epsilon|\mathcal{Q}|}{|\Lambda|}\right)^{p/2-t} \times$$

$$\times 2^{8(p/2-t)} \left(\frac{1}{2}\left(\frac{p}{2}-t\right)\right)^{p/2-t} |\Lambda|^{p/2-t} t^t |\mathcal{Q}|^t \le$$

$$\le 2^{8p} p^p |\mathcal{Q}|^{p/2} \epsilon^{p/2} \sum_{t=0}^{p/2} \epsilon^{-t} (p-2t)^{(p-2t)/2} (p-2t)^{p/2-t} p^t \le$$

$$\le 2^{8p} p^p |\mathcal{Q}|^{p/2} \epsilon^{p/2} \sum_{t=0}^{p/2} \frac{1}{(\epsilon p)^t}. \tag{57}$$

Нам осталось доказать неравенство (52). Для любого $t = 0, 1, \ldots, p/2$ по лемме 3.3 имеем

$$N^*_{p-2t}(\mathcal{Q}') \le 2^p (p-2t)^{(p-2t)/2} \left(\frac{\epsilon|\mathcal{Q}|}{|\Lambda|}\right)^{p/2-t} N_{(p-2t)/2}(\mathbf{\Omega}). \tag{58}$$

Применяя предложение 3.2, находим

$$N^*_{p-2t}(\mathcal{Q}') \le 2^{5p} (p-2t)^{p-2t} |\mathbf{\Omega}|^{(p-2t)/4} \left(\frac{\epsilon|\mathcal{Q}|}{|\Lambda|}\right)^{p/2-t}. \tag{59}$$

Применяя теперь последнее неравенство и оценку (55), получаем

$$N_p(\mathcal{Q}') \le 2^{8p} \sum_{t=0}^{p/2} p^{p-2t} |\mathbf{\Omega}|^{\frac{p-2t}{4}} \left(\frac{\epsilon|\mathcal{Q}|}{|\Lambda|}\right)^{p/2-t} t^t |\mathcal{Q}|^t \le$$

$$\le 2^{8p} p^p |\mathcal{Q}|^{p/2} \epsilon^{p/2} \left(\frac{|\mathbf{\Omega}|}{|\Lambda|^2}\right)^{p/4} \sum_{t=0}^{p/2} \frac{|\Lambda|^t}{\left(\epsilon p \sqrt{|\mathbf{\Omega}|}\right)^t}. \tag{60}$$

Лемма доказана.

***Следствие* 3.1.** *Пусть в условиях предыдущей леммы выполнено* $\epsilon \le 1/(2p)$ *или* $\epsilon \le |\Lambda|/\left(2p\sqrt{|\mathbf{\Omega}|}\right)$. *Тогда* $N_p(\mathcal{Q}) \le 2^{16p} p^{p/2} |\mathcal{Q}|^{p/2}$.

Выведем еще одно следствие из леммы 3.4.

***Следствие* 3.2.** *Пусть* k *— натуральное число,* h *— целое,* $h \le 2k$, p *— четное,* $2 \le p \le k$, C_* *— действительное число,* $\Lambda \subseteq \mathbb{F}_2^n$ *— произвольное множество из семейства* $\mathbf{\Lambda}(4k)$, $|\Lambda| \ge 16$, *и* $\mathcal{Q} \subseteq \Lambda \dotplus \Lambda$ *— некоторое множество,* $|\mathcal{Q}| \ge 2$. *Предположим, что для всех* $\lambda \in \Lambda$ *выполнено*

$$|\mathcal{Q}_\lambda| \le \frac{C_*|\mathcal{Q}|}{|\Lambda|}. \tag{61}$$

Тогда для произвольного целого h *и различных* $\mu_1, \ldots, \mu_h \in \Lambda$ *имеем*

$$N_p(\mathcal{Q}; \mu_1, \ldots, \mu_h) \le$$

$$\le 2^{2p} p^h \max\left\{\left(\frac{C_* p|\mathcal{Q}|}{|\Lambda|}\right)^{h/2} (N_p(\mathcal{Q}))^{(p-h)/p}, (N_p(\mathcal{Q}))^{(p-h/2)/p}\right\}. \tag{62}$$

Если же число $p \geq 3$ нечетное и $h \geq 1$, то

$$N_p(\mathcal{Q}; \mu_1, \ldots, \mu_h) \leq 2^{2p} \max\{\varrho_1, \varrho_2\}, \tag{63}$$

где

$$\varrho_1 = \left(\frac{C_* p|\mathcal{Q}|}{|\Lambda|}\right) \max\left\{\left(\frac{C_* p|\mathcal{Q}|}{|\Lambda|}\right)^{(h-1)/2} (N_{p-1}(\mathcal{Q}))^{(p-h)/(p-1)},\right.$$

$$\left.(N_{p-1}(\mathcal{Q}))^{(p-h-1/2)/(p-1)}\right\}$$

и

$$\varrho_2 = \max\left\{\left(\frac{C_* p|\mathcal{Q}|}{|\Lambda|}\right)^{(h-2)/2} (N_{p-1}(\mathcal{Q}))^{(p-h+1)/(p-1)},\right.$$

$$\left.(N_{p-1}(\mathcal{Q}))^{(p-h/2)/(p-1)}\right\}.$$

Доказательство. Предположим сначала, что число p является четным, и докажем неравенство (62). Рассмотрим уравнение

$$q_1 + \ldots + q_p = \mu_1 + \ldots + \mu_h, \tag{64}$$

где $q_i \in \mathcal{Q}$, $q_i = \lambda_i + \lambda_i'$, $\lambda_i \in \Lambda$, $\lambda_i' \in \Lambda$, $i \in [p]$. Обозначим через σ число решений уравнения (64). По условию множество Λ принадлежит семейству $\mathbf{\Lambda}(4k)$. Отсюда h — четное и $h \leq 2p$, иначе $\sigma = 0$. Поскольку множество Λ принадлежит семейству $\mathbf{\Lambda}(4k)$, среди элементов λ_i, λ_i' обязательно есть $\mu_1, \ldots, \mu_h$. Пусть $\mathcal{M} = \{\mu_1, \ldots, \mu_h\}$. Пусть также $S_1, S_2 \subseteq [p]$ — произвольные множества, $|S_1| + |S_2| = h$. Число решений уравнения (64), для которого выполнено $\lambda_i \in \mathcal{M}$, $i \in S_1$, $\lambda_j' \in \mathcal{M}$, $j \in S_2$, обозначим через $\sigma(S_1, S_2)$. Зафиксируем множества S_1 и S_2, а также элементы μ_i, $i \in S_1$, μ_j, $j \in S_2$. Возьмем произвольное $i \in [p]$ и определим множество $\mathcal{Q}_i$. Если $\lambda_i, \lambda_i' \in \mathcal{M}$, то пусть $\mathcal{Q}_i$ — одноэлементное множество $\{\lambda_i \dotplus \dotplus \lambda_i'\}$. В противном случае положим $\mathcal{Q}_i = \mathcal{Q}_{\lambda_i}$, если $\lambda_i \in \mathcal{M}$, и $\mathcal{Q}_i = \mathcal{Q}_{\lambda_i'}$, если $\lambda_i' \in \mathcal{M}$. Наконец, пусть $\mathcal{Q}_i = \mathcal{Q}$, если $\lambda_i, \lambda_i' \notin \mathcal{M}$. Заметим, что $N_p(\mathcal{D}_\lambda) = N_p(\mathcal{Q}_\lambda)$, $\lambda \in \Lambda$. Применяя лемму 3.2 с $\lambda = \mu_1 + \ldots + \mu_h$, получаем

$$\sigma \leq \sum_{S_1 \subseteq [p],\, S_2 \subseteq [p]} \sigma(S_1, S_2) \leq 2^p p^h \max_{S_1, S_2, \mu_i} \prod_{i=1}^{p} T_{p/2}^{1/p}(\mathcal{Q}_i).$$

Пусть x — число всех $\mathcal{Q}_i$, не совпадающих с $\mathcal{Q}$ и равных некоторым $\mathcal{Q}_{\lambda_i}$, а y — число всех одноэлементных $\mathcal{Q}_i$. Ясно, что $2y + x = h$. Отсюда $0 \leq y \leq h/2$. Применяя предложение 3.1, находим

$$\sigma \leq 2^p p^h \max_{0 \leq y \leq h/2} \left\{\left(\frac{C_* p|\mathcal{Q}|}{|\Lambda|}\right)^{h/2-y} (N_p(\mathcal{Q}))^{(p-h+y)/p}\right\} =$$

$$= 2^p p^h \max\left\{\left(\frac{C_* p|\mathcal{Q}|}{|\Lambda|}\right)^{h/2} (N_p(\mathcal{Q}))^{(p-h)/p}, (N_p(\mathcal{Q}))^{(p-h/2)/p}\right\}.$$

Пусть теперь $p \geq 3$ является нечетным. Тогда $p-1 \geq 2$ — четное. По условию $h \geq 1$. Следовательно, найдется по крайней мере одно множество $\mathcal{Q}_i$, не совпадающее с $\mathcal{Q}$. Пусть это множество $\mathcal{Q}_i$ равно некоторому $\mathcal{Q}_{\lambda_i}$. Без ограничения общности можно считать, что $\mathcal{Q}_{\lambda_i} = \mathcal{Q}_{\mu_1}$. Тогда

$$N_p(\mathcal{Q}; \mu_1, \ldots, \mu_h) \leq p\left(\frac{C_* p|\mathcal{Q}|}{|\Lambda|}\right) N_{p-1}(\mathcal{Q}; \mu_2, \ldots, \mu_h) \leq p\varrho_1,$$

так как мы имеем случай, рассмотренный выше. Пусть теперь множество $\mathcal{Q}_i$ есть одноэлементное множество. Без ограничения общности считаем, что $\mathcal{Q}_i = \{\mu_1 + \\ + \mu_2\}$. Тогда

$$N_p(\mathcal{Q}; \mu_1, \ldots, \mu_h) \leq pN_{p-1}(\mathcal{Q}; \mu_3, \ldots, \mu_h) \leq p\varrho_2,$$

так как мы опять можем применить рассуждения, изложенные выше.

Следствие доказано.

