Конспект спецкурса по аддитивной комбинаторике

Д. М. Столяров[1]

осень 2018 и весна 2022 года

[1]Автор признателен студентам, особенно Дмитрию Крачуну, Святославу Новикову и Ольге Мартыновой, за многочисленные исправления.

Оглавление

Глава 1

Множества с малым удвоением

3.9.2018

Пусть Z — некоторая коммутативная группа, A — её конечное подмножество. Рассмотрим сумму

$$A + A = \{a_1 + a_2 \mid a_1, a_2 \in A\}.$$

Насколько велико или мало может быть множество $A + A$? Например, пусть Z — группа целых чисел $\mathbb{Z}$. Если A — отрезок арифметической прогрессии, то $|A + A| = 2|A| - 1$. Если же A — отрезок геометрической прогрессии, то $|A+A| = \frac{|A|(|A|+1)}{2}$. Можно предположить, что если множество $A+A$ не очень велико по сравнению с A, то множество A обладает богатой арифметической структурой. Теорема Фреймана позволяет точно выразить этот эвристический принцип. Для того, чтобы её сформулировать, нам понадобится обобщить понятие арифметической прогрессии.

Определение 1.0.1. Пусть $g_1, g_2, \dots, g_k$ — элементы группы Z, пусть $I_1, I_2, \dots, I_k$ — отрезки целых чисел. Множество

$$P = \Big\{ \sum_{j=1}^{k} a_j g_j \;\Big|\; \forall j \quad a_j \in I_j \Big\} \tag{1.0.1}$$

называется обобщённой арифметической прогрессией. Наименьшее число k, для которого возможно представление множества P в виде (1.0.1), называется размерностью обобщённой арифметической прогрессии P.

Теорема 1.0.2 (Теорема Фреймана)**.** *Для всякого числа $C > 1$ существуют константы $d(C)$ и $s(C)$, обладающие следующимим свойствами. Для всякого множества $A \subset \mathbb{Z}$, такого что*

$$|A + A| \leqslant C|A|, \tag{1.0.2}$$

существует объемлюшая обобщённая арифметическая прогрессия P размерности не более $d(C)$ и мощности не более $s(C)|A|$.

Множества, удовлетворяющие неравенству (1.0.2), назовём множествами с малым удвоением (здесь надо представлять, что множество A огромно, а константа C сравнительно невелика). Лучшую константу C в неравенстве (1.0.2) назовём константой удвоения множества A. Нетрудно видеть, что обобщённая арифметическая прогрессия P размерности не более α обладает константой удвоения, не большей, чем 2^α.

1.1 «Элементарные» неравенства

Материалы данной главы основываются на второй главе книги [16], конспекте [6], статье [12] и книге [5].

Определение 1.1.1. Пусть A и B — конечные подмножества группы Z. Определим их сумму

$$A+B=\{a+b \mid a\in A, b\in B\}.$$

Также будем писать nA, $n\in\mathbb{N}$, для обозначения n-кратной суммы множества A с самим собой и $-A$ для множества $\{-a \mid a\in A\}$. Таким образом,

$$mB-nB=\Big\{\sum_{i=1}^{m} b_i-\sum_{i=m+1}^{m+n} b_i \;\Big|\; \forall i \quad b_i\in B\Big\}.$$

Нетрудно доказать неравенства

$$\max(|A|,|B|)\leqslant |A+B|\leqslant |A||B|. \tag{1.1.1}$$

Упражнение 1.1.1. *Пусть $Z=\mathbb{Z}$. Докажите неравенство $|A+B|\geqslant |A|+|B|-1$.*

Задача 1.1.2 (Теорема Коши–Давенпорта)**.** *Пусть $Z=\mathbb{Z}_p$ — циклическая группа порядка p, число p простое. Докажите неравенство $|A+B|\geqslant \min(p,|A|+|B|-1)$.*

Изучим случаи равенства в оценке (1.1.1) снизу мощности множества $A+B$.

Лемма 1.1.2. *Следующие пять утверждений равносильны.*

1. $|A+B|=|A|$.
2. $|A-B|=|A|$.
3. $|A+mB-nB|=|A|$ *для некоторой пары* $(m,n)\in\mathbb{Z}^2\setminus\{(0,0)\}$.
4. $|A+mB-nB|=|A|$ *для всех пар* $(m,n)\in\mathbb{Z}^2$.
5. *Существует конечная подгруппа $G\subset Z$, такая что множество A есть объединение её классов смежности, а множество B принадлежит одному классу смежности группы G.*

Доказательство. Отметим, что заменяя множество B его сдвигом $B+\{-b\}$ (здесь $b\in B$ — некоторый элемент), мы не изменим мощности множеств $A+mB-nB$ (каждое такое множество просто сдвинется на $(m-n)b$); также не поменяется выполнимость пятого условия. Поэтому, не умаляя общности, можем считать $0\in B$.

Импликации $5\to 4$ и $4\to 3$ очевидны. Кроме того, очевидны импликации $4\to 2$ и $4\to 1$.

Докажем, что либо $3\to 2$, либо $3\to 1$. Действительно, так как мы предположили $0\in B$, выполнено либо включение $B\subset mB-nB$, либо включение $-B\subset mB-nB$. Поэтому либо $|A+B|\leqslant |A|$, либо $|A-B|\leqslant |A|$. Благодаря неравенству (1.1.1), эти неравенства обязаны обращаться в равенство.

Осталось доказать импликацию $1\to 5$, потому что импликации $2\to 5$ есть ничто иное, как $1\to 5$ для множеств A и $-B$. Итак, предположим, что $|A+B|=|A|$. Так как $0\in B$, имеем $A\subset A+B$, и стало быть, $A+B=A$. Определим группу G:

$$G=\{g\in Z \mid g+A=A\}.$$

Мы показали, что $B\subset G$. Осталось доказать, что A есть объединение классов смежности G (отсюда также будет следовать конечность группы G). Но это очевидным образом следует из определения G. □

Так как мы хотим описывать множества с малым удвоением, желательно получить более гибкий аналог этой леммы, в котором равенства будут заменены на приблизительные равенства. Чтобы мерить малость отклонения, полезно определить подходящую метрику. Определим *дистанцию Ружи.*

Определение 1.1.3. Величина $d(A,B) = \log \frac{|A-B|}{|A|^{\frac{1}{2}}|B|^{\frac{1}{2}}}$ называется дистанцией Ружи между непустыми конечными множествами A и B.

Неравенство (1.1.1) влечёт $d(A,B) \geqslant 0$, однако довольно часто $d(A,A) > 0$. Поэтому дистанция Ружи — не метрика. Тем не менее, неравенство треугольника для неё выполнено.

Лемма 1.1.4 (Неравенство треугольника Ружи)**.** *Для всех непустых конечных множеств A, B и C выполнено неравенство $d(A,C) \leqslant d(A,B) + d(B,C)$.*

Доказательство. Доказываемое неравенство может быть переписано в виде

$$|B||A-C| \leqslant |A-B||B-C|. \tag{1.1.2}$$

Рассмотрим отображение $\Pi\colon (A-B)\times(B-C) \to Z$, которое есть просто сложение координат: $\Pi(x,y) = x+y$. Достаточно показать, что всякий элемент множества $A-C$ накрывается отображением Π хотя бы $|B|$ раз. Рассмотрим произвольный элемент $z \in A-C$ и зафиксируем его представление в виде $z = a-c$, где $a \in A$ и $c \in C$. Каждому элементу $b \in B$ тогда можно сопоставить пару $(x,y) = (a-b, b-c)$. Нетрудно видеть, что все такие пары (x,y) различны и $\Pi(x,y) = z$. $\square$

Замечание 1.1.5. *Хоть дистанция Ружи и не метрика, её сужение на множество всех конечных подгрупп Z является метрикой.*

Вопрос 1.1.3. *Какие непрерывные аналоги дистанции Ружи можно предложить? Скажем, нельзя ли ввести подобную дистанцию на открытых подмножествах прямой?*

Определение 1.1.6. Пусть A — конечное непустое множество. Величина $\sigma[A]$, заданная по правилу

$$\sigma[A] = \frac{|A+A|}{|A|},$$

называется константой удвоения множества A. Величина $\delta[A]$, заданная по правилу

$$\delta[A] = \frac{|A-A|}{|A|},$$

называется константой разности множества A.

Нетрудно видеть, что обе определённые константы могут лежать в пределах от единицы до $\frac{1}{2}|A|$. Множествам с малым удвоением соответствуют малые значения $\sigma[A]$. Опишем случаи равенства этих констант единице.

Лемма 1.1.7. *Следующие шесть утверждений равносильны.*

1. $\sigma[A] = 1$.
2. $\delta[A] = 1$.
3. *Существует непустое конечное множество B, такое что $d(A,B) = 0$.*
4. $|mA - nA| = |A|$ *для некоторой пары* $(m,n) \in \mathbb{Z}^2 \setminus \{(0,0),(\pm 1,0),(0,\pm 1)\}$.
5. $|mA - nA| = |A|$ *для всех пар* $(m,n) \in \mathbb{Z}^2 \setminus \{(0,0)\}$.
6. *Множество A есть класс смежности конечной подгруппы группы Z.*

Доказательство. Импликации $6 \to 5 \to 4$ очевидны. Докажем $4 \to 3$. Не умаляя общности, можно считать, что $m > 0$. Положим $B = (m-1)A - nA$. Согласно нашим предположениям о паре (m, n), множество B непусто. Кроме того, $|A| \leqslant |B|$ и $|B| \leqslant |mA - nA|$ (по неравенству (1.1.1)), поэтому $|B| = |A|$. Стало быть,

$$e^{d(A,B)} = \frac{|mA - nA|}{\sqrt{|A||B|}} = 1.$$

Импликация $3 \to 2$ следует из неравенства треугольника Ружи:

$$\delta[A] = e^{d(A,A)} \leqslant e^{2d(A,B)} = 1.$$

Импликация $2 \to 1$ следует из равносильности первого и второго утверждений леммы 1.1.2. Завершающая круг импликация $1 \to 6$ следует из равносильности второго и пятого утверждений леммы 1.1.2. □

Константы разности и удвоения могут быть равны единице лишь одновременно. Нельзя ли выразить этот факт в виде неравенства? Одно такое неравенство легко следует из неравенства треугольника.

Следствие 1.1.8. *Для всякого конечного множества A имеет место неравенство $\delta[A] \leqslant \sigma^2[A]$.*

Доказательство.

$$\delta[A] = e^{d(A,A)} \leqslant e^{2d(A,-A)} = \sigma^2[A].$$

□

Упражнение 1.1.4. *Рассмотрите множество $A = \{x \in \mathbb{Z}^d \mid \sum_i x_i \leqslant n, \forall i \quad x_i \geqslant 0\}$, вычислите его константу удвоения и константу разности. После чего, подбирая параметры d и n докажите точность по порядку только что доказанного неравенства. А именно, покажите, что ни для какого числа $\varepsilon \in (0, 2)$ не существует константы C_ε, такой что для всякого конечного множества A выполнено неравенство $\delta[A] \leqslant C_\varepsilon \sigma^{2-\varepsilon}[A]$.*

Обратное неравенство $\sigma[A] \leqslant \delta^2[A]$ сложнее и опирается на следующую теорему.

Теорема 1.1.9 (Неравенство Плюннеке)**.** *Пусть A и B — конечные непустые множества, пусть $|A+B| \leqslant K|A|$. Существует непустое подмножество X множества A, такое что для всякого натурального числа n выполнено неравенство $|X + nB| \leqslant K^n|X|$.*

Ненадолго отложим доказательство неравенства Плюннеке. Пока что получим его полезные следствия.

Следствие 1.1.10 (Неравенства Плюннеке–Ружи)**.** *Пусть конечные непустые множества A и B удовлетворяют неравенству $|A + B| \leqslant K|A|$. Тогда $|mB - nB| \leqslant K^{m+n}|A|$.*

Доказательство. Выберем множество X, описанное в теореме 1.1.9 и воспользуемся неравенством треугольника Ружи в форме (1.1.2) (положим $A := mB, C := nB$ и $B := -X$):

$$|-X||mB - nB| \leqslant |mB + X||-X - nB| \leqslant K^{m+n}|X|^2.$$

Сократив на $|X| = |-X|$, получим оценку $|mB - nB| \leqslant K^{m+n}|X|$, что точно не слабее требуемого, так как X — подмножество A. □

Следствие 1.1.11. *Для всякого конечного множества A имеет место неравенство $\sigma[A] \leqslant \delta^2[A]$.*

Доказательство. Подставим $B := -A$, $K = \delta[A]$ в следствие 1.1.10 и выберем $m = 0$ и $n = 2$. □

Упражнение 1.1.5. *Докажите, что существует константа $\varepsilon_0 > 0$, такая что не существует константы C_{ε_0}, такой что для всякого конечного множества A имеет место неравенство $\sigma[A] \leqslant C_{\varepsilon_0}\delta^{1+\varepsilon_0}[A]$.*

10.9.2018

Приступим к доказательству теоремы 1.1.9. Классическое доказательство неравенства Плюннеке весьма изощрённо и опирается на теорию графов, в частности, на теорему Менгера о структуре k-связного графа. С классическим доказательством можно ознакомиться, например, в шестой главе книги [16]. В 2011 году Петридис [12] предложил более короткое доказательство. Оно основывается на следующей замечательной лемме.

Лемма 1.1.12 (Лемма Петридиса)**.** *Пусть A и B — конечные непустые множества, такие что $|A+B| \leqslant C|A|$. Пусть множество A минимально в том смысле, что для всякого множества $T \subsetneq A$ имеет место обратное неравенство $|T+B| \geqslant C|T|$. Тогда $|A+B+S| \leqslant C|A+S|$ для всякого конечного множества $S \subset Z$.*

Доказательство. Будем вести индукцию по мощности множества S. База, когда S состоит из одного элемента, очевидна: от сдвига мощности множеств не меняются. Чтобы осуществить переход, отщепим от множества S один элемент: $S = S' \cup \{x\}$. Запишем мощности оцениваемого и оценивающего множеств при помощи формул де Моргана:

$$|A+S| = |(A+S') \cup (A+\{x\})| = |A+S'| + |A| - |(A+S') \cap (A+\{x\})|;$$
$$|A+B+S| = |(A+B+S') \cup (A+B+\{x\})| = |A+B+S'| + |A+B| - |(A+B+S') \cap (A+B+\{x\})|.$$

Эти формулы показывают, что для доказательства желаемого неравенства $|A+B+S| \leqslant C|A+B|$ достаточно проверить три оценки:

$$|A+B+S'| \leqslant C|A+S'|; \tag{1.1.3}$$
$$|A+B| \leqslant C|A|; \tag{1.1.4}$$
$$|(A+B+S') \cap (A+B+\{x\})| \geqslant C|(A+S') \cap (A+\{x\})|. \tag{1.1.5}$$

Неравенство (1.1.3) есть просто предположение индукции для множества S' (мощность S' меньше мощности S). Неравенство (1.1.4) верно по условию леммы. Последнее неравенство (1.1.5) доказать труднее. Давайте перепишем его, сдвинув оба множества на x:

$$|(A+B+S'-\{x\}) \cap (A+B)| \geqslant C|(A+S'-\{x\}) \cap A|.$$

Обозначим множество $(A+S'-\{x\}) \cap A$ символом T. Очевидно, что $T \subset A$, поэтому к множеству T хочется применить предположение о минимальности A. Рассмотрим два случая.

Случай $T = A$. В этом случае, $A+S'-\{x\} \supset A$. Следовательно, $A+S' \supset A+\{x\}$ и $A+S = A+S'$. Отсюда также следует, что $A+B+S = A+B+S'$. Поэтому, доказываемое неравенство $|A+B+S| \leqslant C|A+S|$ следует из предположения индукции $|A+B+S'| \leqslant C|A+S'|$. В этом случае мы не пользуемся рассуждениями с формулами де Моргана, приведёнными выше.

Случай $T \subsetneq A$. В этом случае мы можем воспользоваться предположением о минимальности A, а именно, неравенством $|T+B| \geqslant C|T|$, которое расшифровывается как

$$\Big|\big((A+S'-\{x\}) \cap A\big) + B\Big| \geqslant C|(A+S'-\{x\}) \cap A|. \tag{1.1.6}$$

Отметим очевидное вложение

$$X \cap Y + B \subset (X+B) \cap (Y+B),$$

которое при подстановке $X := A + S' - \{x\}$ и $Y := A$ влечёт

$$\Big|\big((A + S' - \{x\}) \cap A\big) + B\Big| \leqslant \Big|(A + S' - \{x\} + B) \cap (A + B)\Big|. \tag{1.1.7}$$

Соберём все неравенства вместе:

$$C|(A + S') \cap (A + \{x\})| = C|(A + S' - \{x\}) \cap A| \overset{(1.1.6)}{\leqslant} \Big|\big((A + S' - \{x\}) \cap A\big) + B\Big| \overset{(1.1.7)}{\leqslant}$$
$$\Big|(A + S' - \{x\} + B) \cap (A + B)\Big| = |(A + B + S') \cap (A + B + \{x\})|.$$

Неравенство (1.1.5) доказано, а с ним и лемма. □

Доказательство теоремы 1.1.9. Рассмотрим подмножество X множества A, для которого величина

$$c_X = \frac{|X + B|}{|X|}$$

минимальна среди всех подмножеств множества A. Покажем, что множество X удовлетворяет условиям леммы 1.1.12 в качестве множества A (с константой $C := c_X$). Достаточно проверить лишь минимальность в терминах леммы 1.1.12 множества X. Пусть Y — подмножество X, тогда

$$|Y + B| = c_Y|Y| \geqslant c_X|Y|,$$

что и влечёт минимальность X. Применим лемму 1.1.12 и положим $S = (n-1)B$:

$$|X + nB| = |X + B + S| \leqslant c_X|X + S| = c_X|X + (n-1)B|.$$

Это неравенство можно проитерировать (то есть, последовательно применить лемму Петридиса с $S = (n-2)B$, $S = (n-3)B$ и т.д.) и получить

$$|X + nB| \leqslant c_X^n|X|.$$

Осталось лишь заметить, что $c_X \leqslant K$. □

Упражнение 1.1.6. *Докажите неравенства*

$$|A - A|^{\frac{2}{3}} \leqslant |A + A| \leqslant |A - A|^{\frac{3}{2}}.$$

Как справитесь, докажите неравенства Пигаева–Фреймана

$$|A - A|^{\frac{3}{4}} \leqslant |A + A| \leqslant |A - A|^{\frac{4}{3}}.$$

Замечание 1.1.13. *Неравенство Плюннеке 1.1.9 утверждает, что величина $\frac{|A+B|}{|A|}$ в некотором смысле контролирует величины $\frac{|X+nB|}{|X|}$ для некоторого подмножества $X \subset A$ и всех натуральных чисел n. Естественный вопрос: а нельзя ли получить контроль за подобными выражениями в случае $n \leqslant 0$? Например, не существует ли константы C', зависящей только от C, такой что для всяких множеств A и B, таких что $|A + B| \leqslant C|A|$, существует множество $X \subset A$, удовлетворяющее неравенству $|X - B| \leqslant C'|X|$? Оказывается, что ответ на этот вопрос отрицательный, см. работу* [10].

Неравенство Плюннеке и оценки Плюннеке–Ружи позволят получить более гибкую версию леммы 1.1.7. Чтобы сформулировать её, нам понадобится понятие приблизительной подгруппы.

Определение 1.1.14. Пусть $K \geqslant 1$. Множество $H \subset Z$ называется K-приблизительной подгруппой, если оно симметрично (то есть, $H = -H$) и множество $H + H$ может быть накрыто не более чем $[K]$ сдвигами множества H.

Замечание 1.1.15. *В случае $K = 1$ множество H будет классом смежности. Отметим, что если H — класс смежности, то множество $H - H$ является 1-приблизительной подгруппой.*

Лемма 1.1.16. *Следующие утверждение эквивалентны.*

1. $\sigma[A] \leqslant K^{C_1}$.
2. $\delta[A] \leqslant K^{C_2}$.
3. *Существует множество B, такое что $d(A, B) \leqslant C_3 \log K$.*
4. *Существует константа C_4, такая что неравенство $|mA - nA| \leqslant K^{C_4(|m|+|n|)}|A|$ справедливо для всех пар $(m, n) \in \mathbb{Z}^2$.*
5. *Существует K^{C_5}-приблизительная подгруппа H, такая что $A \subset x + H$ для некоторого элемента x и $|H| \leqslant K^{C_5}|A|$.*

Утверждение леммы следует понимать так: если предположить выполнение утверждения пункта i с константой C_i, то утверждение пункта j выполнено с константой C_j, которая зависит лишь от C_i (например, можно взять $C_j = 239C_i$).

Эквивалентность первых четырёх пунктов есть простое следствие неравенства треугольника и неравенства Плюннеке. Чтобы работать с пятым утверждением, нам понадобится лемма Ружи о покрытии.

Определение 1.1.17. Множества A и B назовём аддитивно независимыми, если $|A + B| = |A||B|$.

Иными словами, множества A и B независимы, если уравнение

$$a_1 + b_1 = a_2 + b_2, \quad a_1, a_2 \in A,\ b_1, b_2 \in B,$$

имеет лишь тривиальные решения $a_1 = a_2$ и $b_1 = b_2$, см. неравенство (1.1.1). Понятие аддитивной независимости родственно понятию независимых множеств в теории графов.

Лемма 1.1.18 (Лемма Ружи о покрытии)**.** *Для всяких конечных непустых множеств A и B существует множество $X \subset B$, аддитивно независимое с множеством A, такое что $B \subset A - A + X$.*

Доказательство. Пусть X — наибольшее подмножество B, независимое с множеством A. Покажем, что $B \subset A - A + X$. Предположим противное, пусть $b \in B$ не принадлежит множеству $A - A + X$, иными словами, уравнение

$$b = a_1 - a_2 + x, \quad a_1, a_2 \in A,\ x \in X,$$

не имеет решений. Но это значит, что уравнение $b + a_2 = a_1 + x$ не имеет решений, и из этого следует, что множество $X' = X \cup \{b\}$ независимо с множеством A, что противоречит максимальности множества X. □

Ценность леммы Ружи в том, что если величина $\frac{|A+B|}{|A|}$ невелика, то мощность множества X тоже. Если $|A + B| \leqslant C|A|$, то

$$|X| = \frac{|A + X|}{|A|} \leqslant \frac{|A + B|}{|A|} \leqslant C.$$

Следствие 1.1.19. *Пусть A и B — конечные множества, такие что $|A+B| \leqslant C|A|$. Множество B можно покрыть не более чем C сдвигами множества $A-A$.*

Отметим, что множество $A-A$ можно рассматривать как "сглаживание" множества A. В некотором смысле, вычитание множества из самого себя "замазывает в нём дыры". Иллюстрацией этого принципа служит хорошо известный факт теории меры: если лебегова мера измеримого множества A на прямой положительна, то множество $A-A$ содержит отрезок.

Доказательство леммы 1.1.16. Доказательства импликаций $4 \to 3$, $3 \to 2$ и $2 \to 1$ полностью повторяют доказательства соответствующих импликаций леммы 1.1.7. Импликация $1 \to 4$ легко выводится из следствия 1.1.10.

Докажем $5 \to 1$:

$$|A+A| \leqslant |H+H| \leqslant K^{C_5}|H| \leqslant K^{2C_5}|A|$$

по определению K^{C_5}-приблизительной подгруппы.

Осталось доказать импликацию $1 \to 5$. Положим $H = A-A$. Очевидно, что это множество симметрично и содержит сдвиг множества A. Кроме того, из эквивалентности первого и второго пунктов настоящей леммы следует, что $|H| \leqslant K^{C_2}|A|$, здесь можно выбрать $C_2 = 2C_1$. Осталось показать, что множество $H+H = 2A-2A$ можно покрыть не более чем K^{C_5} сдвигами множества $H = A-A$. Применим следствие 1.1.19, подставив в него $A := A$, $B := 2A-2A$. Следствие утверждает, что $B = H+H$ можно покрыть C сдвигами множества $A-A = H$, где $C = \frac{|A+2A-2A|}{|A|}$. Константу C нетрудно оценить, пользуясь следствием 1.1.10:

$$C = \frac{|3A-2A|}{|A|} \leqslant K^{5C_1}.$$

Таким образом, мы доказали, что $H = A-A$ есть K^{5C_1}-приблизительная подгруппа. □

17.9.2018

1.2 Обзор доказательства теоремы Фреймана

Напомним читателю классическую формулировку теоремы Фреймана.

Теорема 1.2.1 (Теорема Фреймана, 59–64)**.** *Для всякого числа $C > 1$ существуют константы $d(C)$ и $s(C)$, обладающие следующими свойствами. Для всякого множества $A \subset \mathbb{Z}$, такого что $\sigma[A] \leqslant C$, существует объемлющая обобщённая арифметическая прогрессия P размерности не более $d(C)$ и мощности не более $s(C)|A|$.*

С классическим доказательством теоремы Фреймана можно ознакомиться в его книге [4].

В начале 90-х Ружа предложил доказательство, дающее оценки $d(C) \lesssim C^4$ и $s(C) \lesssim e^{e^C}$ (символ $\lesssim$ означает, что неравенство верно с точностью до мультипликативной константы). В 2002 году Чанг [2] улучшила его метод. Последнее доказательство мы и изложим. Отметим, что, по-видимому, эти оценки не оптимальны по порядку. Кроме того, аналог теоремы Фреймана верен и для случая произвольной объемлющей группы. А именно, Грин и Ружа в 2007 году доказали следующую теорему.

Теорема 1.2.2 (Теорема Грина–Ружи, 2007)**.** *Для всякого числа $C > 1$ существуют константы $d(C)$ и $s(C)$, обладающие следующимим свойствами. Пусть $A \subset Z$ — конечное подмножество произвольной группы, такое что $\sigma[A] \leqslant C$. Тогда существует обобщённая арифметическая прогрессия P размерности не более $d(C)$ и конечная подгруппа H, такие что $A \subset P+H$ и $|P+H| \leqslant s(C)|A|$.*

Упражнение 1.2.1. *Пусть A и B — конечные непустые подмножества $\mathbb{Z}$, каждое из них содержит хотя бы два числа. Докажите, что если в неравенстве упражнения 1.1.1 достигается равенство, то A и B суть отрезки арифметических прогрессий с одинаковым шагом.*

Задача 1.2.2. *Пусть $A \subset \mathbb{Z}$ таково, что $|2A| \leqslant 3|A| - 3$. Докажите, что множество A содержится в отрезке арифметической прогрессии длины не более $|2A| - |A| + 1$.*

Доказательство теоремы Фреймана в форме Чанг разбивается на три части: первая основывается на анализе Фурье, вторая на комбинаторной геометрии решёток и выпуклых тел, третья комбинаторна. Кратко опишем содержание этих частей.

Определение 1.2.3. Обобщённая арифметическая прогрессия P называется правильной, если все суммы $\sum_j a_j g_j$ различны (см. определение 1.0.1).

Первая и вторая часть доказательства теоремы Фреймана показывают, что если подмножество A циклической группы $\mathbb{Z}_N$ (число N будем считать простым) имеет малое удвоение, то множество $2A - 2A$ содержит большую правильную арифметическую прогрессию P. Таким образом, задачами третьей части доказательства являются: а) переход от группы $\mathbb{Z}_N$ к группе $\mathbb{Z}$, б) покрытие множества A небольшим числом сдвигов прогрессии P. Пункт а) будет несложно получить, введя понятие *гомоморфизма Фреймана*. Пункт б) напоминает следствие 1.1.19, и по сути, будет его обобщением (лемму Ружи о покрытии мы заменим леммой Чанг о покрытии, которая предназначена для работы с арифметическими прогрессиями).

Поиск правильной прогрессии P в множестве $2A - 2A$ разбивается на две части: сначала мы найдём в множестве $2A - 2A$ большую окрестность Бора, а потом уже в ней — правильную арифметическую прогрессию.

Определение 1.2.4. Пусть $R \subset \mathbb{Z}_N$ и $\delta > 0$. Определим окрестность Бора $B(R, \delta)$ множества R по формуле

$$B(R,\delta) = \Big\{ x \in \mathbb{Z}_N \;\Big|\; \forall \xi \in R \quad \operatorname{dist}\Big(\frac{x\xi}{N}, \mathbb{Z}\Big) < \delta \Big\}.$$

Как обычно, вычет $x\xi$ мы интерпретируем как целое число отрезка $[0, \dots, N-1]$. Напомним, что число N мы считаем простым.