Кроме множеств D_λ, Q_λ, связанных с некоторым $Q \subseteq \Lambda_1 + \Lambda_2$, $\Lambda_1 \bigsqcup \Lambda_2 \in \\ \in \mathbf{\Lambda}(4k)$, нам понадобится множество Ω из $\Lambda_1 \times \Lambda_1$. Пусть

$$\Omega := \big\{(\lambda, \mu) \in \Lambda_1 \times \Lambda_1 \colon \lambda \neq \mu, \;\; D_\lambda \cap D_\mu \neq \varnothing\big\}.$$

Заметим, что множество Ω является симметричным в том смысле, что $(\lambda, \mu) \in \Omega$ тогда и только тогда, когда $(\mu, \lambda) \in \Omega$. Аналогично, для любого $\lambda \in \Lambda_1$ определим

$$\Omega_\lambda = \{\mu \in \Lambda_1 \colon (\lambda, \mu) \in \Omega\}.$$

Пусть еще

$$\Omega^{\#} := \big\{(\lambda, \mu) \in \Lambda_1 \times \Lambda_1 \colon \lambda \neq \mu, \;\; \Omega_\lambda \cap \Omega_\mu \neq \varnothing\big\}.$$

Наконец, обозначим через $N_t^{**}(Q; \mu_1^{(1)}, \ldots, \mu_{h_1}^{(1)}; \mu_1^{(2)}, \ldots, \mu_{h_2}^{(2)})$ число решений уравнения

$$q_1 + \ldots + q_t = \mu_1^{(1)} + \ldots + \mu_{h_1}^{(1)} + \mu_1^{(2)} + \ldots + \mu_{h_2}^{(2)},$$

где $q_1, \ldots, q_t \in Q$ и при этом все q_r различны, а также $q_r \neq \mu_i^{(1)} + \mu_j^{(2)}$, $i \in [h_1]$, $j \in [h_2]$.

Ясно, что для всех p имеем оценку $T_p(Q) \geq (Kp)^p |Q|^p$ с некоторой положительной константой K. В определенном смысле следующая лемма дает некоторые достаточные условия для выполнения обратного неравенства для величин T_p и N_p. Доказательство представляет собой развитие подхода из [46].

Лемма 3.5. *Пусть k, p, s — натуральные числа, h_1, h_2 — целые неотрицательные числа, $C \geq 1$ — действительное число, $2 \leq p \leq k$, $h_1, h_2 \leq k$, $h_1 + h_2 \geq \\ \geq 1$, $\Lambda_1, \Lambda_2 \subseteq \mathbb{F}_2^n$, $|\Lambda_1| = |\Lambda_2| = s$ — произвольные непересекающиеся множества такие, что $\Lambda_1 \bigsqcup \Lambda_2$ принадлежит семейству $\mathbf{\Lambda}(4k)$ и $\mu_1^{(1)}, \ldots, \mu_{h_1}^{(1)} \in \Lambda_1$, $\mu_1^{(2)}, \ldots, \mu_{h_2}^{(2)} \in \Lambda_2$ — различные элементы. Пусть также Q — некоторое подмножество $\Lambda_1 + \Lambda_2$. Предположим, что $|\Lambda_1| \geq |Q|^{31/32}$, $|Q| \geq |\Lambda_1|$, $|Q| \geq 2^{200} C^{50}$ и*

1) *для любого $\lambda \in \Lambda_1$ имеем $|D_\lambda| \leq C|Q|/s$, а для любого $\mu \in \Lambda_2$ выполнено $|\tilde{D}_\lambda| \leq C|Q|/s$;.*

2) *для произвольных $\lambda, \mu \in \Lambda_1$, $\lambda \neq \mu$, выполняется неравенство $|D_\lambda \cap D_\mu| \leq \\ \leq C$;*

3) *для любого* $\lambda \in \Lambda_1$ *выполнено* $|\Omega_\lambda| \le C|Q|^2/s^2$;

4) *для любых* $\lambda, \mu \in \Lambda_1$, $\lambda \ne \mu$, *имеет место неравенство*

$$|\Omega_\lambda \cap \Omega_\mu| \le \frac{C|Q|}{s} \tag{65}$$

и, наконец,

5) $|\Omega| \ge |Q|^2/(Cs)$, $|Q|^3/(Cs^2) \le |\Omega^\#| \le C|Q|^4/s^3$.

Тогда для всех $2 \le p \le C\sqrt{|Q|}$ *выполнено*

$$N_p\Big(Q; \mu_1^{(1)}, \dots, \mu_{h_1}^{(1)}; \mu_1^{(2)}, \dots, \mu_{h_2}^{(2)}\Big) \le (2^{35}C^5)^p p^{p/2+1}|Q|^{(p-1)/2} \tag{66}$$

и

$$N_p^{**}\Big(Q; \mu_1^{(1)}, \dots, \mu_{h_1}^{(1)}; \mu_1^{(2)}, \dots, \mu_{h_2}^{(2)}\Big) \le$$

$$\le 2^{20p}C^{4p}p^{p+h/2}m^{3p/4+h_2-3h/4}s^{5h/8-5p/8-h_2}. \tag{67}$$

Доказательство. Пусть $m = |Q|$ и $s = |\Lambda_1| = |\Lambda_2|$. Вначале докажем неравенство (66). Для определенности будем считать, что $h_1 \ge h_2$. Рассмотрим уравнение

$$q_1 + \ldots + q_p = \mu_1^{(1)} + \ldots + \mu_{h_1}^{(1)} + \mu_1^{(2)} + \ldots + \mu_{h_2}^{(2)}, \tag{68}$$

где $q_i \in Q$, $i = 1, \dots, p$. Обозначим через σ число решений уравнения (68). Поскольку $Q \subseteq \Lambda_1 + \Lambda_2$, для всех $q \in Q$ выполнено $q = \lambda_1 + \lambda_2$, где $\lambda_1 \in \Lambda_1$, $\lambda_2 \in \Lambda_2$.

Пусть $N_p^*(Q)$ — число решений уравнения (68) с различными q_i. Для доказательства оценки (66) достаточно показать, что для всех $2 \le l \le p \le C\sqrt{m}$ выполняется неравенство

$$N_l^*(Q) \le (2^{30}C^5)^l p^{l/2+1}m^{(l-1)/2}. \tag{69}$$

Действительно, рассуждая, как и при доказательстве леммы 3.4, разобьем все решения уравнения (68) на группы. Пусть $t \le p/2$ — целое неотрицательное число. Тогда в одну группу попадают решения $(q_1, \dots, q_p)$, имеющие ровно t пар элементов q_i, в каждой паре элементы одинаковы и при этом все остальные q_i различны. Индексы этих различных q_i образуют некоторое множество W, и число таких множеств не превышает $\binom{p}{p-2t} \le 2^p$. Далее, любой элемент пары можно выбрать не более чем m способами. Кроме того, сумма всех элементов, образующих пары, равна нулю. Суммируя вышеизложенное и используя для подсчета всех вариантов разбиения множества $[2t]$ на пары лемму 3.1, находим

$$\sigma \le 8^p \sum_{t=0}^{[p/2]} N_{p-2t}^*(Q)t^t m^t \le$$

$$\le g + 8^p(2^{30}C^5)^p \sum_{t=0}^{[p/2]-1} m^{(p-1)/2-t}p^{p/2-t+1}p^t m^t \le$$

$$\le g + (2^{34}C^5)^p p^{p/2+1}m^{(p-1)/2},$$

где $g \le 8^p N_1^*(Q) p^{(p-1)/2} m^{(p-1)/2} \le 8^p p^{(p-1)/2} m^{(p-1)/2}$, если p — нечетное, и $g = 0$, если p — четное. В любом случае получаем неравенство (66). Указанные оценки для величин g и $N_1^*(Q)$ следуют из того факта, что $h_1 + h_2 \ge 1$.

Далее, предположим, что найдутся $i \in [h_1]$, $j \in [h_2]$ такие, что $\mu_i^{(1)} + \mu_j^{(2)} \in Q$, и пусть $N_p^{**}(Q)$ — число решений уравнения (68) с различными q_r и такими, что $q_r \ne \mu_i^{(1)} + \mu_j^{(2)}$, $r \in [p]$. Поскольку $m \ge 2^8 C^2$, то $p \le C\sqrt{m} \le m$. Величина $N_p^*(Q)$ может быть оценена сверху через $N_l^{**}(Q)$:

$$N_p^*(Q) \le \sum_{t=0}^{h_2} \binom{p}{t} \binom{h_2}{t} t! \left(\frac{Cm}{s}\right)^t N_{p-t}^{**}(Q). \tag{70}$$

Действительно, разобьем наборы $(q_1, \ldots, q_p)$, где элементы q_r различны и удовлетворяют уравнению (68), на группы. Пусть $t \le h_2 \le h_1$ — целое неотрицательное число. Тогда в одну группу попадают решения $(q_1, \ldots, q_p)$, имеющие ровно t элементов q_r, равных некоторым $\mu_i^{(1)} + \mu_j^{(2)}$, $i \in [h_1]$, $j \in [h_2]$. Очевидно, что места для этих q_r мы можем выбрать не более чем $\binom{p}{t}$ способами, а элементы $\mu_i^{(1)}$, $\mu_j^{(2)}$ — не более чем $\binom{h_1}{t}\binom{h_2}{t}$ способами. Далее мы можем переставлять элементы $\mu_i^{(1)}$, что дает еще $t!$ вариантов. Используя первый пункт леммы, грубо оцениваем оставшиеся возможности для $\mu_j^{(2)}$ числом $(Cm/s)^t$. Отсюда получаем формулу (70). Имеем $m \ge 2^{200} C^{50}$, $p \le C\sqrt{m}$ и $s \ge m^{31/32}$, откуда

$$s \ge C^{3/2} m^{3/4} \ge C m^{1/2} p^{1/2}. \tag{71}$$

Теперь ясно, что достаточно установить справедливость аналога оценки (69) для величины $N_p^{**}(Q)$, а именно,

$$N_l^*(Q) \le (2^{25} C^5)^l p^{l/2+1} m^{(l-1)/2}, \quad l \in [p],$$

так как тогда

$$N_p^*(Q) \le \sum_{t=0}^{h_2} \binom{p}{t} \binom{h_2}{t} t! \left(\frac{Cm}{s}\right)^t N_{p-t}^{**}(Q) \le$$

$$\le g' + (2^{26} C^5)^p \sum_{t=0}^{h_2} p^t p^{p/2+1-t/2} m^{(p-1)/2-t/2} \left(\frac{Cm}{s}\right)^t \le$$

$$\le g' + (2^{29} C^5)^p p^{p/2+1} m^{(p-1)/2}, \tag{72}$$

где $g' \le \binom{p}{h_2 - 1}(h_2 - 1)! \left(\frac{Cm}{s}\right)^{h_2} N_1^{**}(Q)$, если p — нечетное, и $g' \le \binom{p}{h_2} \times$ $\times h_2! \left(\frac{Cm}{s}\right)^{h_2}$, если p — четное. В первом случае $t = h_2 - 1$ и, следовательно, $N_1^{**}(Q) = 0$, а во втором

$$g' \le 2^{2p} p^{h_2} \left(\frac{Cm}{s}\right)^{h_2} \le 2^{2p} p^p \left(\frac{Cm}{s}\right)^p \le (2^{27} C^5)^p p^{p/2+1} m^{(p-1)/2},$$

так как справедлива оценка (71). Мы опять получаем неравенство (66). Пусть σ^* — число решений уравнения (68) с различными q_r, $q_r \ne \mu_i^{(1)} + \mu_j^{(2)}$, $i \in [h_1]$, $j \in [h_2]$. Заметим, что если $h_1 + h_2 > p$, то величина σ^* равна нулю. Рассмотрим случай, когда $h_1 + h_2 = p$. Последнее равенство возможно, если только p является четным. В этом случае, используя оценки (71), $p \le Cm^{1/2}$, а также пункты 1 и 2 леммы, находим

$$\sigma^* \le C^{p/2}\binom{p}{h_1} h_1! h_2! \left(\frac{Cm}{s}\right)^{h_2} \le 2^p C^{p/2} p^{h_1+h_2} \left(\frac{Cm}{s}\right)^{h_2} =$$

$$= 2^p C^{p/2} p^p \left(\frac{Cm}{s}\right)^{h_2} \le 2^p C^{p/2} p^{p/2+1} m^{(p-1)/2}, \tag{73}$$

и неравенство (66) выполнено. В дальнейшем будем считать, что $h_1 + h_2 < p$.

Среди решений $(q_1, \dots, q_p)$ уравнения (68) найдутся элементы $q_{r(i)}$ такие, что $q_{r(i)} = \tilde{\mu}_i + \mu_i^{(2)}$, $i \in [h_2]$. Элементы $\mu_1^{(2)}, \dots, \mu_{h_2}^{(2)}$ можно расставить в соответствующих q_i не более чем $\binom{p}{h_2} h_2! \le p^{h_2}$ способами. Из свойства 1 следует, что число всех $\tilde{\mu}_i$ не превышает $(Cm/s)^{h_2}$. Не ограничивая общности, считаем, что различными среди элементов $\tilde{\mu}_1, \dots, \tilde{\mu}_{h_2}$ являются элементы $\tilde{\mu}_1, \dots, \tilde{\mu}_{h_2'}$, где $h_2' \le h_2$ и $h_2 - h_2' \equiv 0 \pmod 2$. Пусть $p_2 = (p - h_2)/2$, $\Delta = h_2 - h_2' \ge 0$, $h = h_1 + h_2$ и $h' = h_1 + h_2'$. Ясно, что h — четное, а число p_2 — натуральное, иначе уравнение (68) не имеет решений. Тогда $h' = h - \Delta$ является четным. Применяя лемму 3.3 (см. также замечание 3.1) и условие 2, находим

$$\sigma^* \le 2^{2p} C^p p^{p_2+h_2} \left(\frac{Cm}{s}\right)^{h_2} \max_{\tilde{\mu}_1, \dots, \tilde{\mu}_{h_2'} \in \Lambda_1} N_{p_2}\big(\mathcal{Q}; \mu_1^{(1)}, \dots, \mu_{h_1}^{(1)}, \tilde{\mu}_1, \dots, \tilde{\mu}_{h_2'}\big), \tag{74}$$

где $\mathcal{Q} = \{\lambda \dot{+} \mu \colon (\lambda, \mu) \in \Omega\} \subseteq \Lambda_1 \dot{+} \Lambda_1$. Согласно пунктам 3 и 5 имеем $|\Omega| \ge$ $\ge m^2/(Cs)$ и для всех $\lambda \in \Lambda_1$ выполнено $|\Omega_\lambda| \le Cm^2/s^2$. Отсюда

$$\frac{m^2}{2Cs} \le |\mathcal{Q}| \le \sum_{\lambda \in \Lambda_1} |\mathcal{Q}_\lambda| \le \sum_{\lambda \in \Lambda_1} |\Omega_\lambda| \le \frac{Cm^2}{s}.$$

Согласно четвертому условию леммы для произвольных $\lambda, \mu \in \Lambda_1$, $\lambda \ne \mu$, выполняется неравенство $|\Omega_\lambda \cap \Omega_\mu| \le \dfrac{Cm}{s}$. Следовательно, для любых $\lambda, \mu \in \Lambda_1$, $\lambda \ne \mu$, выполнено

$$|\mathcal{D}_\lambda \cap \mathcal{D}_\mu| \le |\Omega_\lambda \cap \Omega_\mu| \le \frac{\epsilon |\mathcal{Q}|}{s}, \tag{75}$$

где $\epsilon = 2C^2 s/m$. Применяя оценку из пункта 3 еще раз, находим

$$|\mathcal{D}_\lambda| = |\mathcal{Q}_\lambda| \le |\Omega_\lambda| \le \frac{2C^2|\mathcal{Q}|}{s} = \frac{C_*|\mathcal{Q}|}{s}, \tag{76}$$

где $C_* = 2C^2$.

Несложно видеть, что случай $p_2 = 1$ возможен только лишь (при условии $h < p$) когда $p = 3$, $h_1 = h_2 = 1$. В этом случае неравенства (66), (67) следуют из пунктов 1 (или 2)) леммы 3.5. Поэтому в дальнейшем будем считать, что $p_2 \ge$ ≥ 2. Предположим, что p_2 — четное. В этом случае, используя следствие 3.2 и оценку (76), находим

$$N_{p_2}\big(\mathcal{Q}; \mu_1^{(1)}, \dots, \mu_{h_1}^{(1)}, \tilde\mu_1, \dots, \tilde\mu_{h_2'}\big) \le$$

$$\le 2^{2p} p^{h'} \max\left\{\left(\frac{C_* p|\mathcal{Q}|}{s}\right)^{h'2} (N_{p_2}(\mathcal{Q}))^{(p_2-h')/p_2},\, (N_{p_2}(\mathcal{Q}))^{(p_2-h'/2)/p_2}\right\} \tag{77}$$

для любых $\tilde\mu_1, \dots, \tilde\mu_{h_2'}$. Предположим сначала, что $N_{p_2}(\mathcal{Q}) \ge \big(C_* p|\mathcal{Q}|/s\big)^{p_2}$. Тогда

$$N_{p_2}(\mathcal{Q}; \mu_1^{(1)}, \dots, \mu_{h_1}^{(1)}, \tilde\mu_1, \dots, \tilde\mu_{h_2'}) \le 2^{2p} p^{h'} N_{p_2}(\mathcal{Q}) (N_{p_2}(\mathcal{Q}))^{-h'/2p_2}. \tag{78}$$

По условию $|\Omega^\#| \ge m^3/(Cs^2)$. Отсюда $p \ge 2 \ge s/(2\epsilon|\Omega^\#|)$. Пусть

$$\mathbf{\Omega} = \big\{(\lambda, \mu)\colon \mathcal{Q}_\lambda \cap \mathcal{Q}_\mu \ne \varnothing,\ \ \lambda \ne \mu\big\}.$$

Ясно, что $\mathbf{\Omega} = \Omega^\#$. По свойству 5 имеем $|\Omega^\#| \le Cm^4/s^3$. Применяя лемму 3.4 и оценку (75), находим

$$N_{p_2}(\mathcal{Q}) \le 2^{10p} p^{p_2} (|\mathcal{Q}|\epsilon)^{p_2/2} \left(\frac{|\Omega^\#|}{s^2}\right)^{p_2/4} \le 2^{11p} C^p p^{p_2} m^{3p_2/2} s^{-5p_2/4}. \tag{79}$$

Подставляя последнее неравенство в (78), а затем используя неравенство (74), получаем

$$\sigma^* \le 2^{16p} C^{3p} p^p \left(\frac{m}{s}\right)^{h_2} p^{h'} m^{3p_2/2} s^{-5p_2/4} \left(p^{p_2} m^{3p_2/2} s^{-5p_2/4}\right)^{-h'/2p_2} =$$

$$= 2^{16p} C^{3p} p^{p+h/2} m^{3p/4+h_2-3h/4} s^{5h/8-5p/8-h_2} \left(\frac{s^{5/8}}{m^{3/4}}\right)^{h_2-\Delta} \left(\frac{1}{\sqrt{p}}\right)^{\Delta} = \sigma_1\sigma_2. \tag{80}$$

Поскольку $s \le m$, то $\sigma_2 \le \max\{s^{5h_2/8} m^{-3h_2/4}, p^{-h_2/2}\} = \tilde\sigma_2 \le 1$. Проверим, что для всех $p \le C\sqrt{m}$ выполняется неравенство

$$\sigma^* \le \sigma_1\sigma_2 \le (2^{35}C^4)^p p^{p/2+1} |Q|^{(p-1)/2}. \tag{81}$$

Если максимум в $\tilde\sigma_2$ достигается на первой величине, то, применяя оценку $p \le$ $\le C\sqrt{m}$, получаем, что для проверки (81) достаточно установить неравенство

$$m^{p/4+h/4-1/2+3p/4+h_2-3h/4-p/2+1/2-3h_2/4} =$$

$$= m^{p/2-h_1/2-h_2/4} \le s^{5p/8-5h/8+h_2-5h_2/8} = s^{5p/8-5h_1/8-h_2/4}. \tag{82}$$

По условию $m \le s^{1+1/31} = s^{1+\alpha_0}$. С учетом последней оценки неравенство (82) принимает вид

$$\alpha_0\left(\frac{p}{2} - \frac{h_1}{2} - \frac{h_2}{4}\right) \le \frac{p}{8} - \frac{h_1}{8},$$

что верно для всех h_1, h_2, $h_2 \le h_1$, $h_1 + h_2 \le p$ и $\alpha_0 \le 1/4$. Если же максимум в $\tilde\sigma_2$ достигается на его второй величине, то достаточно проверить, что

$$m^{p/4+h/4-1/2+3p/4+h_2-3h/4-p/2+1/2-h_2/4} =$$

$$= m^{p/2-h_1/2+h_2/4} \le s^{5p/8-5h/8+h_2} = s^{5p/8-5h_1/8+3h_2/8} \tag{83}$$

или

$$\alpha_0 \left(\frac{p}{2} - \frac{h_1}{2} + \frac{h_2}{4} \right) \le \frac{p}{8} - \frac{h_1}{8} + \frac{h_2}{8}.$$

Последнее неравенство следует из оценки $\alpha_0 \le 1/4$. Поэтому если $N_{p_2}(\mathcal{Q}) \ge$ $\ge (C_* p|\mathcal{Q}|/s)^{p/2}$ и число p_2 — четное, то неравенство (66) доказано.