Про окрестность Бора можно думать двумя способами. С одной стороны, если множество R состоит из одной точки, а число δ достаточно мало, то множество R напоминает арифметическую прогрессию. С другой стороны, окрестность Бора можно интерпретировать как "поляру" множества R.

Первая часть состоит в доказательстве следующей теоремы.

Теорема 1.2.5. *Пусть $|A| = \alpha N$ и $\sigma[A] \leqslant C$. Существует множество $K \subset \mathbb{Z}_N$ и число $\delta > 0$, такие что $|K| \leqslant 8C|\log \alpha|$, $\delta \geqslant \frac{1}{160C|\log \alpha|}$ и $B(K, \delta) \subset 2A - 2A$.*

Вторая же часть состоит в доказательстве следующей теоремы.

Теорема 1.2.6. *Пусть $R \subset \mathbb{Z}_N$ и $\delta \in (0, \frac{1}{2})$. Тогда множество $B(R, \delta)$ содержит правильную арифметическую прогрессию размерности $|R|$ и мощности хотя бы $(\frac{\delta}{|R|})^{|R|} N$.*

1.3 Доказательство теоремы 1.2.5: анализ Фурье

Определение 1.3.1. Пусть A и B — конечные непустые подмножества группы Z. Определим их аддитивную энергию $E(A, B)$ согласно формуле

$$E(A,B) = \Big| \Big\{ (a_1, a_2, b_1, b_2) \in A \times A \times B \times B \;\Big|\; a_1 + b_1 = a_2 + b_2 \Big\} \Big|. \tag{1.3.1}$$

Упражнение 1.3.1. *Докажите неравенство*

$$E(A,B)^2 \leqslant E(A,A)E(B,B).$$

Аддитивная энергия двух множеств достигает наименьшего возможного значения $|A||B|$, если множества A и B аддитивно независимы и тем больше, чем "лучше складываются" множества A и B.

Лемма 1.3.2. *Аддитивная энергия удовлетворяет неравенству*

$$E(A,B) \geqslant \frac{|A|^2|B|^2}{|A+B|}.$$

Доказательство. Формулу (1.3.1) можно записать чуть иначе:

$$E(A,B) = \sum_{x\in A+B} \Big|\Big\{(a,b)\in A\times B \;\Big|\; a+b=x\Big\}\Big|^2. \tag{1.3.2}$$

Воспользуемся неравенством Коши–Буняковского–Шварца:

$$E(A,B)|A+B| = \Big(\sum_{x\in A+B} \Big|\Big\{(a,b)\in A\times B \;\Big|\; a+b=x\Big\}\Big|^2\Big)\Big(\sum_{x\in A+B} 1^2\Big) \geqslant$$
$$\Big(\sum_{x\in A+B} \Big|\Big\{(a,b)\in A\times B \;\Big|\; a+b=x\Big\}\Big|\Big)^2 = |A|^2|B|^2.$$

□

Эвристический принцип: преобразование Фурье характеристической функции множества с малым удвоением хорошо сконцентрировано. Точное выражение этого принципа, используемое в доказательстве теоремы Фреймана, содержится в лемме 1.3.3 ниже. Сейчас мы разберём пример. Пусть A — отрезок арифметической прогрессии:

$$A = \{j\nu \subset \mathbb{Z}_N \mid j\in[a..b]\}, \quad \nu\in\mathbb{Z}_N\setminus\{0\}.$$

Предположим, что мощность множества A сравнима с числом N (скажем, $|A| = \alpha N$, где число $\alpha < \frac{1}{2}$, но например, $\alpha > N^{-\varepsilon}$). Как мы знаем, отрезок арифметической прогрессии — множество с очень малым удвоением. Вычислим соответствующее преобразование Фурье, сложив сумму геометрической прогрессии:

$$\hat{\chi}_A(\xi) = \sum_{j\in[a,b]} e^{2\pi i\frac{j\nu\xi}{N}} = e^{2\pi i\frac{a\nu\xi}{N}}\frac{1-e^{2\pi i\frac{(b-a+1)\nu\xi}{N}}}{1-e^{\frac{2\pi i\nu\xi}{N}}}.$$

Рассмотрим множество $B = \Big\{\xi \;\Big|\; \operatorname{dist}\Big(\frac{\nu\xi}{N},\mathbb{Z}\Big)\leqslant\frac{1}{2|A|}\Big\}$ и отметим, что так как $b-a+1=|A|$, при $\xi\in B$ верны неравенства

$$\big|1-e^{2\pi i\frac{(b-a+1)\nu\xi}{N}}\big| \geqslant \frac{|A|\nu\xi}{2N};$$
$$\big|1-e^{2\pi i\frac{\nu\xi}{N}}\big| \leqslant \frac{2\nu\xi}{N}.$$

Стало быть,

$$|\hat{\chi}_A(\xi)| \geqslant \frac{|A|}{4}, \quad \xi\in B.$$

Отметим, что в множестве B лежит примерно $\frac{N}{2|A|}$ точек (это можно понять наглядно, изобразив $\mathbb{Z}_N$ как множество комплексных корней из единицы N-ой степени — тогда множество B будет объединением "отрезков окружности", в каждом из которых лежит примерно $\frac{N}{2\nu|A|}$ точек, а всего отрезков ν). Отметим, что по теореме Планшереля,

$$\sum_{\xi\in\mathbb{Z}_N}|\hat{\chi}_A(\xi)|^2 = N|A|.$$

С другой стороны, мы показали, что

$$\sum_{\xi\in B}|\hat{\chi}_A(\xi)|^2 \gtrsim \Big(\frac{|A|}{4}\Big)^2\frac{N}{2|A|} \geqslant \frac{N|A|}{32}.$$

Таким образом, функция $\hat{\chi}_A$ набирает существенную часть своей L_2-нормы на множестве B. Что можно сказать о множестве B? Если наша прогрессия достаточно длинная (что мы предположили), то множество B имеет ничтожную меру. То есть, функция $\hat{\chi}_A$ концентрируется на множестве малой меры: вероятность попасть в B равна примерно $\frac{1}{2|A|} = \frac{1}{2\alpha N}$. Кроме того, мы видим, что множество B хорошо структурировано, оно напоминает арифметическую прогрессию. Теперь перейдём к рассуждениям для произвольного множества с малым удвоением.

Удивительно, но аддитивную энергию можно легко выразить в терминах преобразования Фурье характеристических функций множеств A и B.

Лемма 1.3.3. *Пусть A и B — подмножества группы $\mathbb{Z}_N$. Справедливо равенство*

$$E(A,B) = \frac{1}{N}\sum_{\xi\in\mathbb{Z}_N}\big|\hat{\chi}_A(\xi)\big|^2\big|\hat{\chi}_B(\xi)\big|^2.$$

Доказательство. Отметим равенство

$$\Big|\Big\{(a,b)\in A\times B\;\Big|\;a+b=x\Big\}\Big| = \chi_A * \chi_B\,(x),$$

которое следует из определения свёртки. Подставим его в формулу (1.3.2):

$$E(A,B) = \sum_{x\in A+B}\Big|\chi_A * \chi_B\,(x)\Big|^2 = \sum_{x\in\mathbb{Z}_N}\Big|\chi_A * \chi_B\,(x)\Big|^2.$$

Согласно теореме Планшереля и тому, что преобразование Фурье переводит свёртку в умножение, получаем требуемое:

$$\sum_{x\in\mathbb{Z}_N}\Big|\chi_A * \chi_B\,(x)\Big|^2 = \frac{1}{N}\sum_{\xi\in\mathbb{Z}_N}\Big|\Big(\chi_A * \chi_B\Big)\hat{}\,(\xi)\Big|^2 = \frac{1}{N}\sum_{\xi\in\mathbb{Z}_N}\Big|\hat{\chi}_A(\xi)\Big|^2\Big|\hat{\chi}_B(\xi)\Big|^2.$$

□

Замечание 1.3.4. *Эта лемма верна в большей общности, объемлющая группа может быть произвольной конечной.*

Совмещая леммы 1.3.2 и 1.3.3, видим, что множества с малым удвоением имеют большую L_4-норму преобразования Фурье, а именно,

$$\sum_{\xi\in\mathbb{Z}_N}|\hat{\chi}_A(\xi)|^4 \geqslant \frac{N|A|^3}{\sigma[A]}. \tag{1.3.3}$$

Следующее упражнение не имеет прямого отношения к аддитивной комбинаторике, но оно очень хорошо показывает связь множеств Бора с преобразованием Фурье.

Упражнение 1.3.2. *Пусть f — суммируемая функция на пространстве $\mathbb{R}^d$. Пусть множество R таково, что*

$$\int\limits_R f \geqslant 0.9\|f\|_{L_1(\mathbb{R}^d)}.$$

Тогда

$$\Re\hat{f}(\xi) \geqslant 0.5\|f\|_{L_1}, \quad \xi \in 0.1R^*.$$

Символом R^* обозначена поляра множества R.

Вернёмся теперь к конечным группам.

Теорема 1.3.5 (Теорема Боголюбова–Ружи)**.** *Пусть множество $A \subset \mathbb{Z}_N$ удовлетворяет неравенству $\sigma[A] \leqslant C$. Тогда $B(R, \frac{1}{20}) \subset 2A - 2A$, где*

$$R = \Big\{\xi \in \mathbb{Z}_N \;\Big|\; |\hat{\chi}_A(\xi)| \geqslant \frac{|A|}{2\sqrt{C}}\Big\} \setminus \{0\}.$$

Доказательство. Отметим, что точка x принадлежит множеству $2A - 2A$, если $\chi_A * \chi_A * \chi_{-A} * \chi_{-A}(x) > 0$. Нетрудно видеть, что

$$\Big(\chi_A * \chi_A * \chi_{-A} * \chi_{-A}\Big)\hat{} = \hat{\chi}_A^2\bar{\hat{\chi}}_A^2 = |\hat{\chi}_A|^4.$$

Поэтому, достаточно доказать неравенство

$$\sum_{\xi\in\mathbb{Z}_N} |\hat{\chi}_A(\xi)|^4 e^{-2\pi i\frac{\xi x}{N}} > 0 \tag{1.3.4}$$

для всякой точки $x \in B(R, \frac{1}{20})$. (Хотя в левой части неравенства и написано, вообще говоря, комплексное число, оно, на самом деле, вещественно.) Перепишем его левую часть как

$$\sum_{\xi\in\mathbb{Z}_N} |\hat{\chi}_A(\xi)|^4 - \sum_{\xi\in\mathbb{Z}_N} |\hat{\chi}_A(\xi)|^4(1 - e^{-2\pi i\frac{\xi x}{N}})$$

и воспользуемся двумя неравенствами

$$\Big|1 - e^{-2\pi i\frac{\xi x}{N}}\Big| \leqslant \frac{1}{2}, \quad \xi \in R \cup \{0\}, x \in B\Big(R, \frac{1}{20}\Big);$$
$$\Big|1 - e^{-2\pi i\frac{\xi x}{N}}\Big| \leqslant 2, \quad \text{во всех остальных случаях.}$$

Получим оценку

$$\sum_{\xi\in\mathbb{Z}_N} |\hat{\chi}_A(\xi)|^4 - \sum_{\xi\in\mathbb{Z}_N} |\hat{\chi}_A(\xi)|^4(1 - e^{-2\pi i\frac{\xi x}{N}}) \geqslant \frac{1}{2}\sum_{\xi\in\mathbb{Z}_N} |\hat{\chi}_A(\xi)|^4 - 2\sum_{\substack{\xi\notin R\\ \xi\neq 0}} |\hat{\chi}_A(\xi)|^4, \quad x \in B\Big(R, \frac{1}{20}\Big)$$

Чтобы оценить первую сумму снизу, воспользуемся неравенством (1.3.3), которое в нашем случае даст

$$\frac{1}{2}\sum_{\xi\in\mathbb{Z}_N} |\hat{\chi}_A(\xi)|^4 \geqslant \frac{N|A|^3}{2C}.$$

Оценить вторую сумму сверху поможет определение множества R и теорема Планшереля:

$$2\sum_{\substack{\xi\notin R\\ \xi\neq 0}} |\hat{\chi}_A(\xi)|^4 \leqslant 2\max_{\substack{\xi\notin R\\ \xi\neq 0}} |\hat{\chi}_A(\xi)|^2 \sum_{\xi\in\mathbb{Z}_N} |\hat{\chi}_A(\xi)|^2 < \frac{N|A|^3}{2C}.$$

Таким образом, неравенство (1.3.4) доказано, а с ним и теорема. □

Отметим тривиальную оценку мощности множества R, которая получается из неравенства Чебышева и теоремы Планшереля:

$$|R| = \Big|\Big\{|\hat{\chi}_A| \geqslant \frac{|A|}{2\sqrt{C}}\Big\}\Big| \leqslant \frac{4CN}{|A|}.$$

Чтобы доказать теорему 1.2.5, нам понадобится существенно уменьшить множество R, при этом, разумеется, уменьшив $\delta = \frac{1}{20}$.

Определение 1.3.6. Множество $\Lambda \subset \mathbb{Z}_N$ называется диссоциативным, если уравнение

$$\sum_{\lambda_i \in \tilde{\Lambda}} \pm\lambda_i = 0, \quad \tilde{\Lambda} \subset \Lambda,$$

допускает лишь тривиальное решение $\tilde{\Lambda} = \varnothing$.

Теорема 1.3.7. *Пусть $A \subset \mathbb{Z}_N$ — подмножество и $|A| = \alpha N$. Любое диссоциативное подмножество множества*

$$R = \{\xi \in \mathbb{Z}_N \mid |\hat{\chi}_A(\xi)| \geqslant \rho|A|\}$$

имеет мощность не более $2^{\frac{|\log \alpha|}{\rho^2}}$.

Доказательству теоремы 1.3.7 предпошлём лемму о тригонометрических полиномах, частоты которых принадлежат диссоциативному множеству.