Пусть теперь p — любое, $p \le C\sqrt{m}$, p_2 — четное и $N_{p_2}(\mathcal{Q}) \le (C_* p|\mathcal{Q}|/s)^{p_2}$. Тогда

$$N_{p_2}(\mathcal{Q}) \le \left(\frac{C_* p|\mathcal{Q}|}{s} \right)^{p_2} \le 2^p C^{2p} p^{p_2} \left(\frac{m}{s} \right)^{p-h_2}. \tag{84}$$

Используя последнюю оценку и неравенства (74), (77), находим

$$\sigma^* \le 2^{16p} C^{4p} p^p \left(\frac{m}{s} \right)^{h_2} p^{h'} \left(\frac{pm^2}{s^2} \right)^{h'/2} \left(\frac{m}{s} \right)^{p-h_2} \left(\frac{pm^2}{s^2} \right)^{-h'} =$$

$$= 2^{16p} C^{4p} p^{p+h/2} m^{p+h_2-h} s^{-p-h_2+h} \left(\frac{s}{m} \right)^{h_2-\Delta} \left(\frac{1}{\sqrt{p}} \right)^{\Delta} = \sigma_3 \sigma_3' = \sigma_4. \tag{85}$$

Так как $s \le m$, то $\sigma_3' \le \max\left\{ s^{h_2} m^{-h_2}, p^{-h_2/2} \right\} = \tilde{\sigma}_3' \le 1$. Если максимум в $\tilde{\sigma}_3'$ достигается на второй величине, то

$$\sigma^* \le \sigma_3 \sigma_3' \le 2^{16p} C^{4p} p^{p+h/2} m^{p+h_2-h} s^{-p-h_2+h} p^{-h_2/2} \le C^p \sigma_1 p^{-h_2/2}, \tag{86}$$

что, очевидно, не превышает $C^p \sigma_1 \tilde{\sigma}_2$. Неравенство (86) эквивалентно

$$\alpha_0 \left(\frac{p}{4} - \frac{h}{4} \right) \le \frac{p}{8} - \frac{h}{8} \tag{87}$$

и следует из оценки $\alpha_0 \le 1/2$. Если же максимум в σ_3' достигается на его первой величине, то

$$\sigma^* \le \sigma_3 \sigma_3' \le 2^{16p} C^{4p} p^{p+h/2} m^{p+h_2-h} s^{-p-h_2+h} s^{h_2} m^{-h_2} \le$$

$$\le (2^{35} C^5)^p p^{p/2+1} m^{(p-1)/2}, \tag{88}$$

так как

$$m^{p+h_2-h-h_2-(p-1)/2+p/4+h/4-1/2} = m^{3p/4-3h/4} \le s^{p+h_2-h-h_2} = s^{p-h}. \tag{89}$$

Неравенство (89) эквивалентно

$$\alpha_0 \left(\frac{3p}{4} - \frac{3h}{4} \right) \le \frac{p}{4} - \frac{h}{4} \tag{90}$$

и следует из оценки $\alpha_0 \le 1/3$. Из неравенств (86), (88) и (81) получаем неравенство (66) в случае четного p_2.

Пусть теперь число p_2 — нечетное. Тогда $p_2 \ge 3$, и мы можем применить следствие 3.2. Нетрудно проверить, что в случае нечетного p_2 получающиеся оценки

для σ^* не слишком отличаются от ситуации, когда p_2 является четным. Пусть, например, в формуле (63) максимум достигается на величине ϱ_1, а максимум в ϱ_1 — на его второй величине. Используя (79) и (80) с $p_2 = p_2 - 1$, $h' = h' - 1$, находим

$$\sigma^* \le \sigma_1\sigma_2 \frac{C_* C p m^2}{s^2} \frac{s^{5/8}}{p^{3/2} m^{3/4}} \le \sigma_1\sigma_2 \frac{C_* C m^{5/4}}{s^{11/8}} \le \sigma_1\sigma_2,$$

так как $s \ge m^{31/32}$ и $m \ge 2^{200} C^{50}$. Если максимум в ϱ_1 достигается на его первой величине, то, используя (84), (85) с $p_2 = p_2 - 1$, $h' = h' - 1$, получаем

$$\sigma^* \le \sigma_3\sigma_3' \frac{C_* C p m^2}{s^2} \frac{s}{p^{3/2} m} \le \sigma_3\sigma_3' \frac{C_* C m}{s} = \sigma_3\sigma_3'\sigma_3''.$$

Из-за наличия множителя σ_3'', $\sigma_3'' > 1$, неравенства (87), (90) примут вид

$$\alpha_0 \left(\frac{p}{4} - \frac{h}{4} + 1 \right) \le \frac{p}{8} - \frac{h}{8} \quad \text{и} \quad \alpha_0 \left(\frac{3p}{4} - \frac{3h}{4} + 1 \right) \le \frac{p}{4} - \frac{h}{4}.$$

Последние неравенства выполнены, так как $h < p$ и $\alpha_0 \le 1/31$.

Пусть теперь максимум в формуле (63) достигается на величине ϱ_2. Пусть, кроме того, максимум в самом ϱ_2 достигается на его второй величине. Используя (79) и (80) с $p_2 = p_2 - 1$, $h' = h' - 2$, находим

$$\sigma^* \le \frac{\sigma_1\sigma_2}{p^2} \le \sigma_1\sigma_2.$$

Если максимум в ϱ_2 достигается на его первой величине, то, используя (84), (85) с $p_2 = p_2 - 1$, $h' = h' - 2$, получаем

$$\sigma^* \le \frac{\sigma_3\sigma_3'}{p^2} \le \sigma_3\sigma_3'.$$

Таким образом, случай нечетного p_2 проанализирован полностью. Одновременно мы убедились в выполнении неравенства (67). Действительно, $\sigma_1\sigma_2 \le \sigma_1$, $\sigma_3\sigma_3' \le$ $\le \sigma_3$ и по неравенству (86) имеем $\sigma_3 \le \sigma_1$. Следовательно, для $h < p$

$$N_p^{**}\big(Q; \mu_1^{(1)}, \ldots, \mu_{h_1}^{(1)}; \mu_1^{(2)}, \ldots, \mu_{h_2}^{(2)}\big) \le$$

$$\le \sigma_1 \le 2^{20p} C^{4p} p^{p+h/2} m^{3p/4+h_2-3h/4} s^{5h/8-5p/8-h_2}.$$

Кроме того, из оценки (73) в случае $h = p$ следует, что

$$N_p^{**}\big(Q; \mu_1^{(1)}, \ldots, \mu_{h_1}^{(1)}; \mu_1^{(2)}, \ldots, \mu_{h_2}^{(2)}\big) \le$$

$$\le 2^p C^{p/2} p^p \left(\frac{Cm}{s} \right)^{h_2} \le (2C)^p p^{3p/2} \left(\frac{m}{s} \right)^{h_2} =$$

$$= (2C)^p p^{p+h/2} m^{3p/4+h_2-3h/4} s^{5h/8-5p/8-h_2}.$$

Лемма доказана.

Нам потребуется одно утверждение из теории графов, которое используется в доказательстве леммы 3.6, приведенной ниже. Мы благодарны С. Еханину за сообщение нам доказательства этой леммы.

Напомним, что *обхват* g неориентированного конечного графа $\Gamma = (V, E)$ — это длина минимального цикла. Связь между количеством вершин, числом ребер и обхватом изучалась во многих работах (см., например, [39 – 42]). Нам понадобится одно предложение из [42].

Предложение 3.3. *Пусть* $\Gamma = (V, E)$ *— конечный граф с обхватом* g *и* $k = \big\lceil |E|/|V| \big\rceil \geq 2$. *Тогда* $g \leq 2 + 2\log_k(|E|/4)$.

Заметим, что если $g \leq 4$, то оценка $g \leq 2 + 2\log_k(|E|/4)$ является очевидной.

С помощью предложения 3.3 мы доказываем следующую лемму.

Лемма 3.6. *Пусть* Λ, A_1, $A_2 \subseteq \mathbb{F}_2^n$ *— некоторые множества,* $\Lambda \subseteq A_1 + A_2$ *и* $|A_1| = |A_2| = t \geq 16$. *Пусть также множество* Λ *принадлежит семейству* $\mathbf{\Lambda}(2 + 2\log t)$. *Тогда* $|\Lambda| < 4t$.

Доказательство. Предположим противное. Пусть $|\Lambda| \geq 4t$ и $\Lambda' \subseteq \Lambda$ — произвольное множество мощности $4t$. Ясно, что Λ' принадлежит семейству $\mathbf{\Lambda}(2 + 2\log t)$. Построим неориентированный граф $\Gamma = (V, E)$. Множество вершин графа Γ — это объединение множеств A_1 и A_2, а вершина x соединена с вершиной y тогда и только тогда, когда $x + y \in \Lambda'$. Если некоторый элемент $\lambda \in \Lambda'$ представляется в виде суммы $x + y$ несколькими способами, то соединим ребром лишь одну пару таких вершин. Тогда $|E| = 4t$, $|V| = 2t$ и $|E|/|V| = 2$. Применяя предложение 3.3, находим в графе Γ цикл длины g, $g \leq 2 + 2\log t$. Пусть $(z_1, z_2), (z_2, z_3), \ldots, (z_{g-1}, z_g), (z_g, z_1)$ — этот цикл, $z_{g+1} := z_1$ и $\lambda_i = z_i + z_{i+1}$, $i = 1, \ldots, g$. Ясно, что все $\lambda_i \in \Lambda'$ различны. Кроме того, $\sum_{i=1}^{g} \lambda_i = 2\sum_{i=1}^{g} z_i = 0$. Получили противоречие с тем фактом, что $\Lambda \in \mathbf{\Lambda}(2 + 2\log t)$.

Лемма доказана.

Лемма 3.6 будет использована нами при доказательстве теорем 1.3 и 1.4.

В завершение настоящего пункта приведем простую лемму.

Лемма 3.7. *Пусть* N, t, k *— натуральные числа,* $k \leq t$ *и* $N > \binom{t}{k} 2^k$. *Тогда семейство* $\mathbf{\Lambda}(k)$ *содержит некоторое множество из* t *элементов.*

Доказательство. Рассмотрим все наборы длины t — $(a_1, \ldots, a_t)$, где $a_i \in \mathbb{F}_2^n$. Ясно, что существует ровно N^t таких наборов. Далее, существует не более $\binom{t}{k} 2^k$ уравнений

$$\sum_{i=1}^{t} a_i \varepsilon_i = 0, \quad a_i \in \mathbb{F}_2^n, \quad \varepsilon_i \in \{0, 1\}, \tag{91}$$

с коэффициентами ε_i, $\sum_{i=1}^{t} \varepsilon_i \leq k$. Любому уравнению (91), не все коэффициенты которого нулевые, удовлетворяет не более $N^{k-1}N^{t-k} = N^{t-1}$ решений $(a_1, \ldots, a_t)$. Кроме того,

$$N^{t-1}\binom{t}{k} 2^k < N^t.$$

Значит, найдется набор $(a_1, \ldots, a_t)$, удовлетворяющий только одному уравнению (91), а именно, уравнению с нулевыми коэффициентами. Легко видеть, что все элементы в наборе $(a_1, \ldots, a_t)$ различны. Отсюда множество $\Lambda = \{a_1, \ldots, a_t\}$, состоящее из t элементов, принадлежит семейству $\mathbf{\Lambda}(k)$.