Лемма 1.3.8. *Пусть Λ — диссоциативное множество. Рассмотрим функцию*

$$f(x) = \sum_{\lambda_i \in \Lambda} c_i \cos\Big(\frac{2\pi x\lambda_i}{N} + \beta_i\Big), \quad c_i, \beta_i \in \mathbb{R}. \tag{1.3.5}$$

Эта функция удовлетворяет неравенству

$$\frac{1}{N}\sum_{x \in \mathbb{Z}_N} e^{tf(x)} \leqslant \exp\Big(\frac{t^2}{N}\sum_{x \in \mathbb{Z}_N} f^2(x)\Big), \quad t \in \mathbb{R}.$$

Перед тем как доказывать лемму, постараемся подобрать родственное ей классическое утверждение. В гармоническом анализе известен принцип, что функции ζ_i вида

$$\zeta_i(x) = \cos(2\pi\lambda_i x), \quad x \in [0, 1),$$

ведут себя как независимые случайные величины, если последовательность λ_i растёт достаточно быстро (хотя бы как 2^i). Диссоциативность множества Λ позволяет использовать подобный принцип для функций

$$\zeta_i(x) = \cos\Big(\frac{2\pi x\lambda_i}{N} + \beta_i\Big), \quad \lambda_i \in \Lambda.$$

Превратим множество $\mathbb{Z}_N$ в вероятностное пространство, снабдив равномерной вероятностной мерой. О функциях ζ_i будем думать как о случайных величинах. Нетрудно видеть, что ноль не может лежать в диссоциативном множестве. Поэтому,

$$\mathbb{E}\zeta_i = \frac{1}{N}\sum_{x \in \mathbb{Z}_N} \cos\Big(\frac{2\pi x\lambda_i}{N} + \beta_i\Big) = 0.$$

Если бы величины ζ_i и ζ_j были независимыми в строгом смысле слова, то обязательно выполнялось бы равенство $\mathbb{E}\zeta_i\zeta_j = 0$. Так ли это в нашем случае? Проверим:

$$\frac{1}{N}\sum_{x\in\mathbb{Z}_N}\cos\Big(\frac{2\pi x\lambda_i}{N}+\beta_i\Big)\cos\Big(\frac{2\pi x\lambda_j}{N}+\beta_j\Big) = \\ \frac{1}{2N}\sum_{x\in\mathbb{Z}_N}\left(\cos\Big(\frac{2\pi x(\lambda_i+\lambda_j)}{N}+\beta_i+\beta_j\Big)+\cos\Big(\frac{2\pi x(\lambda_i-\lambda_j)}{N}+\beta_i-\beta_j\Big)\right)=0,$$

так как $\lambda_i+\lambda_j\neq 0$ и $\lambda_i-\lambda_j\neq 0$ по диссоциативности множества Λ. Аналогично, для всякого множества $\tilde{\Lambda}\subset\Lambda$,

$$\mathbb{E}\prod_{\lambda_j\in\tilde{\Lambda}}\zeta_j = 0. \tag{1.3.6}$$

Таким образом, можно считать, что величины ζ_j, до некоторой степени независимы. По крайней мере, они ортогональны как элементы L_2. В частности, для функции f, заданной формулой (1.3.5), имеет место равенство:

$$\frac{1}{N}\sum_{x\in\mathbb{Z}_N}f^2(x) = \mathbb{E}\big(\sum_j c_j\zeta_j\big)^2 = \sum_j c_j^2\mathbb{E}\zeta_j^2+\sum_{i\neq j}c_ic_j\mathbb{E}\zeta_j\zeta_i = \sum_j c_j^2\mathbb{E}\zeta_j^2 = \frac{1}{2}\sum_j c_j^2, \tag{1.3.7}$$

так как

$$\mathbb{E}\zeta_j^2 = \frac{1}{N}\sum_{x\in\mathbb{Z}_N}\cos^2\Big(\frac{2\pi x\lambda_j}{N}+\beta_j\Big) = \frac{1}{2}+\frac{1}{2N}\sum_{x\in\mathbb{Z}_N}\cos\Big(\frac{4\pi x\lambda_j}{N}+2\beta_j\Big) = \frac{1}{2}.$$

Напомним читателю, что число N простое (и не 2). Если функцию $f=\sum c_j\zeta_j$ интерпретировать как случайную величину, то лемма 1.3.8 утверждает неравенство

$$\mathbb{E}e^{t\zeta}\leqslant e^{t^2\mathbb{E}\zeta^2}.$$

У этого неравенства есть чисто вероятностный аналог.

Упражнение 1.3.3. *Пусть $\xi_1,\xi_2,\dots,\xi_n$ — независимые случайные величины с нулевыми средними, такие что $|\xi_j|\leqslant c_j$. Докажите неравенство Хоффдинга:*

$$\mathbb{P}\Big(\xi>t\Big)\leqslant e^{-\frac{n^2t}{2\sum c_j^2}},\quad \xi=\sum_{j=1}^n\xi_j.$$

Доказательство леммы 1.3.8. Подметим элементарное неравенство $e^{\tau y}\leqslant \operatorname{ch}\tau+y\operatorname{sh}\tau$, $|y|\leqslant 1$. Чтобы его доказать, достаточно заметить, что слева стоит выпуклая функция параметра y, справа линейная, а на концах отрезка $|y|\leqslant 1$ достигается равенство. Подставим в это элементарное неравенство $\tau=c_it$ и $y=\cos(\frac{2\pi\lambda_ix}{N}+\beta_i)$ при каждом $\lambda_i\in\Lambda$, перемножим по всем $\lambda_i\in\Lambda$ и усредним по параметру x:

$$\frac{1}{N}\sum_{x\in\mathbb{Z}_N}e^{tf(x)} = \frac{1}{N}\sum_{x\in\mathbb{Z}_N}\prod_{\lambda_i\in\Lambda}e^{c_it\cos(\frac{2\pi\lambda_ix}{N}+\beta_i)}\leqslant\frac{1}{N}\sum_{x\in\mathbb{Z}_N}\prod_{\lambda_i\in\Lambda}\Big(\operatorname{ch}(c_it)+\operatorname{sh}(c_it)\cos\Big(\frac{2\pi\lambda_ix}{N}+\beta_i\Big)\Big).$$

Теперь мысленно раскроем скобки в последнем произведении и переставим знаки суммы. Получится

$$\frac{1}{N}\sum_{x\in\mathbb{Z}_N}\prod_{\lambda_i\in\Lambda}\Big(\operatorname{ch}(c_it)+\operatorname{sh}(c_it)\cos\Big(\frac{2\pi\lambda_ix}{N}+\beta_i\Big)\Big) = \sum_{\tilde{\Lambda}\subset\Lambda}K_{\tilde{\Lambda}}\mathbb{E}\prod_{\lambda_i\in\tilde{\Lambda}}\cos\Big(\frac{2\pi\lambda_ix}{N}+\beta_i\Big),$$

где $K_{\tilde\Lambda} = \prod_{\lambda_i\in\tilde\Lambda}\operatorname{sh}(c_it)\prod_{\lambda_i\notin\tilde\Lambda}\operatorname{ch}(c_it)$. Равенство (1.3.6) подсказывает нам, что во внешней сумме (по параметру $\tilde\Lambda$) не равно нулю лишь слагаемое с $\tilde\Lambda = \varnothing$, то есть,

$$\frac{1}{N}\sum_{x\in\mathbb{Z}_N}\prod_{\lambda_i\in\Lambda}\Big(\operatorname{ch}(c_it)+\operatorname{sh}(c_it)\cos\Big(\frac{2\pi\lambda_i x}{N}+\beta_i\Big)\Big) = \prod_{\lambda_i\in\Lambda}\operatorname{ch}(c_it).$$

Подметим ещё одно элементарное неравенство:

$$\operatorname{ch} u = \sum_{k=0}^{\infty}\frac{u^{2k}}{(2k)!}\leqslant\sum_{k=0}^{\infty}\frac{u^{2k}}{2^k k!} = e^{\frac{u^2}{2}}.$$

Применив его к каждому множителю и воспользовавшись равенством (1.3.7), завершаем доказательство

$$\prod_{\lambda_i\in\Lambda}\operatorname{ch}(c_it)\leqslant e^{\frac{t^2}{2}\sum\limits_{\lambda_i\in\Lambda}c_i^2} = e^{\frac{t^2}{N}\sum\limits_{x\in\mathbb{Z}_N}f^2(x)}.$$

□

Доказательство теоремы 1.3.7. Пусть Λ — диссоциативное подмножество R. Рассмотрим тригонометрический полином

$$f(x) = \Re\Big(\sum_{r\in\Lambda}\hat\chi_A(r)e^{2\pi i\frac{rx}{N}}\Big)$$

и изучим его свойства. Во-первых,

$$f(x) = \sum_{r\in\Lambda}|\hat\chi_A(r)|\cos\Big(\frac{2\pi rx}{N}+\arg\big(\hat\chi_A(r)\big)\Big),$$

то есть, многочлен f имеет вид (1.3.5) с $c_i = |\hat\chi_A(r_i)|$. Во-вторых,

$$\hat f(\xi) = \begin{cases}\frac{N}{2}\hat\chi_A(\xi), & \xi\in\Lambda\cup(-\Lambda),\\ 0, & \text{иначе.}\end{cases}\tag{1.3.8}$$

Действительно, по формуле $\Re(ab) = \frac{1}{2}(ab+\bar a\bar b)$,

$$f(x) = \Re\Big(\sum_{r\in\Lambda}\hat\chi_A(r)e^{2\pi i\frac{rx}{N}}\Big) = \sum_{r\in\Lambda}\Big(\frac{1}{2}\hat\chi_A(r)e^{2\pi i\frac{rx}{N}}+\frac{1}{2}\bar{\hat\chi}_A(r)e^{-2\pi i\frac{rx}{N}}\Big) = \sum_{r\in\Lambda}\Big(\frac{1}{2}\hat\chi_A(r)e^{2\pi i\frac{rx}{N}}+\frac{1}{2}\hat\chi_A(-r)e^{-2\pi i\frac{rx}{N}}\Big).$$

Формулу (1.3.8) можно записать чуть иначе:

$$\hat f = \frac{N}{2}\hat\chi_A\chi_{\Lambda\cup(-\Lambda)},$$

то есть, функция $2f/N$ есть ортогональная проекция в L_2 функции χ_A на пространство функций, носитель преобразования Фурье которых лежит в множестве $\Lambda\cup(-\Lambda)$. Отсюда следует равенство

$$\sum_{x\in\mathbb{Z}_N}f(x)\chi_A(x) = \frac{2}{N}\sum_{x\in\mathbb{Z}_N}f^2(x).\tag{1.3.9}$$

Эту формулу можно доказать, просто пользуясь формулой (1.3.8) и теоремой Планшереля.

Применим теперь лемму 1.3.8 к нашему многочлену f:

$$\exp\Big(\frac{t^2}{N}\sum_{x\in\mathbb{Z}_N} f^2(x)\Big) \geqslant \frac{1}{N}\sum_{x\in\mathbb{Z}_N} e^{tf(x)} \geqslant \frac{1}{N}\sum_{x\in A} e^{tf(x)} \overset{\text{AM-GM}}{\geqslant} \frac{|A|}{N}\exp\Big(\frac{1}{|A|}\sum_{x\in A} tf(x)\Big) \overset{(1.3.9)}{=} \frac{|A|}{N}\exp\Big(\frac{2t}{N|A|}\sum_{x\in\mathbb{Z}_N} f^2(x)\Big).$$

Таким образом,

$$\alpha = \frac{|A|}{N} \leqslant \exp\left(\Big(\frac{t^2}{N} - \frac{2t}{N|A|}\Big)\sum_{x\in\mathbb{Z}_N} f^2(x)\right).$$

Выбирая $t = \frac{1}{|A|}$, получаем оценку

$$\sum_{x\in\mathbb{Z}_N} f^2(x) \leqslant N|A|^2|\log\alpha|.$$

Но с другой стороны, по теореме Планшереля, формуле (1.3.8) и тому, что Λ лежит в множестве надуровня $\hat{\chi}_A$ (а тогда и $-\Lambda$ тоже, т.к. $\hat{\chi}_A(-\xi) = \bar{\hat{\chi}}_A(\xi)$),

$$\sum_{x\in\mathbb{Z}_N} f^2(x) = \frac{1}{N}\frac{N^2}{4}\sum_{r\in\Lambda\cup-\Lambda} |\hat{\chi}_A(r)|^2 \geqslant |\Lambda|\frac{\rho^2|A|^2N}{2}.$$

Сравнивая посление два неравенства, получаем требуемое. □

1.10.2018

Доказательство теоремы 1.2.5. Воспользуемся теоремой 1.3.5, определим множество R как в этой теореме. Положим $\rho = \frac{1}{2\sqrt{C}}$ и $K = \Lambda$, где Λ — наибольшее по включению диссоциативное подмножество множества R. Теорема 1.3.7 даёт оценку

$$|K| \leqslant \frac{2|\log\alpha|}{\rho^2} = 8C|\log\alpha|. \tag{1.3.10}$$

Осталось лишь проверить вложение $B(K, \frac{1}{160C|\log\alpha|}) \subset B(R, \frac{1}{20})$. Выберем любой элемент ξ из множества $B(K, \frac{1}{160C|\log\alpha|})$:

$$\forall\lambda\in\Lambda \quad \operatorname{dist}\Big(\frac{\xi\lambda}{N}, \mathbb{Z}\Big) \leqslant \frac{1}{160C|\log\alpha|}. \tag{1.3.11}$$

Нетрудно видеть, что любой элемент $r \in R$ представляется в виде $\sum_{\lambda_i\in\tilde{\Lambda}} \pm\lambda_i$ (иначе множество Λ — не максимальное по включению). Поэтому для всякого элемента $r \in R$,

$$\operatorname{dist}\Big(\frac{r\xi}{N}, \mathbb{Z}\Big) = \operatorname{dist}\Big(\frac{\xi\sum_{\lambda_i\in\tilde{\Lambda}}\pm\lambda_i}{N}, \mathbb{Z}\Big) \leqslant |\Lambda|\max_{\lambda\in\Lambda}\operatorname{dist}\Big(\frac{\xi\lambda}{N}, \mathbb{Z}\Big) \overset{\substack{(1.3.10),\\(1.3.11)}}{\leqslant} \frac{1}{20},$$

что и означает $\xi \in B(R, \frac{1}{20})$.

1.4 Доказательство теоремы 1.2.6: геометрия решеток

Определение 1.4.1. Пусть $v_1, v_2, \ldots, v_s$ — линейно независимые векторы в $\mathbb{R}^d$. Множество $\Lambda = \bigoplus_{j=1}^{s} \mathbb{Z}v_j$ называется решёткой.