Лемма доказана.

4. Доказательство основного результата. Примером множеств Q, удовлетворяющих условиям леммы 3.5, являются случайные подмножества $\Lambda_1 + \Lambda_2$. Для доказательства нам понадобится широко известное неравенство Бернштейна [17] (см. также [36]) об оценках вероятностей больших уклонений суммы независимых случайных величин. Нужный нам вариант этого неравенства содержится в [19].

Теорема 4.1. *Пусть $X_1, \ldots, X_n$ — последовательность независимых случайных величин, каждая из которых имеет нулевое математическое ожидание $\mathbb{E}X_j = 0$ и конечный второй момент $\mathbb{E}|X_j|^2 = \sigma_j^2$. Пусть $\sigma^2 = \sigma_1^2 + \ldots + \sigma_n^2$ и для всех $j \in [n]$ выполнено $|X_j| \le 1$. Пусть, наконец, t — вещественное число такое, что $\sigma^2 \ge 6nt$. Тогда*

$$\mathbb{P}\left(\left|\frac{X_1 + \ldots + X_n}{n}\right| \ge t\right) \le 4e^{-n^2t^2/8\sigma^2}.$$

Построим случайное множество $U \subset [s]\times[s]$ следующим образом. Зафиксируем $m \in (s, s^2]$. Возьмем s^2 независимых случайных величин $\xi_{i,j}$, $i, j \in [s]$, таких, что для всех i, j выполнено

$$\xi_{i,j} \in \{0, 1\}, \qquad \mathbb{P}(\xi_{i,j} = 1) = \frac{m}{s^2}.$$

Пусть

$$U = \big\{(i, j)\colon \xi_{i,j} = 1\big\}.$$

Лемма 4.1. *Пусть s, m, ρ, K — положительные целые числа такие, что $m > s$, $\rho m < s^2$, $K = \kappa\rho$ и, более того,*

$$\kappa \ge \frac{2\log(m/s)}{\log(s^2/(m\rho))} + 2, \tag{92}$$

$$\kappa \ge 5. \tag{93}$$

Тогда событие

$$\max_{I\subset[s], J\subset[s],\, |I|=|J|=\rho} \big|(I \times J) \cap U\big| \ge K$$

имеет вероятность $< 2^{-\rho}$.

Доказательство. Возьмем произвольные множества $I \subset [s]$ и $J \subset [s]$ такие, что $|I| = |J| = \rho$. Вероятность $P_{I,J}$ события $|(I \times J) \cap U| \ge K$ может быть оценена следующим образом:

$$P_{I,J} \le \binom{\rho^2}{K} \left(\frac{m}{s^2}\right)^K.$$

Далее,

$$\sum_{I,J} P_{I,J} \le \binom{s}{\rho}^2 \binom{\rho^2}{K} \left(\frac{m}{s^2}\right)^K \le$$

$$\le \left(\frac{es}{\rho}\right)^{2\rho} \left(\frac{e\rho^2}{K}\right)^K \left(\frac{m}{s^2}\right)^K = \left(\frac{es}{\rho}\right)^{2\rho} \left(\frac{e\rho m}{\kappa s^2}\right)^{\kappa\rho} = \Pi_1^\rho \Pi_2^\rho,$$

где

$$\Pi_1 = \left(\frac{\rho m}{s^2}\right)^{\kappa-2} \frac{m^2}{s^2},$$

$$\Pi_2 = \frac{e^{\kappa+2}}{\kappa^\kappa}.$$

Согласно (92) имеем $\Pi_1 \le 1$. Аналогично, по (93) выполнено $\Pi_2 < 1/2$. Таким образом,

$$\sum_{I,J} P_{I,J} < 2^{-\rho},$$

и лемма 4.1 доказана.

Пусть Λ_1, Λ_2 — произвольные непересекающиеся подмножества $\mathbb{F}_2^n$, $|\Lambda_1| = |\Lambda_2| = s$ и $\Lambda_1 \bigsqcup \Lambda_2 \in \mathbf{\Lambda}(2\rho+2)$. Пусть также

$$\Lambda_\nu = \{\lambda_1^\nu, \ldots, \lambda_s^\nu\} \quad \nu = 1, 2.$$

Используя построенное выше множество U, получаем случайное множество

$$Q = \{\lambda_i^1 + \lambda_j^2 \colon (i,j) \in U\}.$$

***Следствие* 4.1.** *Пусть условия леммы* 4.1 *выполнены. Тогда событие, заключающееся в том, что существует подпространство $\mathbb{F}_2^n$ размерности ρ, имеющее не менее K общих элементов с Q, имеет вероятность меньше $2^{-\rho}$.*

Доказательство. Возьмем произвольное подпространство $Y \subset \mathbb{F}_2^n$ размерности ρ, и пусть E — максимальное линейно независимое подмножество векторов из $(\Lambda_1 + \Lambda_2) \cap Y$. Очевидно, что $|E| \le \rho$, и мы находим множества $H \subseteq [s]$, $J \subseteq [s]$ такие, что $|H| = |J| = \rho$ и

$$Y \cap Q \subseteq \{\lambda_i^1 + \lambda_j^2 \in Q \colon i \in H,\, j \in J\}.$$

Теперь осталось применить лемму 4.1.

Следствие доказано.

Покажем, что построенное выше случайное множество Q удовлетворяет всем условиям леммы 3.5. Сохраним все обозначения леммы 3.5.

Лемма 4.2. *Пусть Q — такое же, как в предыдущей лемме, $s \ge 16$, $s \ge m^{31/32}$ и $m \ge 2^{20} s \log s$. Тогда с вероятностью больше $1/2$ для всех $\lambda, \lambda' \in \Lambda_1$, $\lambda \ne \lambda'$, выполняется неравенство*

$$|D_\lambda \cap D_{\lambda'}| \le 4, \tag{94}$$

для любого $\lambda \in \Lambda_1$ имеем $|D_\lambda| \le 4m/s$, а для произвольного $\mu \in \Lambda_2$ выполнено $|\tilde{D}_\mu| \le 4m/s$. Далее, для любого $\lambda \in \Lambda_1$ выполнено $|\Omega_\lambda| \le 16m^2/s^2$, для произвольных $\lambda, \lambda' \in \Lambda_1$, $\lambda \ne \lambda'$, имеем

$$|\Omega_\lambda \cap \Omega_{\lambda'}| \le \frac{64m}{s} \tag{95}$$

и $m/2 \le |Q| \le 2m$, $|\Omega| \ge m^2/(32s)$, $m^3/(2^{18}s^2) \le |\Omega^\#| \le 2^8 m^4/s^3$.

Доказательство. Пусть $K = 4$ и $q = m/s$. Возьмем произвольные λ, $\lambda' \in [s]$, $\lambda \ne \lambda'$. Вероятность $p_{\lambda,\lambda'}$ события $|D_\lambda \cap D_{\lambda'}| \ge K$ оценивается следующим образом:

$$p_{\lambda,\lambda'} \le \binom{s}{K} \left(\frac{m}{s^2}\right)^{2K}.$$

По условию $s \geq m^{31/32}$. Следовательно,

$$\sum_{\lambda,\lambda' \in \Lambda_1} p_{\lambda,\lambda'} \leq s^2 \left(\frac{es}{K}\right)^K \left(\frac{m}{s^2}\right)^{2K} = s^2 \left(\frac{em^2}{Ks^3}\right)^K \leq \left(\frac{e}{4}\right)^4 < \frac{1}{4} < 1,$$

и мы видим, что с вероятностью больше $3/4$ неравенство (94) выполнено.

Докажем, что для любого $\lambda \in \Lambda_1$ выполнено $m/(4s) \leq |D_\lambda| \leq 4m/s$. Применяя теорему 4.1 с $t = m/(12s^2)$, получаем, что вероятность противоположного события, заключающегося в том, что $|D_\lambda| > 4m/s$ или $|D_\lambda| < m/(4s)$ (константу 4 можно заменить числом, близким к 1) для какого-либо $\lambda \in \Lambda_1$, не превышает $4se^{-2^{-12}q}$. Напомним, что

$$\tilde{D}_\mu = \{\lambda \in \Lambda_1 \colon \lambda + \mu \in Q\}, \quad \mu \in \Lambda_2.$$

Аналогично вышеизложенному, вероятность события $|\tilde{D}_\mu| > 4m/s$ или $|\tilde{D}_\mu| < m/(4s)$ для какого-либо $\mu \in \Lambda_2$ не больше $4se^{-2^{-12}q}$. По условию $m \geq 2^{20} s \log s$. Отсюда $8se^{-2^{-12}q} < 1/16$ и, следовательно, с вероятностью больше $15/16$ для всех $\lambda \in \Lambda_1$ выполнено $m/(4s) \leq |D_\lambda| \leq 4m/s$; подобным образом с вероятностью больше $15/16$ для любого $\mu \in \Lambda_2$ имеем $m/(4s) \leq |\tilde{D}_\mu| \leq 4m/s$. Значит, для произвольного $\lambda \in \Lambda_1$ имеет место неравенство $|\Omega_\lambda| \leq |D_\lambda| \max_{\mu \in \Lambda_2} |\tilde{D}_\mu| \leq 16m^2/s^2$. Действуя, как и выше, получаем, что вероятность события $|Q| > 2m$ или $|Q| < m/2$ не превышает $4e^{-2^{-12}m}$. Поскольку $m \geq 2^{20} s \log s$, то $4e^{-2^{-12}m} < 1/32$.

Проверим выполнение неравенства (95). Пусть $K' = 11$ и $t = [4m/s]$. Возьмем $\lambda, \lambda' \in \Lambda_1$, $\lambda \neq \lambda'$. Тогда вероятность того, что $m/4s \leq |\tilde{D}_\mu| \leq 4m/s$ при всех $\mu \in \Lambda_2$, далее, $|D_{\lambda_1} \cap D_{\lambda_1'}| \leq 4$ для всевозможных $\lambda_1, \lambda_1' \in \Lambda_1$, $\lambda_1 \neq \lambda_1'$ и при этом $|\Omega_\lambda \cap \Omega_{\lambda'}|$ больше $64m/s$, не превышает

$$\mathbb{P}\left\{|(\Omega_\lambda \cap \Omega_{\lambda'}) \setminus \{\lambda, \lambda'\}| > \frac{64m}{s} - 2\right\} \leq$$

$$\leq \mathbb{P}\left\{\sum_{\nu \in D_\lambda} \left|\left(\tilde{D}_\nu \cap \left(\bigcup_{\nu' \in D_{\lambda'},\, \nu' \neq \nu} \tilde{D}_{\nu'}\right)\right) \setminus \{\lambda, \lambda'\}\right| > \frac{64m}{s} - 2 - \sum_{\nu \in D_\lambda \cap D_{\lambda'}} |\tilde{D}_\nu|\right\} \leq$$

$$\leq \mathbb{P}\left\{\sum_{\nu \in D_\lambda} \left|\left(\tilde{D}_\nu \cap \left(\bigcup_{\nu' \in D_{\lambda'},\, \nu' \neq \nu} \tilde{D}_{\nu'}\right)\right) \setminus \{\lambda, \lambda'\}\right| > \frac{4m}{s} K'\right\},$$

поскольку $\Omega_\lambda \subseteq \bigcup_{\nu \in D_\lambda} \tilde{D}_\nu$, $\Omega_{\lambda'} \subseteq \bigcup_{\nu' \in D_{\lambda'}} \tilde{D}_{\nu'}$ и все $\tilde{D}_\nu$ здесь содержат элемент λ, а все $\tilde{D}_{\nu'}$ — элемент λ'. По условию $s \geq m^{31/32}$. Отсюда вероятность события

$$\mathbb{P}\left\{\left|\bigcup_{\nu \in D_\lambda} \left(\tilde{D}_\nu \cap \left(\bigcup_{\nu' \in D_{\lambda'},\, \nu' \neq \nu} \tilde{D}_{\nu'}\right)\right) \setminus \{\lambda, \lambda'\}\right| > \frac{4m}{s} K'\right\}$$

не превышает

$$s\binom{s}{K'} \left(\frac{m}{s^2}\right)^{2K'} t^{K'} \leq s\left(\frac{em^2 t}{K' s^3}\right)^{K'} < \frac{1}{16s^2}$$

и, значит, с вероятностью больше $5/8$ выполнено

$$\frac{m}{4s} \le |\tilde{D}_\mu| \le \frac{4m}{s} \quad \forall \mu \in \Lambda_2,$$

$$\left|D_{\lambda_1} \cap D_{\lambda_1'}\right| \le 4 \quad \forall \lambda_1, \lambda_1' \in \Lambda_1, \lambda_1 \ne \lambda_1', \tag{96}$$

$$\left|\Omega_\lambda \cap \Omega_{\lambda'}\right| \le \frac{64m}{s} \quad \forall \lambda, \lambda' \in \Lambda_1, \lambda \ne \lambda'.$$

Докажем неравенство $|\Omega^\#| \le 2^8 m^4/s^3$. Имеем

$$s\left(\frac{16m^2}{s^2}\right)^2 \ge \sum_{\lambda\in\Lambda_1} |\Omega_\lambda|^2 = \sum_\lambda \left(\sum_x \Omega_\lambda(x)\right)^2 =$$

$$= \sum_{x,y} \left|\Omega_x \cap \Omega_y\right| \ge \sum_{(x,y)\in\Omega^\#} \left|\Omega_x \cap \Omega_y\right| \ge |\Omega^\#|,$$

и мы получили оценку $|\Omega^\#| \le 2^8 m^4/s^3$.

Нам осталось доказать, что $|\Omega| \ge m^2/(32s)$ и $m^3/(2^{20}s^2) \le |\Omega^\#|$. Второе неравенство вытекает из первого. Действительно, применяя неравенство Коши – Буняковского, находим

$$|\Omega|^2 = \left(\sum_{\lambda\in\Lambda_1} |\Omega_\lambda|\right)^2 = \left(\sum_{\lambda\in\Lambda_1}\sum_{x\in\Lambda_1} \Omega_\lambda(x)\right)^2 \le \left(\sum_{\lambda,\lambda'\in\Lambda_1} |\Omega_\lambda \cap \Omega_{\lambda'}|\right) s.$$

Из последнего неравенства и оценки (96) следует, что

$$\frac{|\Omega|^2}{s} \le |\Omega| + \sum_{(\lambda,\lambda')\in\Omega^\#} |\Omega_\lambda \cap \Omega_{\lambda'}| \le |\Omega| + \frac{64m}{s}|\Omega^\#|.$$

Считая доказанным неравенство $|\Omega| \ge m^2/(32s)$ и используя оценку $m \ge 2^{20} s \log s$, получаем $|\Omega|^2/s - |\Omega| \ge |\Omega|^2/2s$ и, следовательно, $|\Omega^\#| \ge m^3/(2^{20}s^2)$.

Докажем, что $|\Omega| \ge m^2/(32s)$. Используя формулу $|\tilde{D}_\lambda| = |Q_\lambda|$, учитывая $|\tilde{D}_\lambda| \ge m/4s$ и (94), находим

$$\frac{m^2}{16s} \le \sum_{\lambda\in\Lambda_2} |\tilde{D}_\lambda|^2 = \sum_{\lambda\in\Lambda_2} \left(\sum_{x\in\Lambda_1} Q(x+\lambda)\right)^2 = \sum_{x,y\in\Lambda_1}\sum_{\lambda\in\Lambda_2} D_x(\lambda) D_y(\lambda) =$$

$$= \sum_{x,y\in\Lambda_1,\, x\ne y} |D_x \cap D_y| + |Q| \le 4|\Omega| + |Q|. \tag{97}$$

Еще раз применяя неравенство $m \ge 2^{20} s \log s$, оценку $|Q| \le 2m$ и используя (97), получаем $|\Omega| \ge m^2/(32s)$. Итак, все утверждения леммы 4.2 выполнены с вероятностью не меньшей

$$\frac{5}{8} - \frac{1}{32} - \frac{1}{16} = \frac{17}{32} > \frac{1}{2} > 0.$$

Лемма доказана.

***Замечание* 4.1.** Выше были доказаны не совпадающие по порядку неравенства $m^3/(2^{18}s^2) \le |\Omega^{\#}| \le 2^8 m^4/s^3$. Можно получить верхнюю оценку для мощности множества $\Omega^{\#}$ вида Mm^3/s^2, где M — некоторая абсолютная константа, но нам это более тонкое неравенство не потребуется.

Итак, построенное множество Q удовлетворяет всем условиям леммы 3.5 и, следовательно, для него выполнена оценка (66). Использовав этот факт, докажем обобщение леммы 4.1.

Лемма 4.3. *Пусть p — нечетное число, ρ — натуральное число и Y — подпространство размерности ρ. Пусть Q — такое же, как в предыдущей лемме, а C — число из леммы 3.5. Предположим, что $\rho \le \sqrt{s}$ и $s \ge m^{31/32}$, $s \ge 2^{500}$. Тогда для всех $p \le C\sqrt{m}$ с положительной вероятностью выполнено*

$$\sum_{x \in \mathbb{F}_2^n} (Q *_{p-1} Q)(x) Y(x) \le (2^{100}\kappa C^5)^p \rho p^{(p-1)/2} m^{(p-1)/2}. \tag{98}$$

Доказательство. Пусть $C_1 = 2^{35}C^5$. Будем доказывать неравенство (98) индукцией по p. Для $p = 1$ последнее неравенство было получено в следствии 4.1. Предположим, что $p \ge 3$. Так как $s \ge 2^{500}$, то $s^{3/8}m^{-1/4} \le \sqrt{s}/2$. Дополняя пространство Y базисными векторами, добиваемся выполнения неравенств $s^{3/8}m^{-1/4} \le \rho \le \sqrt{s}$. Пусть H и J — такие же, как и в следствии 4.1. Другими словами, они обладают тем свойством, что для множества E — максимального линейно независимого подмножества векторов из $Y \cap (\Lambda_1 + \Lambda_2)$ — выполнено

$$E \subseteq \{\lambda_i^1 + \lambda_j^2 \colon \lambda_i^1 \in \Lambda_1,\, \lambda_j^2 \in \Lambda_2,\, i \in H,\, j \in J\}.$$

Пусть также $\Lambda_1' = \{\lambda_i \in \Lambda_1 \colon i \in H\}$, $\Lambda_2' = \{\lambda_i \in \Lambda_2 \colon i \in J\}$. Требуется оценить число решений уравнения

$$q_1 + \ldots + q_p = y = \mu_1^{(1)} + \ldots + \mu_{h_1}^{(1)} + \mu_1^{(2)} + \ldots + \mu_{h_2}^{(2)}, \tag{99}$$

где $h_1, h_2 \le p$ — нечетные, $y \in Y$, $q_j \in Q$, $j \in [p]$, $\mu_i^{(1)} \in \Lambda_1'$, $i \in [h_1]$ и $\mu_i^{(2)} \in \Lambda_2'$, $i \in [h_2]$. Очевидно, можно считать, что все элементы $\mu_i^{(1)}$, $\mu_i^{(2)}$ различны. При этом порядок $\mu_i^{(1)}$, $\mu_i^{(2)}$ в уравнении не имеет значения. Всюду ниже будем предполагать, для определенности, что $h_2 \le h_1$. Обозначим число решений уравнения (99) через $\tilde{N}_p(Q) := \sigma$, а число решений (99) с фиксированными $\mu_1^{(1)}, \ldots, \mu_{h_1}^{(1)}, \mu_1^{(2)}, \ldots, \mu_{h_2}^{(2)}$ через $\tilde{N}_p\big(Q; \mu_1^{(1)}, \ldots, \mu_{h_1}^{(1)}; \mu_1^{(2)}, \ldots, \mu_{h_2}^{(2)}\big)$. Аналогично обозначим количество решений (99) с различными q_i через $\tilde{N}_p^*(Q)$, число решений (99) с различными q_r, $q_r \ne \mu_i^{(1)} + \mu_j^{(2)}$, $i \in [h_1]$, $j \in [h_2]$, через $\tilde{N}_p^{**}(Q)$, а также определим соответствующие величины $\tilde{N}_p^*\big(Q; \mu_1^{(1)}, \ldots, \mu_{h_1}^{(1)}; \mu_1^{(2)}, \ldots, \mu_{h_2}^{(2)}\big)$, $\tilde{N}_p^{**}(Q; \mu_1^{(1)}, \ldots, \mu_{h_1}^{(1)}; \mu_1^{(2)}, \ldots, \mu_{h_2}^{(2)})$. Для доказательства (98) достаточно показать, что для всех $2 \le l \le p$ выполняется неравенство

$$\tilde{N}_l^*(Q) \le (2^{15}C_2)^l \kappa^l \rho p^{(l-1)/2} m^{(l-1)/2}.$$

Действительно, применяя лемму 3.1, следствие 4.1 и рассуждая, как и при доказательстве леммы 3.4, находим

$$\sigma \le 8^p \tilde{N}_1^*(Q) p^{(p-1)/2} m^{(p-1)/2} + 8^p \sum_{t=0}^{(p-3)/2} \tilde{N}_{p-2t}^*(Q) t^t m^t \le$$

$$\le 8^p\kappa\rho p^{(p-1)/2}m^{(p-1)/2} + 8^p(\kappa 2^{15}C_2)^p\rho\sum_{t=0}^{(p-3)/2} p^{(p-1)/2-t}m^{(p-1)/2-t}p^t m^t \le$$

$$\le (2^{20}\kappa C_2)^p\rho p^{(p-1)/2}m^{(p-1)/2}.$$

Пусть $h = h_1 + h_2$. Если мы докажем теперь, что для всех p выполнено

$$\tilde N_p^{**}(Q) \le (\kappa C_2)^p p^{p+h/2}m^{3p/4+h_2-3h/4}s^{5h/8-5p/8-h_2}\frac{\rho^{h_1+h_2}}{h_1!\,h_2!}, \tag{100}$$