Лемма 1.4.2. *Пусть* $\Lambda = \bigoplus_{j=1}^{d} \mathbb{Z}v_j$ *— решётка в* $\mathbb{R}^d$*, а* $B_r(x)$ *— евклидов шар радиуса* r *с центром в точке* x*. Имеет место предельное соотношение*

$$|\Lambda \cap B_R(x)| = \frac{\operatorname{vol} B_R(x)}{|\det[v_1, v_2, \dots, v_d]|} + o(R^d), \quad R \to \infty.$$

Доказательство. Любая точка пространства $\mathbb{R}^d$ может быть единственным образом представлена как линейная комбинация векторов v_j. Поэтому параллелепипеды p_m, $m \in \mathbb{Z}^d$,

$$p_m = \Big\{ x \in \mathbb{R}^d \;\Big|\; x = \sum_{j=1}^{d} x_j v_j, \quad x_j \in [m_j, m_j + 1) \Big\},$$

замощают $\mathbb{R}^d$. Нетрудно видеть, что $\operatorname{vol} p_m = \det[v_1, v_2, \dots, v_d]$ и $\operatorname{diam} p_m \leqslant \sum \|v_j\| = V$ (обозначим последнюю сумму символом V). Отметим также, что различные точки множества Λ лежат в различных параллелепипедах p_m. Рассмотрим фигуру F_R, образованную параллелепипедами p_m, накрывающими точки множества $\Lambda \cap B_R(x)$. Получаем:

$$|\lambda \cap B_R(x)| \det[v_1, v_2, \dots, v_d] = \operatorname{vol}(F_R) \overset{F_R \subset B_{R+V}(x)}{\leqslant} \operatorname{vol}(B_{R+V}(x)) = \operatorname{vol}(B_R(x)) + o(R^d).$$

Оценка в обратную сторону получается из вложения $B_{R-V}(x) \subset F_R$. □

Следствие 1.4.3. *Величина* $|\Lambda| = |\det[v_1, v_2, \dots, v_d]|$ *не зависит от выбора базиса* $\{v_j\}$*, а лишь от самого множества* Λ*. Она называется модулем решётки.*

Следствие 1.4.4. *Любая дискретная подгруппа* $\mathbb{R}^d$ *— решётка.*

Доказательство. Пусть Λ — дискретная подгруппа $\mathbb{R}^d$. Не умаляя общности, можно считать, что её линейная оболочка — всё пространство $\mathbb{R}^d$. Пусть число r столь мало, что $B_r(0) \cap \Lambda = \{0\}$. Нетрудно видеть, что

$$|\Lambda \cap B_R(x)| \leqslant \frac{\operatorname{vol} B_{R+r}(x)}{\operatorname{vol} B_{\frac{r}{2}}(0)},$$

так как шарики $B_{\frac{r}{2}}(x)$ и $B_{\frac{r}{2}}(y)$, $x \neq y \in \Lambda$, не пересекаются. Стало быть, существует положительная константа c, такая что $|\Lambda \cap B_R(x)| \leqslant cR^d$. Посмотрим теперь на всевозможные линейно независимые системы $\{v_j\}_{j=1}^d$ в группе Λ и пусть μ — инфимум функции $|\det[v_1, v_2, \dots, v_d]|$ на множестве всех таких базисов. Рассмотрим теперь какую-нибудь конкретную систему $\{v_j\}_{j=1}^d$, на которой инфимум почти достигается:

$$|\det[v_1, v_2, \dots, v_d]| \leqslant 1.1\mu.$$

Докажем, что тогда $\Lambda = \bigoplus \mathbb{Z}v_j$. Не умаляя общности, можно считать, что $\det[v_1, v_2, \dots, v_d] > 0$.

Предположим противное. Пусть существует элемент $w = \sum_1^d m_j v_j \in \Lambda$, такой что для некоторого индекса k коэффициент m_k нецелый. Покажем, что в этом случае существует $w' = \sum_1^d m'_j v_j \in \Lambda$ с $m'_k \in (0, \frac{1}{2}]$. Будем изменять элемент w и коэффициенты m_k, сохраняя их обозначения. Вычитая из элемента w кратное количество векторов v_k, можем добиться того, что $m_k \in [0, 1)$. Если $m_k \in (\frac{1}{2}, 1)$, заменим элемент w на $v_k - w$ и получим $m_k \in [0, \frac{1}{2}]$ (а если это вложение и так было верно, оставим всё как есть). Посмотрим теперь на значение функции, которую мы минимизировали, на базисе $v_1, v_2, \dots, v_{k-1}, w, v_{k+1}, \dots, v_d$ (в базисе $\{v_j\}$ мы заменили вектор v_k на w):

$$\det[v_1, v_2, \dots, v_{k-1}, w, v_{k+1}, \dots, v_d] = m_k \det[v_1, v_2, \dots, v_d] \leqslant \frac{1}{2} \cdot 1.1\mu < \mu.$$

Противоречие. □

Следствие 1.4.5. *Пусть Λ — решётка в $\mathbb{R}^d$, а Λ' — её подрешётка. Тогда индекс Λ' в Λ как подгруппы равен $\frac{|\Lambda'|}{|\Lambda|}$.*

Доказательство. Пусть индекс Λ' в Λ равен k. Выберем в Λ элементы $w_1, w_2, \dots, w_k$ — представителей различных элементов Λ/Λ'. В таком случае, множества $w_j + \Lambda'$ не пересекаются и покрывают Λ. Остаётся подметить равенство

$$|\Lambda \cap B_R(0)| = \sum_{j=1}^{k} \big|(w_j + \Lambda') \cap B_R(0)\big| = \sum_{j=1}^{k} \big|\Lambda' \cap B_R(-w_j)\big|$$

и воспользоваться леммой 1.4.2. □

Лемма 1.4.6 (Лемма Блихфельдта)**.** *Пусть Λ — решётка в $\mathbb{R}^d$, а K — измеримое множество, такое что $\operatorname{vol} K > |\Lambda|$. Существуют векторы $a \neq b \in K$, такие что $b - a \in \Lambda$.*

Доказательство. Не умаляя общности, можем считать множество K ограниченным. Предположим противное: пусть для всяких $a \neq b \in \Lambda$ множества $a + K$ и $b + K$ не пересекаются. Рассмотрим множество $\cup_{a\in\Lambda\cap B_R(0)}(K + a)$. По лемме 1.4.2,

$$\operatorname{vol}\Big(\cup_{a\in\Lambda\cap B_R(0)}(K+a)\Big) = \operatorname{vol} K|\Lambda \cap B_R(0)| = \frac{\operatorname{vol} K}{|\Lambda|}\operatorname{vol}(B_R(0)) + o(R^d).$$

С другой стороны, $\cup_{a\in\Lambda\cap B_R(0)}(K + a) \subset B_{R+\operatorname{diam} K}(0)$ и поэтому,

$$\operatorname{vol}\Big(\cup_{a\in\Lambda\cap B_R(0)}(K+a)\Big) \leqslant \operatorname{vol}(B_R(0)) + o(R^d),$$

что противоречит неравенству $|\Lambda| < \operatorname{vol} K$. □

Определение 1.4.7. Пусть Λ — решётка в $\mathbb{R}^d$, а K — выпуклое центрально-симметричное тело. Определим числа λ_i согласно формуле

$$\lambda_i = \inf\Big\{\lambda \in \mathbb{R}_+ \;\Big|\; \lambda K \cap \Lambda \quad \text{содержит хотя бы } i \text{ линейно независимых векторов}\Big\}.$$

Теорема 1.4.8 (Вторая теорема Минковского)**.** *Пусть Λ — решётка в $\mathbb{R}^d$, а K — выпуклое центрально-симметричное тело. Тогда*

$$\lambda_1\lambda_2\dots\lambda_d \operatorname{vol} K \leqslant 2^d|\Lambda|.$$

Идея доказательства состоит в построении множества A, такого что $\operatorname{vol} A = 2^{-d}\lambda_1\lambda_2\dots\lambda_d \operatorname{vol} K$ и при этом $A - A \cap \Lambda = \{0\}$. Множество A будет получаться из множества $\frac{1}{2}\lambda_d K$ последовательными сжатиями. На самом деле, кроме сжатий, нам придётся немного сдвигать различные слои множества.

Доказательство. Пусть $b_1, b_2, \dots, b_d$ — линейно независимые элементы решётки Λ, такие что $b_i \in \lambda_i\overline{K}$. Пусть кроме того V_j — линейная оболочка векторов $b_1, b_2, \dots, b_j$. Будем последовательно строить множества K_j начиная с $K_d = \frac{1}{2}\lambda_d K$ и заканчивая на K_1. Пока что нам будут важны следующие два свойства множеств K_j:

$$K_j \subset K_{j+1}, \tag{1.4.1}$$

$$\forall \omega \in \mathbb{R}^d \text{ множество} \quad K_j \cap (V_i + \omega) \text{ выпукло, если } i \leqslant j. \tag{1.4.2}$$

Пусть множество K_j уже построено, опишем построение множества K_{j-1}. Будем работать в координатах $V_{j-1} \times V_{j-1}^{\perp}$. Для всякой точки $w \in V_{j-1}^{\perp}$ выберем произвольную точку $(f(w), w)$ в множестве $K_j \cap (V_{j-1} + (0, w))$ (если последнее множество пусто, ничего выбирать не будем). От функции f мы не будем требовать никаких свойств, кроме измеримости (хотя читатель с лёгкостью построит, например, непрерывную функцию f); например, в качестве $f(w)$ можно взять центр масс множества $K_j \cap (V_{j-1} + (0, w))$. Построим множество K_{j-1}:

$$K_{j-1} = \Big\{ (v, w) \;\Big|\; v = \theta u + (1-\theta) f(w), \quad (u, w) \in K_j \Big\},$$

где $\theta = \frac{\lambda_{j-1}}{\lambda_j}$. Иными словами, мы сначала режем множество K_j на слои сдвигами плоскости V_{j-1}, после чего к каждому сечению применяем гомотетию с коэффициентом θ и центром внутри сечения. Правильный выбор центра гомотетии позволяет удовлетворить свойству (1.4.1). Кроме того, так как гомотетия сохраняет выпуклость множеств, построенные таким образом множества K_j удовлетворяют и свойству (1.4.2).

Докажем по индукции формулу $\operatorname{vol} K_j = 2^{-d} \lambda_d \lambda_{d-1} \dots \lambda_{j+1} \lambda_j^j \operatorname{vol} K$. Индукция, разумеется, имеет случай $j = d$ в качестве базы, и переход от j к $j-1$. Осуществим переход. Воспользуемся теоремой Фубини (символом vol_s обозначим s-мерный объём):

$$\operatorname{vol} K_{j-1} = \int\limits_{V_{j-1}^{\perp}} \operatorname{vol}_{j-1} \Big(K_{j-1} \cap (V_{j-1} + w) \Big)\, dw = \int\limits_{V_{j-1}^{\perp}} \theta^{j-1} \operatorname{vol}_{j-1} \Big(K_j \cap (V_{j-1} + w) \Big)\, dw = \theta^{j-1} \operatorname{vol} K_j.$$

Осталось вспомнить, что $\theta = \frac{\lambda_{j-1}}{\lambda_j}$ и воспользоваться индукционным предположением.

Докажем теперь по индукции вложение

$$(K_j - K_j) \cap V_j \subset \lambda_j K.$$

База $j = d$ очевидна, докажем переход от j к $j-1$. Будем работать в координатах $V_{j-1} \times V_{j-1}^{\perp}$, и пусть некоторая точка лежит в множестве $K_{j-1} - K_{j-1} \cap V_{j-1}$. Это значит, что она может быть представленая как $(x, w) - (y, w)$, где $(x, w), (y, w) \in K_{j-1}$. По определению множеств K_{j-1},

$$x = \theta \tilde{x} + (1-\theta) f(w), \quad y = \theta \tilde{y} + (1-\theta) f(w), \quad (\tilde{x}, w), (\tilde{y}, w) \in K_j, \; \theta = \frac{\lambda_{j-1}}{\lambda_j}.$$

Поэтому $(x, w) - (y, w) = \frac{\lambda_{j-1}}{\lambda_j} (\tilde{x} - \tilde{y}, 0)$. Последняя точка лежит в множестве $\theta(K_j - K_j) \cap V_j$, что лежит в $\lambda_{j-1} K$ по предположению индукции.

Теперь мы можем завершить доказательство. Достаточно доказать, что множество $K_1 - K_1$ пересекается с Λ лишь по началу координат (тогда утверждение теоремы следует из уже доказанной формулы $\operatorname{vol} K_1 = 2^{-d} \lambda_1 \lambda_2 \dots \lambda_d \operatorname{vol} K$ и леммы 1.4.6). Пусть не так и нашлась точка $L = \sum_1^k m_j b_j$ (пусть $m_k \neq 0$), лежащая в множестве $K_1 - K_1$. В таком случае,

$$L \in K_1 - K_1 \cap V_k \overset{(1.4.1)}{\subset} K_k - K_k \cap V_k.$$

Это множество, как мы доказали, лежит в $\lambda_k K$. А это уже противоречит тому, что $m_k \neq 0$, так как $\lambda_k K \cap \Lambda \subset V_{k-1}$. □

8.10.2018

Доказательство теоремы 1.2.6. Пусть $R = \{r_1, r_2, \dots, r_k\}$. Так как наличие или отсутствие нуля в множестве не влияет на его окрестность Бора, можем считать, что $r_j \neq 0$. Положим

$$\Lambda = N\mathbb{Z}^k + (r_1, r_2, \dots, r_k)\mathbb{Z}.$$

По следствию 1.4.4, Λ — решётка. Нетрудно видеть, что индекс $N\mathbb{Z}^k$ в группе Λ равен N (напомним читателю, что число N простое). Поэтому, по следствию 1.4.5

$$|\Lambda| = N^{k-1}. \tag{1.4.3}$$

Пусть $K = \{x \in \mathbb{R}^k \mid \forall j \quad |x_j| \leqslant 1\}$ — единичный шар пространства ℓ_∞. Пусть числа λ_j и векторы b_j определены так же, как в доказательстве теоремы 1.4.8. Определим вычеты s_j согласно формуле

$$s_j(r_1, r_2, \ldots, r_k) \equiv_N b_j$$

и отрезки $I_j = \Big[-\frac{\delta N}{\lambda_j k}, \frac{\delta N}{\lambda_j k} \Big]$. Зададим нашу обобщённую арифметическую прогрессию P формулой

$$P = \Big\{ \sum_{j=1}^{k} a_j s_j \;\Big|\; \forall j \quad a_j \in I_j \Big\}.$$

Начнём с того, что докажем неравенство

$$\Big\| \sum_{j=1}^{k} a_j b_j \Big\|_{\ell_\infty} \leqslant \delta N. \tag{1.4.4}$$

Действительно,

$$\Big\| \sum_{j=1}^{k} a_j b_j \Big\|_{\ell_\infty} \leqslant k \max_j |a_j| \|b_j\|_{\ell_\infty} \leqslant k \max_j \frac{\delta N}{\lambda_j k} \lambda_j \leqslant \delta N.$$

Нам надо доказать три факта про построенную прогрессию P. Во-первых, что $P \subset B(R, \delta)$; во-вторых, что P — правильная; и в третьих, оценку мощности P.