то, использовав лемму 4.1, получим

$$\tilde N_p^*(Q) \le g + \sum_{t=0}^{h_2}\binom{p}{t}t!\,\tilde N_{p-t}^{**}(Q)\binom{[\kappa\rho]}{t} \le$$

$$\le g + 2^{2p}\sum_{t=0}^{h_2}\frac{\rho p^t}{t!(h_1-t)!(h_2-t)!}(\kappa C_2)^{p-t}p^{p-t+h/2-t}\times$$

$$\times m^{3(p-t)/4+h_2-t-3h/4+3t/2}s^{5h/8-5t/4-5p/8+5t/8-h_2+t}\rho^{h-2t}(\kappa\rho)^t =$$

$$= g + \frac{(8\kappa C_2)^p}{h_2!}\frac{\rho}{\sqrt{pm}}\sum_{t=0}^{h_2}\frac{h_2!}{t!(h_1-t)!(h_2-t)!}\times$$

$$\times p^{p+h/2-t}m^{3p/4+h_2-3h/4-t/4}s^{5h/8-5p/8-h_2+3t/8}\rho^{h-t}, \tag{101}$$

$$g \le p!\binom{[\kappa\rho]}{p} \le (\kappa\rho)^p \le \kappa^p\rho m^{(p-1)/2} \le \kappa^p\rho p^{(p-1)/2}m^{(p-1)/2},$$

так как $\rho \le \sqrt{s} \le \sqrt{m}$. Ясно, что $h_1 \le p$, поскольку в противном случае уравнение (99) не имеет решений. Отсюда $(h_1-t)!p^t \ge h_1!$ для любого $t \le h_2$. Применяя последнее неравенство и оценку $s^{3/8}m^{-1/4} \le \rho$, находим

$$\tilde N_p^*(Q) \le \frac{(2^4\kappa C_2)^p}{h_1!h_2!}\frac{\rho}{\sqrt{pm}}p^{p+h/2}m^{3p/4+h_2-3h/4}s^{5h/8-5p/8-h_2}\rho^h = \tilde\sigma. \tag{102}$$

Небольшое вычисление показывает, что последнее выражение не превышает $(2^{15}C_2)^p\kappa^p\rho p^{(p-1)/2}m^{(p-1)/2}$. Действительно, предположим сначала, что $h \le p/8$, и не будем учитывать множитель $1/(h_1!h_2!)$ в неравенстве (102). По условию $\rho \le \sqrt{s}$ и $p \le C\sqrt{m}$. С учетом последних неравенств и оценки (102) достаточно проверить, что

$$s^{5p/8+h_2-5h/8-h/2} = s^{5p/8+h_2-9h/8} \ge$$

$$\ge m^{3p/4+h_2-3h/4-(p-1)/2+p/4+h/4} = m^{p/2+h_2-h/2}. \tag{103}$$

Имеем $s^{32/31} = s^{1+\alpha_0} \ge m$. Значит, неравенство (103) принимает вид

$$\alpha_0\left(\frac{p}{2}+h_2-\frac{h}{2}\right) \le \frac{p}{8}-\frac{5h}{8}. \tag{104}$$

Последнее неравенство, очевидно, выполнено, поскольку $\alpha_0 \le 1/31$ и $h \le p/8$.

Пусть теперь $h \ge p/8$. Тогда

$$\frac{1}{h_1!h_2!} = \frac{1}{(h_1+h_2)!}\binom{h_1+h_2}{h_1} \le \frac{2^p}{(h_1+h_2)!} \le \frac{(2e)^p}{(h_1+h_2)^{h_1+h_2}} \le 2^{6p}p^{-h}.$$

Снова используя оценки $\rho \le \sqrt{s}$, $p \le C\sqrt{m}$, записываем неравенство (102) в виде

$$s^{5p/8+h_2-5h/8-h/2} = s^{5p/8+h_2-9h/8} \ge m^{p/2+h_2-h/2-h/2} = m^{p/2+h_2-h}. \qquad (105)$$

Для проверки последнего неравенства достаточно убедиться в том, что

$$\alpha_0\left(\frac{p}{2} - h_1\right) \le \frac{p}{8} - \frac{h}{8}. \qquad (106)$$

Если $h_1 \ge p/2$, то последнее неравенство выполнено. Если же $h_1 < p/2$, то неравенство (106) принимает вид

$$\alpha_0 \le \frac{1}{4}\left(1 + \frac{h_1 - h_2}{p - 2h_1}\right),$$

что верно, поскольку $\alpha_0 \le 1/4$.

Итак, достаточно оценить величину

$$\tilde{N}_p^{**}(Q) = \sum_{\mu_1^{(1)},\ldots,\mu_{h_1}^{(1)},\,\mu_1^{(2)},\ldots,\mu_{h_2}^{(2)}}{}^{*} \tilde{N}_p^{**}\big(Q;\mu_1^{(1)},\ldots,\mu_{h_1}^{(1)};\mu_1^{(2)},\ldots,\mu_{h_2}^{(2)}\big),$$

где $\sum^{*}$ означает, что мы не учитываем перестановки элементов $\mu_1^{(1)},\ldots,\mu_{h_1}^{(1)}$, $\mu_1^{(2)},\ldots,\mu_{h_2}^{(2)}$. Ясно, что

$$\tilde{N}_p^{**}(Q) = \sum_{\mu_1^{(1)},\ldots,\mu_{h_1}^{(1)},\,\mu_1^{(2)},\ldots,\mu_{h_2}^{(2)}}{}^{*} N_p^{**}(Q;\mu_1^{(1)},\ldots,\mu_{h_1}^{(1)};\mu_1^{(2)},\ldots,\mu_{h_2}^{(2)}) \le$$

$$\le \max_{\mu_1^{(1)},\ldots,\mu_{h_1}^{(1)},\,\mu_1^{(2)},\ldots,\mu_{h_2}^{(2)}} N_p^{**}(Q;\mu_1^{(1)},\ldots,\mu_{h_1}^{(1)};\mu_1^{(2)},\ldots,\mu_{h_2}^{(2)})\frac{\rho^{h_1+h_2}}{h_1!\,h_2!}.$$

Применяя неравенство (67) для любого набора $\mu_1^{(1)},\ldots,\mu_{h_1}^{(1)}$, $\mu_1^{(2)},\ldots,\mu_{h_2}^{(2)}$, находим

$$N_p^{**}(Q;\mu_1^{(1)},\ldots,\mu_{h_1}^{(1)};\mu_1^{(2)},\ldots,\mu_{h_2}^{(2)}) \le$$

$$\le C_2^p p^{p+h/2} m^{3p/4+h_2-3h/4} s^{5h/8-5p/8-h_2}\frac{\rho^{h_1+h_2}}{h_1!\,h_2!},$$

и мы получили (100).

Лемма доказана.

Перейдем к доказательству основного результата настоящей статьи.

***Доказательство теоремы* 1.3.** Пусть $C = 2^{20}$, $C_1 = 2^{35}C^5 = 2^{135}$, $M = 2^{100}\cdot 8\cdot C^5 = 2^{203}$, а также $K = 2^5C_1 = 2^{140}$ и $c = 2^7$. Положим $t = \left[\log\left(\frac{1}{2\delta}\right)\right]$,

$n = td$, d — натуральное число, $m = \left[2^{-7}K^{-4}\delta^2\alpha^{-2}c^{-2}\right]$, $k = \left[\sqrt{m}\,\right] \le [\delta\alpha^{-1}] = k'$ и $s = \lceil m^{(31+\varepsilon)/32}\rceil \ge m^{31/32}$. Пусть Λ_1, Λ_2 — непересекающиеся множества равной мощности s такие, что их объединение принадлежит семейству $\mathbf{\Lambda}(4k')$. Множества Λ_1, Λ_2 с указанным свойством существуют, поскольку из неравенства (9) следует, что $[N/t] \ge \binom{s}{4k'}2^{4k'}$, и мы можем применить лемму 3.7.

Выберем в качестве Q случайное подмножество суммы $\Lambda_1 + \Lambda_2$ так, чтобы каждый элемент принадлежал Q с вероятностью m/s^2. Тогда для множества Q справедливы все леммы этого пункта. Поскольку $s \ge m^{31/32}$, можно взять в качестве числа κ в лемме 4.1 и следствии 4.1, например, число 8, так как для всех $\rho \le \sqrt{s}$ имеем

$$\frac{2\log(m/s)}{\log(s^2/(m\rho))} + 2 \le \frac{4}{29} + 2 < 3.$$

По условию $\alpha \le 2^{-1000/(1-\varepsilon)^2}\delta$. Отсюда $|Q| \ge m/2 \ge 16c^2K^2$, $m \ge 2^{1000/(1-\varepsilon)^2}$ и, следовательно, $m \ge 2^{20}s\log s$. Применяя лемму 4.2, получаем, что все условия леммы 3.5 выполнены с константой $C = 2^{20}$. Далее, из леммы 4.3 следует, что множество Q удовлетворяет неравенству (98). Значит, мы имеем оценку (24), причем константа M в этой оценке равна $2^{100}\kappa C^5 = 2^{203}$. Следовательно, мы можем применить предложение 2.1 и построить множество A, для которого справедливы пункты 1 и 2 этого предложения, а также выполнена оценка (25). Отсюда следует неравенство (10).

Имеем $0 < \alpha \le 2^{-1000/(1-\varepsilon)^2}\delta$. Используя неравенство (9), легко видеть, что $2 + 2\log s \le 4k'$. Применяя лемму 3.6, получаем, что любое множество из семейства $\mathbf{\Lambda}(4k')$, принадлежащее $\Lambda_1 + \Lambda_2$, имеет мощность не больше $4s$. Отсюда максимальное диссоциативное подмножество $\mathcal{R}_\alpha(A)$, принадлежащее семейству $\mathbf{\Lambda}(4k')$, имеет мощность не больше $4st$ и мы получаем (11).