Сначала докажем, что $P \subset B(R, \delta)$. Достаточно доказать

$$\forall i \quad \operatorname{dist}\Big(\frac{\sum a_j s_j r_i}{N}, \mathbb{Z} \Big) < \delta.$$

Это равносильно неравенству

$$\operatorname{dist}\Big(\sum a_j s_j r_i, N\mathbb{Z} \Big) < \delta N,$$

которое, в свою очередь следует из

$$\operatorname{dist}\Big(\sum a_j b_j, N\mathbb{Z}^k \Big) < \delta N.$$

А это неравенство легко вывести из (1.4.4) и ограничения $\delta < \frac{1}{2}$.

Теперь покажем, что P — правильная обобщённая арифметическая прогрессия. Пусть не так, и нашлись два набора $\{a_j\}$ и $\{\tilde{a}_j\}$, такие что

$$\sum_{j=1}^{k} a_j s_j \equiv_N \sum_{j=1}^{k} \tilde{a}_j s_j, \quad \forall j \quad a_j, \tilde{a}_j \in I_j.$$

В таком случае,

$$\sum_{j=1}^{k} a_j b_j \equiv_N \sum_{j=1}^{k} \tilde{a}_j b_j.$$

Неравенство (1.4.4) и ограничение $\delta < \frac{1}{2}$ влекут

$$\sum_{j=1}^{k} a_j b_j = \sum_{j=1}^{k} \tilde{a}_j b_j,$$

что противоречит линейной независимости векторов b_j.

Наконец, оценим мощность прогрессии P_j. Отметим, что количество целочисленных точек в отрезке I_j — не менее $\frac{\delta N}{\lambda_j k}$. Поэтому,

$$|P| \geqslant \prod_{j=1}^{k} \frac{\delta N}{\lambda_j k} = \Big(\frac{\delta}{k}\Big)^k \frac{N^k}{\prod \lambda_j}.$$

Отметим, что $\operatorname{vol} K = 2^k$, поэтому, принимая во внимание формулу (1.4.3), теорема 1.4.8 позволяет нам заключить:

$$\prod_{j=1}^{k} \lambda_j \leqslant N^{k-1},$$

что и даёт требуемую оценку $|P| \geqslant \left(\frac{\delta}{k}\right)^k N$. □

1.5 Гомоморфизмы Фреймана и конец главы

Определение 1.5.1. Пусть $k \geqslant 2$ — натуральное число, Z_1 и Z_2 — коммутативные группы. Отображение $\varphi\colon X \to Z_2$, $X \subset Z_1$, называется гомоморфизмом Фреймана порядка k, если для всяких элементов $x_1, x_2, \ldots, x_k, y_1, y_2, \ldots, y_k \in X$, таких что

$$x_1 + x_2 + \ldots + x_k = y_1 + y_2 + \ldots + y_k,$$

также выполнено соотношение

$$\varphi(x_1) + \varphi(x_2) + \ldots + \varphi(x_k) = \varphi(y_1) + \varphi(y_2) + \ldots + \varphi(y_k).$$

Гомоморфизм Фреймана порядка k называют изоморфизмом Фреймана порядка k, если он есть биекция на образ, и обратное отображение является гомоморфизмом Фреймана порядка k.

Замечание 1.5.2. *Отображение φ является гомоморфизмом Фреймана порядка k тогда и только тогда, когда его естественное продолжение*

$$\varphi^*(x_1 + x_2 + \ldots + x_k) = \varphi(x_1) + \varphi(x_2) + \ldots + \varphi(x_k)$$

корректно определено на множестве kX.

Замечание 1.5.3. *Групповые гомомофизмы суть гомоморфизмы Фреймана произвольного порядка.*

Упражнение 1.5.1. *Пусть I — отрезок из вычетов группе $\mathbb{Z}_N$ (мы смотрим на вычеты как на комплексные корни из единицы порядка N и берём несколько пордяд идущих). Пусть длина I (то есть, число элементов минус один) не превосходит $\frac{N-1}{k}$. Тогда сужение на отрезок I стандартного вложения $\mathbb{Z}_N$ в $\mathbb{Z}$ (вложение есть представление вычета остатком по модулю N) есть гомоморфизм Фреймана порядка k.*

Упражнение 1.5.2. *Пусть конечные множества A и B изоморфны порядка 2. Тогда $E(A,A) = E(B,B)$.*

Упражнение 1.5.3. *Пусть φ — гомоморфизм Фреймана порядка tn и в группе Z_2 нет элементов порядка t. Тогда φ — гомоморфизм Фреймана порядка n.*

Лемма 1.5.4. *Пусть $A \subset \mathbb{Z}$ — конечное подмножество, такое что $|A| = n$ и $|A+A| \leqslant cn$, $k \geqslant 2$ — натуральное число, а число $m > 2c^{2k}n$ — простое. Существует подмножество $A' \subset A$ мощности хотя бы $\frac{n}{k}$, изоморфное порядка k подмножеству $\mathbb{Z}_m$.*

Доказательство. Пусть p — очень большое простое число (много большее, чем максимальный элемент множества A). Рассмотрим последовательность отображений:

$$[0..(p-1)] \xrightarrow{\psi_1} \mathbb{Z}_p \xrightarrow{\psi_2[q]} \mathbb{Z}_p \xrightarrow{\psi_3} \mathbb{Z} \xrightarrow{\psi_4} \mathbb{Z}_m.$$

Здесь ψ_1 — "зацикливание" отрезка $[0..(p-1)]$ (как мы предположили, всё множество A содержится в этом отрезке), то есть, рассмотрение числа отрезка $[0..(p-1)]$ как вычета по модулю p. Отображение $\psi_2[q]$ есть просто умножение на вычет q в группе $\mathbb{Z}_p$. Отображение ψ_3 — "расцикливание" группы $\mathbb{Z}_p$, это отображение каждому элементу $\mathbb{Z}_p$ естественным образом сопоставляет остаток по модулю p. Наконец, отображение ψ_4 — зацикливание по модулю m (то есть, оно сопоставляет каждому числу его остаток по модулю m). Отметим, что отображения $\psi_1, \psi_2[q], \psi_4$ — гомоморфизмы Фреймана порядка k. Отметим, что благодаря упражнению 1.5.1, отображение ψ_3 станет гомоморфизмом Фреймана порядка k, если его сузить на множество вида

$$\psi_1^{-1} \circ (\psi_2[q])^{-1}\Big(\Big[\frac{j-1}{k}(p-1), \frac{j}{k}(p-1)\Big]\Big). \tag{1.5.1}$$

(естественно, мы рассматриваем лишь целочисленные точки отрезка $\Big[\frac{j-1}{k}(p-1), \frac{j}{k}(p-1)\Big]$). Отметим, что при некотором выборе индекса j множество A', получаемое как пересечение прообраза (1.5.1) с множеством A, имеет мощность хотя бы $\frac{n}{k}$. Для каждого вычета q зафиксируем это множество A' раз и навсегда. Тогда отображение $\phi = \psi_4 \circ \psi_3 \circ \psi_2[q] \circ \psi_1 \colon A' \to \mathbb{Z}_m$ — гомоморфизм Фреймана порядка k.

Покажем, что параметр q можно подобрать так, чтобы отображение ϕ было изоморфизмом Фреймана порядка k. Пусть при некотором выборе q отображение ϕ не является изоморфизмом Фреймана порядка k. Это значит, что найдётся ненулевой элемент $s \in kA - kA$ и элементы $x_1, x_2, \dots, x_k, y_1, y_2, \dots y_k$, такие что

$$\begin{gathered} s = x_1 + x_2 + \dots + x_k - y_1 - y_2 - \dots y_k, \text{ но} \\ \phi(x_1) + \phi(x_2) + \dots + \phi(x_k) - \phi(y_1) - \phi(y_2) - \dots \phi(y_k) = 0. \end{gathered} \tag{1.5.2}$$

Для каждого ненулевого элемента $s \in kA - kA$, мы хотим оценить количество элементов q, таких что выполнены условия (1.5.2). Отметим, что первое условие в (1.5.2) влечёт

$$\phi_2[q](x_1) + \phi_2[q](x_2) + \dots + \phi_2[q](x_k) - \phi_2[q](y_1) - \phi_2[q](y_2) - \dots \phi_2[q](y_k) \equiv_p qs, \quad \phi_2[q] = \psi_2[q] \circ \psi_1. \tag{1.5.3}$$

Теперь припомним, что все элементы $\phi_2[q](z)$, $z \in A'$, лежат в отрезке вида $\Big[\frac{j-1}{k}(p-1), \frac{j}{k}(p-1)\Big]$ (см. формулу (1.5.1)). Поэтому, всевозможные суммы вида

$$\phi_3[q](z_1) + \phi_3[q](z_2) + \dots + \phi_3[q](z_k), \quad z_j \in A', \quad \phi_3[q] = \psi_3 \circ \phi_2[q],$$

лежат в некотором отрезке длины не более $p-1$, а стало быть, разности таких сумм принадлежат отрезку $[-(p-1), p-1]$. Поэтому, из (1.5.3) следует

$$\phi_3[q](x_1) + \phi_3[q](x_2) + \dots + \phi_3[q](x_k) - \phi_3[q](y_1) - \phi_3[q](y_2) - \dots \phi_3[q](y_k) = \begin{cases} qs, \\ qs - p. \end{cases}$$

Здесь вычет qs рассматриваем как остаток по модулю p, то есть, число отрезка $[0..p-1]$. С другой стороны, вторая строка равенства (1.5.2) гласит, что

$$\phi_3[q](x_1)+\phi_3[q](x_2)+\ldots+\phi_3[q](x_k)-\phi_3[q](y_1)-\phi_3[q](y_2)-\ldots\phi_3[q](y_k)\equiv_m 0$$

и поэтому либо qs, либо $qs-p$ делится на m. Напомним, что, фиксируя $s\in(kA-kA)\setminus\{0\}$, мы хотим оценить количество "плохих" вычетов q, то есть таких, для которых возможно равенство (1.5.3). Теперь видно, что таких вычетов q не более, чем $\frac{2p}{m}$.

Таким образом, всего "плохих" вычетов q, то есть таких, что для некоторого $s\in(kA-kA)\setminus\{0\}$ возможна ситуация (1.5.2) (т.е. ϕ — не изоморфизм Фреймана порядка k), не более $\frac{2p}{m}|kA|$. По следствию 1.1.10, это не превосходит $\frac{2pc^{2^k}n}{m}<p$. Поэтому найдётся вычет q, для которого ϕ — изоморфизм Фреймана порядка k. □

Следствие 1.5.5. *Пусть конечное множество $A\subset\mathbb{Z}$ таково что $|A+A|\leqslant C|A|$. Тогда множество $2A-2A$ содержит правильную обобщённую арифметическую прогрессию размерности не более $2^{11}C\log C$ и мощности хотя бы* $\exp(-2^{14}C(\log C)^2)|A|$.

Доказательство. Выберем $k=8$ и m — простое число интервала $2C^{16}|A|,4C^{16}|A|$ (которое существует по постулату Бертрана). По лемме 1.5.4, существует подмножество $A'\subset A$ мощности хотя бы $\frac{1}{8}|A|$, изоморфное порядка 8 некоторому множеству $X\subset\mathbb{Z}_m$. Число m нечётно, поэтому множества $A'+A'$ и $X+X$ изоморфны порядка 4 и

$$|X+X|=|A'+A'|\leqslant 8C|X|.$$

Кроме того,

$$\alpha=\frac{|X|}{m}\geqslant\frac{|A|}{8\cdot 4C^{16}|A|}\geqslant 2^{-5}C^{-16}.$$

Поэтому, теорема 1.2.5 позволяет найти множество $K\subset\mathbb{Z}_m$ мощности не более $8\cdot 8C|\log 2^{-5}C^{-16}|\leqslant 2^{11}C\log C$, такое что множество $2X-2X$ содержит окрестность Бора $B(K,\delta)$, и $\delta\geqslant\frac{2^{-14}}{C\log C}$. По теореме 1.2.6, окрестность Бора $B(K,\delta)$ содержит правильную обобщённую арифметическую прогрессию размерности не более $2^{11}C\log C$ и мощности хотя бы

$$\Big(\frac{1}{2^{14}C\log C\cdot 2^{11}C\log C}\Big)^{2^{11}C\log C}4C^{16}|A|\gtrsim\exp^{-2^{14}C(\log C)^2}|A|.$$

Осталось заметить, что отображение ϕ^{-1}, будучи изоморфизмом Фреймана порядка 8, естественным образом продолжается до 2-изоморфизма множеств $2X-2X$ и $2A'-2A'$, и заметить, что изоморфизмы Фреймана порядка 2 переводят правильные обобщённые арифметические прогрессии в правильные обобщённые арифметические прогрессии. □

15.10.2018

Мы хотим вывести теорему Фреймана из следствия 1.5.5. Это значит, что мы хотим покрыть множество A небольшим количеством сдвигов большой части множества $2A-2A$. Мы уже использовали подобную конструкцию в лемме 1.1.18. Теперь нам придётся её немного усложнить.

Лемма 1.5.6 (Лемма Чанг о покрытии)**.** *Пусть множество $A\subset\mathbb{Z}$ таково, что $|A|=n$, $|A+A|\leqslant Cn$ и множество $2A-2A$ содержит правильную обобщённую арифметическую прогрессию P размерности d и мощности ηn. Тогда множество A содержится в обобщённой арифметической прогрессии размерности $d+4C\log(\frac{C^4}{\eta})$ и мощности не более $2^d(\frac{C^4}{\eta})^{5C}\eta n$.*

Доказательство. Построим последовательность множеств P_j, R_j и S_j индуктивно. Основную роль играют множества P_j, а S_j и R_j — вспомогательную. В качестве множества P_0 выберем исходную прогрессию P.

На j-м шаге, мы рассматриваем множество P_{j-1} и в качестве R_j выбираем наибольшее по включению подмножество A, аддитивно независимое с множеством P_{j-1} (см. определение 1.1.17). Далее рассматриваем два случая.

1. Если $|R_j| > 2C$, то в качестве S_j полагаем любое подмножество R_j мощности $2C$ (отметим, что тогда множества P_{j-1} и S_j аддитивно независимы), после чего определяем $P_j := P_{j-1} + S_j$ и переходим к следующему шагу алгоритма.

2. Если $|R_j| \leqslant 2C$, то алгоритм прекращает свою работу.

Покажем, что алгоритм закончит свою работу не позже, чем через $\log_2(\frac{C^4}{\eta})$ шагов. Действительно, нетрудно видеть, что $|P_j| = |P|(2C)^j = (2C)^j \eta n$. С другой стороны, множество P_j содержится в множестве $2A - 2A + jA = (j+2)A - 2A$. По следствию 1.1.10,

$$(2C)^j \eta n = |P_j| \leqslant |(j+2)A - 2A| \leqslant C^{j+4} n.$$

Сравнивая левую часть с правой, получаем оценку $j \leqslant \log_2(\frac{C^4}{\eta})$.

Пусть алгоритм остановился на шаге $t \leqslant \log_2(\frac{C^4}{\eta})$. Аналогично доказательству леммы 1.1.18,

$$A \subset P_t - P_t + R_{t+1},$$

так как R_t — наибольшее по включению подмножество A, независимое с P_t. Таким образом,

$$A \subset P_0 - P_0 + S_0 - S_0 + S_1 - S_1 + \ldots + S_t - S_t + R_{t+1}.$$

Это множество содержится в арифметической прогрессии

$$\mathfrak{P} = (P_0 - P_0) + \bar{S}_0 + \bar{S}_1 + \ldots \bar{S}_t + \bar{R}_{t+1},$$

где $\bar{X}$ — арифметическая прогрессия, образующими которой служат элементы множества X, а отрезками I — отрезки $\{-1, 0, 1\}$ из трёх элементов. Размерность прогрессии $\mathfrak{P}$ не превосходит

$$d + (2C) \cdot (t+2) \leqslant d + 4C \log\Big(\frac{C^4}{\eta}\Big),$$

так как размерность прогрессии $P_0 - P_0$ равна d. Осталось оценить мощность $\mathfrak{P}$:

$$|\mathfrak{P}| \leqslant 2^d \eta n \big(3^{2C}\big)^{\log\left(\frac{C^4}{\eta}\right)} \leqslant 2^d \eta n \Big(\frac{C^4}{\eta}\Big)^{5C}.$$

□

Отметим, что чем меньше параметр η, тем хуже оценка размерности и мощности построенной прогрессии. На первый взгляд, это кажется странным, так как прогрессия $\mathfrak{P}$ получилась из P прибавлением множеств фиксированной мощности. На самом деле, ничего странного нет, просто при малом η алгоритм будет работать дольше, и поэтому размерность и мощность $\mathfrak{P}$ могут стать больше.

Теорема 1.5.7 (Эффективная теорема Фреймана)**.** *Пусть A — конечное подмножество целых чисел, такое что $|A + A| \leqslant C|A|$. Множество A содержится в обобщённой арифметической прогрессии размерности не более $2^{20} C^2 (\log C)^2$ и мощности не более $\exp(2^{20} C^2 (\log C)^2)|A|$.*

Доказательство этой теоремы состоит в применении леммы 1.5.6 к результатам следствия 1.5.5.

Глава 2

В поисках арифметической прогрессии

2.1 Теорема Семереди и лемма об удалении треугольника

Теорема 2.1.1 (Теорема Семереди, 1975)**.** *Для всякого числа $\nu > 0$ и всякого натурального числа $k \geqslant 3$, найдётся число $N(\nu, k)$, такое что для всякого натурального $N > N(\nu, k)$, всякое множество $A \subset [1..N]$, удовлетворяющее неравенству $|A| \geqslant \nu N$, содержит невырожденную арифметическую прогрессию длины k.*

Замечание 2.1.2. *Если $k > 3$, оценки числа $N(\nu, k)$ очень плохие.*

Существует несколько доказательств теоремы Семереди: чисто комбинаторное доказательство Семереди, эргодическое доказательство (Кацнельсон и Фюрстенберг, 1977), гармонико-аналитическое (Гауэрс, 2001) и графское (несколько авторов, приблизительно 2006). Все они весьма трудны, мы постараемся изложить основные идеи последнего подхода. Отметим, что все доказательства используют следующую схему: если множество A "хаотично" (псевдослучайно), то существование в нём арифметической прогрессии следует из принципов сродни закону больших чисел, а если A упорядоченно, то можно перейти к его подмножеству, лежащему в арифметической прогрессии, и имеющему в этой арифметической прогрессии большую плотность.

Развитие сюжета привело к доказательству теоремы Грина–Тао о том, что множество простых чисел содержит сколь угодно длинные арифметические прогрессии. Конечно, множество простых чисел имеет нулевую плотность, как известно,

$$|\mathbb{P} \cap [1..N]| \sim \frac{N}{\log N}, \quad N \to \infty.$$

Грину и Тао удалось показать, что множество простых чисел псевдослучайно (простые числа ведут себя хаотически), и поэтому к нему применимы принципы первого сценария доказательства теоремы Семереди. Отметим любопытную гипотезу.

Гипотеза 2.1.3 (Гипотеза Эрдёша–Турана)**.** *Пусть бесконечная последовательность $\{a_n\}_n$ натуральных чисел такова, что*

$$\sum_n \frac{1}{a_n} = \infty.$$

Тогда множество её значений содержит арифметическую прогрессию сколь угодно большой длины.

Наша ближайшая цель — доказать теорему Семереди в случае $k = 3$ (этот частный случай получен Ротом в 1954 году при помощи анализа Фурье). Мы же хотим следовать графскому доказательству и поэтому воспользуемся леммой об удалении треугольника.

Лемма 2.1.4 (Лемма об удалении треугольника)**.** *Для всякого числа $\varepsilon > 0$ найдётся число $\delta > 0$, такое что из всякого графа G на n вершинах, имеющего не более δn^3 треугольников, можно удалить не более εn^2 рёбер, уничтожив все треугольники.*

Раз и навсегда постулируем, что наши графы не имеют петель и кратных рёбер.

Вывод случая $k = 3$ в теореме 2.1.1 из леммы 2.1.4. Зафиксируем параметр ν. Пусть нам также дано некоторое множество $A \subset [1..N]$ плотности хотя бы ν. Построим граф G, он будет трёхдольным, с долями

$$V_1 = [1..3N],\ V_2 = [1..3N],\ V_3 = [1..3N].$$

Вершины $x \in V_1$ и $y \in V_2$ соединим ребром, если $y - x \in A$, вершины $y \in V_2$ и $z \in V_3$ соединим ребром, если $z - y \in A$, а вершины $x \in V_1$ и $z \in V_3$ соединим ребром, если $\frac{z-x}{2} \in A$ (в частности, разность $z-x$ должна быть чётной). В графе G получилось $9N$ вершин. Отметим, что треугольники в графе G соответствуют арифметическим прогрессиям длины 3 в множестве A по правилу:

$$\begin{aligned} y - x &= a; \\ z - y &= b; \quad \Longleftrightarrow \quad a + b = 2c. \\ z - x &= 2c; \end{aligned}$$

Предположим, что в множестве A нет невырожденных арифметических прогрессий, и покажем, что в таком случае число N ограничено сверху некоторой константой, зависящей лишь от параметра ν. Если в множестве A нет невырожденных арифметических прогрессий, то все трегольники в графе G соответствуют вырожденным арифметическим прогрессиям (то есть тем, для которых $a = b = c$). Каждый такой треугольник (x, y, z) однозначно задаётся числом $a \in A$ и например, числом $x \in [1..3N]$. Значит, число таких треугольников лежит в пределах от νN^2 до $9N^2$. Отметим также, что любые два таких треугольника не имеют общих рёбер.

Возьмём теперь $\varepsilon < \frac{1}{81}\nu$ и по этому числу ε выберем δ, такое что верно условие леммы 2.1.4. Если число N столь велико, что $9N^2 < 729\delta N^3$, то мы можем применить лемму 2.1.4 и удалить не более чем $81\varepsilon N^2$ рёбер, уничтожив все треугольники. Это противоречит неравенству $\varepsilon < \frac{1}{81}\nu$ (напомним, что треугольники, порождаемые вырожденными арифметическими прогрессиями, дизъюнктны). □

Замечание 2.1.5. *Мы получили оценку $N(\nu, 3) \leqslant 27\delta$, где $\delta = \delta(\frac{1}{81}\nu)$ задаётся леммой об удалении треугольника.*

2.2 Лемма регулярности Семереди

Определение 2.2.1. Пусть A и B — подмножества множества вершин графа G. Плотностью пары (A, B) назовём величину

$$d(A, B) = \frac{|E(A, B)|}{|A||B|}.$$

Здесь $E(A, B)$ — множество рёбер, соединяющих множество A с множеством B.

Определение 2.2.2. Пусть $\varepsilon \in (0, 1)$. Пару (A, B) множеств вершин графа G назовём ε-регулярной, если для всякой пары множеств $A' \subset A$, $B' \subset B$, таких что $|A'| \geqslant \varepsilon|A|$ и $|B'| \geqslant \varepsilon|B|$, имеет место неравенство

$$\Big|d(A', B') - d(A, B)\Big| < \varepsilon.$$

Определение 2.2.3. Пусть $X = (X_1, X_2, \dots, X_n)$ — разбиение множества вершин графа G. Назовём его ε-регулярным, если

$$\frac{1}{|V(G)|^2} \sum_{\substack{(X_i, X_j) \text{ не} \\ \varepsilon-\text{регулярна}}} |X_i||X_j| \leqslant \varepsilon.$$

Лемма 2.2.4 (Лемма регулярности Семереди)**.** *Для всякого числа $\varepsilon > 0$ существует число $M \in \mathbb{N}$, такое что для любого графа G существует ε-регулярное разбиение на не более чем M частей.*

Неформальный смысл леммы регулярности состоит в том, что граф на большом числе вершин приблизительно выглядит как случайный граф. Вероятностная интерпретация здесь очень важна, поэтому доказательству леммы регулярности предпошлём вероятностное истолкование введённых понятий. 22.10.2018

Множество V будем интерпретировать как вероятностное пространство, снабдив его алгеброй всех множеств и равномерной вероятностной мерой (мера каждой вершины равна $\frac{1}{|V(G)|}$). Таким образом, множество $V \times V$ тоже снабжено структурой вероятностного пространства. Рассмотрим на этом пространстве важную случайную величину

$$E(i,j) = \begin{cases} 0, & \text{вершины } i \text{ и } j \text{ не соединены ребром;} \\ 1, & \text{вершины } i \text{ и } j \text{ соединены ребром,} \end{cases} \qquad i, j \in V(G).$$

В таком случае, $|E(G)| = |V|^2 \mathbb{E}E$. Пусть A и B — подмножества множества вершин. Тогда

$$d(A,B) = \frac{1}{|A||B|} \sum_{\substack{i \in A \\ j \in B}} E(i,j) = \mathbb{E}(E \mid A \times B). \tag{2.2.1}$$

Разбиению X мы сопоставим алгебру множеств $\mathfrak{X}$, порождаемую элементами разбиения. Кроме того, с каждым разбиением свяжем важную величину. Сначала дадим комбинаторное определение.

Определение 2.2.5. Пусть $X = (X_1, X_2, \dots, X_n)$ — разбиение множества вершин графа. Определим среднеквадратичную плотность графа по этому разбиению формулой

$$\mathrm{MSD}(G, X) = \frac{1}{|V(G)|^2} \sum_{i,j=1}^{n} |X_i||X_j| d^2(X_i, X_j).$$

Среднеквадратичная плотность допускает вероятностную интерпретацию, следующую из интерпретации плотности:

$$\mathrm{MSD}(G, X) = \frac{1}{|V(G)|^2} \sum_{i,j=1}^{n} |X_i||X_j| \Big(\mathbb{E}(E \mid X_i \times X_j)\Big)^2 = \mathbb{E}\Big(\mathbb{E}(E \mid \mathfrak{X} \times \mathfrak{X})\Big)^2.$$

Следующая лемма есть прямое следствие неравенства Йенсена для условных математических ожиданий (или следствие определения условного математического ожидания как ортогонального проектора в L_2). Ввиду простоты, мы опустим её доказательство.

Лемма 2.2.6. *Пусть Y — подразбиение X (то есть, каждое множество разбиения Y содержится в некотором множестве разбиения X). Для каждой пары (A, B) множеств, измеримых относительно алгебры $\mathfrak{X}$, имеет место соотношение*

$$\mathbb{E}\Big[\Big(\mathbb{E}(E \mid \mathfrak{X} \times \mathfrak{X})\Big)^2 \chi_A \chi_B\Big] \leqslant \mathbb{E}\Big[\Big(\mathbb{E}(E \mid \mathfrak{Y} \times \mathfrak{Y})\Big)^2 \chi_A \chi_B\Big],$$

где $\mathfrak{Y}$ — алгебра, порождённая Y. В частности, $\mathrm{MSD}(G, X) \leqslant \mathrm{MSD}(G, Y)$.

Эта лемма утверждает, что среднеквадратичная плотность есть полуинвариант относительно измельчения разбиения. Более того, это свойство монотонности локально. Теперь мы можем перевести на язык теории вероятностей понятие ε-регулярной пары множеств. Точнее, мы извлечём из этого понятия следствие, которое выражается на вероятностном языке.