Еще раз используя условие $\alpha \le 2^{-1000/(1-\varepsilon)^2}\delta$, находим $\sqrt{s} \le 2^{-10}M^{-3}\sqrt{m}$. В лемме 4.3 на параметр ρ накладывается ограничение $\rho \le \sqrt{s}$. Значит, при условии (12) неравенство (13) выполнено.

Теорема доказана.

Аналогичным образом доказывается теорема 1.4.

***Доказательство теоремы* 1.4.** Как и в доказательстве теоремы 1.3, возьмем $C = 2^{20}$, $C_1 = 2^{35}C^5 = 2^{135}$, $M = 2^{100}\cdot 8\cdot C^5 = 2^{203}$, $K = 2^5C_1 = 2^{140}$, $K' = 2^5MK = 2^{348}$, $c = 2^7$, $t = \left[\log\left(\dfrac{1}{2\delta}\right)\right]$, $n = td$, d — натуральное число, $m = \left[2^{-7}(K')^{-4}\delta^2\alpha^{-2}c^{-2}\right]$, $k = \left[\sqrt{m}\,\right] \le [\delta\alpha^{-1}] = k'$ и $s = \lceil m^{(31+\varepsilon_1)/32}\rceil \ge$ $\ge m^{31/32}$. Пусть Λ_1, Λ_2 — непересекающиеся множества равной мощности s такие, что их объединение принадлежит семейству $\mathbf{\Lambda}(4k')$. Действуя, как и выше, убеждаемся, что любое множество из семейства $\mathbf{\Lambda}(4k')$, принадлежащее $\Lambda_1 + \Lambda_2$, имеет мощность не больше $4s$. Выберем в качестве Q случайное подмножество суммы $\Lambda_1 + \Lambda_2$ так, чтобы каждый элемент принадлежал Q с вероятностью m/s^2. Тогда для множества Q справедливы все леммы этого пункта. Значит, Q удовлетворяет условиям леммы 3.5 и, следовательно, имеет место неравенство (23). Используя предложение 2.1, получаем множество A, для которого выполнены неравенства (17), (18).

Нам осталось доказать неравенство (19). По условию $I \subseteq \mathcal{R}_\alpha(A)$, $s \ge m^{31/32}$ и

$$|I| \le \left(\frac{\delta}{\alpha}\right)^{\frac{15+\varepsilon_1-\varepsilon_2}{8}} \le s^2 m^{-(1+\varepsilon_2/16)} < \frac{s^2}{m}.$$

Из пункта 2 следует, что $\mathcal{R}_\alpha(A) = \{0\} \bigsqcup \left(\bigsqcup_{w=1}^{t} Q_w\right)$. Пусть Y_w — аффинное подпространство, натянутое на векторы из $I \cap \mathcal{L}_w$, $\rho_w = \dim Y_w$, $w \in [t]$. Пусть также $\rho = |I|$ и $\kappa = \dfrac{2\log(m/s)}{\log(s^2/(m\rho))} + 2$. Применяя следствие 4.1, получаем, что $|Y_w \cap Q_w| \le \kappa\rho_w$. Отсюда

$$\left|\mathrm{Span}\,(I) \cap \mathcal{R}_\alpha(A)\right| \le \sum_{w=1}^{t} |Y_w \cap Q_w| \le \kappa\rho \le \frac{2^{10}|I|}{\varepsilon_2}.$$

Теорема доказана.

1. *Behrend F. A.* On sets of integers which contain no three terms in arithmetic progression // Proc. Nat. Acad. Sci. – 1946. – **23**. – P. 331 – 332.
2. *Erdös P., Turán P.* On some sequences of integers // J. London Math. Soc. – 1936. – **11**. – P. 261 – 264.
3. *Frankl P., Graham G., Rödl V.* On sets of abelian groups with no 3-term arithmetic progressions // J. Combin. Theory. – 1987. – **45**, Ser. A. – P. 157 – 161.
4. *Furstenberg H.* Recurrence in ergodic theory and combinatorial number theory. – Princeton, N.J., 1981.
5. *Furstenberg H.* Ergodic behavior of diagonal measures and a theorem of Szemerédi on arithmetic progressions // J. Anal. Math. – 1977. – **31**. – P. 204 – 256.
6. *Furstenberg H., Katznelson Y.* An ergodic Szemerédi theorem for commuting transformations // Ibid. – 1978. – **34**. – P. 275 – 291.
7. *Furstenberg H., Ornstein D., Katznelson Y.* The ergodic theoretical proof of Szemerédi's theorem // Bull. Amer. Math. Soc. – 1982. – **7**, № 3. – P. 527 – 552.
8. *Gowers W. T.* Rough structure and classification // Geom. Funct. Anal. Special Volume GAFA2000 "Visions in Mathematics", Tel Aviv. – 1999. – Pt I. – P. 79 – 117.
9. *Gowers W. T.* A new proof of Szemerédi's theorem for arithmetic progressions of length four // Geom. Funct. Anal. – 1998. – **8**. – P. 529 – 551.
10. *Gowers W. T.* A new proof of Szemerédi's theorem // Ibid. – 2001. – **11**. – P. 465 – 588.
11. *Lev V. F.* Progressions-free sets in finite abelian groups // J. Number Theory. – 2004. – **104**, № 1. – P. 162 – 169.
12. *Meshulam R.* On subsets of finite abelian groups with no 3-term arithmetic progressions // J. Combin. Theory. – 1995. – **71**, Ser. A. – P. 168 – 172.
13. *Nathanson M.* Additive number theory. Inverse problems and the geometry of sumsets // Grad. Texts Math. – 1996. – **165**.
14. *Rankin R. A.* Sets of integers containing not more than a given number of terms in arithmetic progression // Proc. Roy. Soc. Edinburgh A. – 1961. – **65**, № 4. – P. 332 – 344.
15. *Roth K. F.* On certain sets of integers // J. London Math. Soc. – 1953. – **28**. – P. 245 – 252.
16. *Chang M.-C.* A polynomial bound in Freiman's theorem // Duke Math. J. – 2002. – **113**, № 3. – P. 399 – 419.
17. *Bernstein S.* Sur une modification de l'inéqualité de Tchebichef // Ann. Sci. Inst. Sav. Ukr. Sect. Math. I. – 1924.
18. *Spencer J.* Six standard deviations suffice // Trans. Amer. Math. Soc. – 1985. – **289**. – P. 679 – 706.
19. *Green B.* Arithmetic progressions in sumsets // Geom. Funct. Anal. – 2002. – **12**, № 3. – P. 584 – 597.
20. *Green B.* A Szemerédi-type regularity lemma in abelian groups // Ibid. – 2005. – **15**, № 2. – P. 340 – 376.
21. *Green B.* Some constructions in the inverse spectral theory of cyclic groups // Combin. Probab. Comput. – 2003. – **12**, № 2. – P. 127 – 138.
22. *Green B.* Spectral structure of sets of integers // Fourier Analysis and Convexity (Survey Article, Milan 2001). Appl. Numer. Harmon. Anal. – Boston, MA: Birkhäuser, 2004. – P. 83 – 96.
23. *Green B.* Structure theory of set addition // ICMS Instruct. Conf. Comb. Aspects Math. Anal. (Edinburgh, March 25 – April 5, 2002). – P. 1 – 27.

24. *Green B.* Finite field model in additive combinatorics // Surv. Combinatorics. LMS Lect. Notes. – 2005. – **329**. – P. 1 – 29.
25. *Green B., Tao T.* An inverse theorem for the Gowers U^3-norm, with applications // Proc. Edinburgh Math. Soc. Ser. 2. – 2008. – **51**, № 1. – P. 73 – 153.
26. *Green B., Tao T.* New bounds for Szemerédi's theorem, II: A new bound for $r_4(N)$ // Anal. Number Theory. – Cambridge: Cambridge Univ. Press, 2009. – P. 180 – 204.
27. *Rudin W.* Fourier analysis on groups. – Wiley, 1990 (репринт издания 1962 года).
28. *Rudin W.* Trigonometric series with gaps // J. Math. and Mech. – 1960. – **9**. – P. 203 – 227.
29. *Ruzsa I.* Arithmetic progressions in sumsets // Acta Arithm. – 1991. – **60**, № 2. – P. 191 – 202.
30. *Sanders T.* Appendix to 'Roth's theorem on progressions revisited' by J. Bourgain // J. Anal. Math. – 2008. – **104**, № 1. – P. 193 – 206.
31. *Szemerédi E.* On sets of integers containing no k elements in arithmetic progression // Acta Arithm. – 1975. – **27**. – P. 299 – 345.
32. *Tao T., Vu V.* Additive combinatorics. – Cambridge Univ. Press, 2006.
33. *Tao T.* Lecture notes 5 for Math 254A // UCLA 2003, available at http://math.ucla.edu/ tao/254a.1.03w/notes5.dvi
34. *Bourgain J.* On triples in arithmetic progression // Geom. Funct. Anal. – 1999. – **9**. – P. 968 – 984.
35. *Bourgain J.* Roth's theorem on progressions revisited. – Preprint, 2007.
36. *Spencer J.* Six standard deviations suffice // Trans. Amer. Math. Soc. – 1985. – **289**. – P. 679 – 706.
37. *Szegö G.* Orthogonal polynomials. – New York: Amer. Math. Soc., 1939.
38. *Rivlin T. J.* Chebyshev polynomials // Approxim. Theory Algebra and Number Theory. – New York: John Wiley and Sons, 1990. – 249 p.
39. *Turan P.* Eine Extremalaufgabe aus der Graphentheorie // Mat. Fiz. Lapok. – 1941. – **48**. – P. 436 – 452.
40. *Bollobás B.* Ket fuggelten kort nem tartalmazo grafokrol // Mat. Lapok. – 1963. – **14**. – P. 311 – 321.
41. *Bollobás B.* Extremal graph theory. – New York: Acad. Press, 1978.
42. *Dutton R. D., Brigham R. C.* Edges in graphs with large girth // Graphs and Combinatorics. – 1991. – **7**. – P. 315 – 321.
43. *Шкредов И. Д.* О множествах больших тригонометрических сумм // Докл. АН СССР. – 2006. – **411**, № 4. – С. 455 – 459.
44. *Шкредов И. Д.* О множествах больших тригонометрических сумм // Изв. РАН. Сер. мат. – 2008. – **72**, № 1. – С. 161 – 182.
45. *Шкредов И. Д.* Некоторые примеры множеств больших тригонометрических сумм // Мат. сб. – 2007. – **198**, № 12. – С. 105 – 140.
46. *Shkredov I. D.* On sumsets of dissociated sets // Online J. Anal. Combinatorics. – 2009. – **4**. – P. 1 – 27.

Получено 29.12.09