Лемма 2.2.7. *Пусть G — граф и пара (A, B) не ε-регулярна. Тогда существуют разбиения $A = A_1 \cup A_2$ и $B = B_1 \cup B_2$, такие что*

$$\mathbb{E}\Big[\sum_{i,j=1}^{2}\Big(\mathbb{E}(E \mid A_i \times B_j)\Big)^2 \chi_{A_i}\chi_{B_j}\Big] \geqslant \mathbb{E}\Big[\Big(\mathbb{E}(E \mid A \times B)\Big)^2 \chi_A \chi_B\Big] + \varepsilon^4 P(A)P(B).$$

Доказательство. Так как пара (A, B) не является ε-регулярной, существуют подмножества $A' \subset A$ и $B' \subset B$, такие что

$$|A'| \geqslant \varepsilon|A|,\ |B'| \geqslant \varepsilon|B|, \quad \text{и} \quad |d(A, B) - d(A', B')| \geqslant \varepsilon.$$

Положим $A_1 = A'$ и $B_1 = B'$ (соответственно, $A_2 = A \setminus A'$ и $B_2 = B \setminus B'$). Воспользуемся тождеством

$$\mathbb{E}\Big[\sum_{i,j=1}^{2}\Big(\mathbb{E}(E \mid A_i \times B_j)\Big)^2 \chi_{A_i}\chi_{B_j} - \Big(\mathbb{E}(E \mid A \times B)\Big)^2 \chi_A\chi_B\Big] =$$

$$\mathbb{E}\Big[\sum_{i,j=1}^{2}\Big(\mathbb{E}(E \mid A_i \times B_j) - \mathbb{E}(E \mid A \times B)\Big)^2 \chi_{A_i}\chi_{B_j}\Big] \geqslant$$

$$\mathbb{E}\Big[\Big(\mathbb{E}(E \mid A_1 \times B_1) - \mathbb{E}(E \mid A \times B)\Big)^2 \chi_{A_1}\chi_{B_1}\Big] \overset{(2.2.1)}{=} P(A_1)P(B_1)(d(A_1, B_1) - d(A, B))^2 \geqslant \varepsilon^4 P(A)P(B).$$

□

Иными словами, если пара (A, B) не ε-регулярна, то её можно подразбить так, что кусочек суммы, дающей среднеквадратичную плотность, подрастёт хотя бы на $\varepsilon^4 P(A)P(B)$.

Лемма 2.2.8. *Пусть разбиение $X = (X_1, X_2, \ldots, X_k)$ не является ε-регулярным. Тогда существует его подразбиение $\tilde{X}$, состоящее не более чем из $k2^k$ множеств, такое что*

$$\mathrm{MSD}(G, \tilde{X}) \geqslant \mathrm{MSD}(G, X) + \varepsilon^5.$$

Доказательство. Рассмотрим каждую пару (X_i, X_j), не являющуюся ε-регулярной. По лемме 2.2.7, существуют подразбиения $X_i = X_{i1} \cup X_{i2}$ и $X_j = X_{j_1} \cup X_{j_2}$, такие что выполнено определённое неравенство. Пополним разбиение X множествами X_{i1} и X_{j1} и полученное разбиение назовём $\tilde{X}_{ij}$. Тогда, мы неравенство из леммы 2.2.7 можно записать в форме

$$\mathbb{E}\Big[\Big(\mathbb{E}(E \mid \tilde{X}_{ij})\Big)^2 \chi_{X_i}\chi_{X_j}\Big] \geqslant \mathbb{E}\Big[\Big(\mathbb{E}(E \mid X)\Big)^2 \chi_{X_i}\chi_{X_j}\Big] + \varepsilon^4 P(X_i)P(X_j). \tag{2.2.2}$$

Разбиение $\tilde{X}$ определим как объединение разбиений $\tilde{X}_{ij}$ по всем парам (i, j), таким что пара (X_i, X_j) не ε-регулярна. Отметим, что при переходе от X к $\tilde{X}$, каждое множество X_i разбилось не более чем на 2^k подмножеств (потому что каждая пара (X_i, X_j), $j \in [1..k]$, даёт разбиение на две части), стало быть, $\tilde{X}$ — разбиение на не более, чем $k2^k$ частей. Оценим приращение среднеквадратичной

плотности:

$$\mathrm{MSD}(G,\tilde{X}) = \sum_{i,j}\mathbb{E}\Big[\Big(\mathbb{E}(E\mid\tilde{X})\Big)^2\chi_{X_i}\chi_{X_j}\Big] \overset{\text{Лем. 2.2.6}}{\geqslant}$$
$$\sum_{\substack{(X_i,X_j)\text{ не}\\ \varepsilon-\text{регулярна}}}\mathbb{E}\Big[\Big(\mathbb{E}(E\mid\tilde{X}_{i,j})\Big)^2\chi_{X_i}\chi_{X_j}\Big] + \sum_{\substack{(X_i,X_j)\\ \varepsilon-\text{регулярна}}}\mathbb{E}\Big[\Big(\mathbb{E}(E\mid X)\Big)^2\chi_{X_i}\chi_{X_j}\Big] \overset{(2.2.2)}{\geqslant}$$
$$\sum_{i,j}\mathbb{E}\Big[\Big(\mathbb{E}(E\mid X)\Big)^2\chi_{X_i}\chi_{X_j}\Big] + \varepsilon^4\sum_{\substack{(X_i,X_j)\text{ не}\\ \varepsilon-\text{регулярна}}}P(X_i)P(X_j) \geqslant \mathrm{MSD}(G,X)+\varepsilon^5$$

потому что разбиение X не ε-регулярно. □

Доказательство леммы регулярности 2.2.4. Построим последовательность измельчающихся разбиений X_j по следующему правилу. Во-первых, X_0 есть тривиальное разбиение. Во-вторых, если разбиение X_j является ε-регулярным, алгоритм заканчивает работу. Если же X_j — не ε-регулярно, то при помощи леммы 2.2.8 мы строим разбиение X_{j+1}, такое что

$$|X_{j+1}| \leqslant 3^{|X_j|} \quad \text{и} \quad \mathrm{MSD}(G,X_{j+1}) \geqslant \mathrm{MSD}(G,X_j)+\varepsilon^5.$$

Так как среднеквадратичная плотность не превосходит единицу, алгоритм закончит свою работу не позднее, чем через $[\varepsilon^{-5}]$ ходов. Стало быть, по завершении его работы мы получим ε-регулярное разбиение из не более чем $M(\varepsilon) = T(3,[\varepsilon^{-5}])$ частей. Функция $T(3,n)$ есть башня из троек высоты n, то есть,

$$T(3,n+1) = 3^{T(3,n)};\quad T(3,1)=3.$$

□

Замечание 2.2.9. *Оказывается, что оценки числа $M(\varepsilon)$ не могут быть существенно лучше полученных нами. А именно, Гауэрс [7] показал, что функция $M(\varepsilon)$ растёт хотя бы как башня высоты полиномиальной зависимости от ε^{-1} по основанию* 2.

2.3 Доказательство леммы об удалении треугольника

Лемма 2.3.1 (Считающая лемма)**.** *Пусть пары (X,Y), (X,Z) и (Y,Z) множеств вершин графа G являются ε-регулярными и*

$$d(X,Y)=\alpha,\ d(Y,Z)=\beta,\ d(X,Z)=\gamma.$$

Если $\alpha,\beta,\gamma \geqslant 2\varepsilon$, то число треугольников графа G вида (x,y,z), $x\in X$, $y\in Y$ и $z\in Z$, не менее $(1-2\varepsilon)(\alpha-\varepsilon)(\beta-\varepsilon)(\gamma-\varepsilon)|X||Y||Z|$.

Доказательство. Символом $\deg_U(v)$ обозначим число вершин из множества U, смежных с v. Рассмотрим два множества

$$\{x\in X \mid \deg_Y(x) < (\alpha-\varepsilon)|Y|\} \quad \text{и} \quad \{x\in X\mid \deg_Z(x)<(\gamma-\varepsilon)|Z|\}.$$

Из ε-регулярности пар (X,Y) и (X,Z) легко вывести, что мощность каждого из этих множеств не более $\varepsilon|X|$. Все вершины множества X, не принадлежащие этим двум множествам, назовём хорошими. Таким образом, хороших вершин хотя бы $(1-2\varepsilon)|X|$.

Пусть x — хорошая вершина, а Y_x и Z_x — множества её соседей в множествах Y и Z соответственно. Так как пара (Y, Z) является ε-регулярной и

$$|Y_x| \geqslant (\alpha - \varepsilon)|Y| \geqslant \varepsilon|Y| \quad \text{и} \quad |Z_x| \geqslant (\gamma - \varepsilon)|Z| \geqslant \varepsilon|Z|,$$

число рёбер между вершинами множеств Y_x и Z_x — не менее

$$(\beta - \varepsilon)|Y_x||Z_x| \geqslant (\alpha - \varepsilon)(\beta - \varepsilon)(\gamma - \varepsilon)|Y||Z|.$$

Стало быть, всего треугольников хотя бы $(1 - 2\varepsilon)(\alpha - \varepsilon)(\beta - \varepsilon)(\gamma - \varepsilon)|X||Y||Z|$, так как хороших вершин хотя бы $(1 - 2\varepsilon)|X|$. □

29.10.2018

Доказательство леммы 2.1.4 об удалении треугольника. Выберем $\frac{1}{4}\varepsilon$-регулярное разбиение графа G на не более чем M частей согласно лемме регулярности 2.2.4. Выкинем из графа рёбра следующих трёх типов:

1) Все рёбра между частями X_i и X_j, если пара (X_i, X_j) не $\frac{1}{4}\varepsilon$-регулярна;

2) Все рёбра между частями X_i и X_j, если $d(X_i, X_j) \leqslant \frac{1}{2}\varepsilon$;

3) Все рёбра с концом в части X_i, если $|X_i| \leqslant \frac{1}{4M}\varepsilon n$.

Напомним, что $n = |V(G)|$. Покажем, что мы выкинули не более чем εn^2 рёбер. Оценим число рёбер первого типа:

$$\sum_{\substack{(X_i, X_j) \\ \text{не } \frac{1}{4}\varepsilon-\text{регулярна}}} |E(X_i, X_j)| \leqslant \sum_{\substack{(X_i, X_j) \\ \text{не } \frac{1}{4}\varepsilon-\text{регулярна}}} |X_i||X_j| \leqslant \frac{\varepsilon n^2}{4}$$

по определению $\frac{1}{4}\varepsilon$-регулярного разбиения. Рёбра второго типа:

$$\sum_{d(X_i, X_j) \leqslant \frac{1}{2}\varepsilon} |E(X_i, X_j)| \leqslant \sum_{1 \leqslant i,j \leqslant M} \frac{1}{2}\varepsilon|X_i||X_j| = \frac{\varepsilon n^2}{2}.$$

И наконец, рёбра третьего типа:

$$\sum_{|X_i| \leqslant \frac{1}{4M}\varepsilon n} n|X_i| \leqslant \frac{\varepsilon n^2}{4},$$

так как всего частей не более M. Складывая три оценки, получаем, что всего выкинуто не более εn^2 рёбер. Покажем, что после выкидывания рёбер треугольников не осталось, если

$$\delta < \Big(1 - \frac{1}{2}\varepsilon\Big)\frac{\varepsilon^6}{3 \cdot 2^{12} M^3}. \tag{2.3.1}$$

Действительно, если после выкидывания остался треугольник, значит существуют три множества X_i, X_j, X_k, такие что все пары (X_i, X_j), (X_i, X_k), и (X_j, X_k) $\frac{1}{4}\varepsilon$-регулярны, плотность этих пар не менее $\frac{1}{2}\varepsilon$, а также размер каждого из множеств не менее $\frac{1}{4M}\varepsilon n$. Согласно считающей лемме 2.3.1, в исходном графе было не менее $(1 - \frac{1}{2}\varepsilon)\frac{\varepsilon^6}{3 \cdot 2^{12} M^3} n^3$ треугольников с вершинами в множествах X_i, X_j и X_k (мы поделили количество треугольников на три в том случае, если $i = j = k$). Что противоречит нашему предположению. □

Замечание 2.3.2. *Как мы видим, оценка* (2.3.1) *включает в себя число $M(\varepsilon)$, поэтому зависимость δ от ε довольно плохая.*

На самом деле, приведённое доказательство даёт немного больше информации, чем осталось от него в формулировке леммы об удалении треугольника. Мы удаляем рёбра по очень простой схеме. А именно, удаляем все рёбра, соединящие вершины определённых частей графа, полученных при разбиении конечной сложности. Такая более полная формулировка пригодится нам в следующей главе. Сформулируем лемму для случая трёхдольных графов (версия для обычных графов получается из этой утроением графа).

Лемма 2.3.3 (Лемма об удалении треугольника, вторая версия)**.** *Для всякого числа $\varepsilon > 0$ существуют числа $\delta > 0$ и M со следующим свойством. Для всяких конечных множеств V_1, V_2, V_3, и всякого трёхдольного графа $G = (V_1, V_2, V_3, E_{12}, E_{13}, E_{23})$, содержащего не более $\delta|V_1||V_2||V_3|$ треугольников, существуют разбиения X_1, X_2, X_3 сложности не более M множеств V_1, V_2, V_3 соответственно, а также множества рёбер $E'_{12} \subset V_1 \times V_2$, $E'_{23} \subset V_2 \times V_3$ и $E'_{13} \subset V_1 \times V_3$, такие что:*

1) Граф $G' = (V_1, V_2, V_3, E'_{12}, E'_{13}, E'_{23})$ не содержит треугольников;

2) Для пар $i \neq j \in [1..3]$ имеет место соотношение $|E_{ij} \setminus E'_{ij}| \leqslant \varepsilon|V_i \times V_j|$;

3) Множество E'_{ij} измеримо относительно алгебры $\mathfrak{X}_i \times \mathfrak{X}_j$ ($i \neq j \in [1..3]$).

Граф G' строится так. По графу G выбираем $\frac{1}{4}\varepsilon$-регулярное разбиение (если в какое-то множество разбиения попали вершины разных долей, надо это множество ещё разбить на три множества). Пусть $X_i^1 \subset V_1$ и $X_j^2 \subset V_2$ — два множества разбиения разных долей. Пару (X_i^1, X_j^2) назовём хорошей, если, во-первых, она $\frac{1}{4}\varepsilon$-регулярна, во-вторых, выполнено неравенство $d(X_i^1, X_j^2) > \frac{1}{2}\varepsilon$, и в третьих, множества пары не слишком малы, $|X_i^1| \geqslant \frac{1}{4M}\varepsilon|V_1|$ и $|X_j^2| \geqslant \frac{1}{4M}\varepsilon|V_2|$. Аналогично определим хорошесть пар множеств разбиения из других пар долей. Две вершины в графе G' соединены ребром если и только если пара множеств разбиения, к которым они принадлежат, хорошая. Таким образом, граф G' устроен просто (измерим относительно алгебры конечной сложности) и при этом приближает граф G. Отсутствие треугольников в G' следует из считающей леммы 2.3.1. Отметим, что граф G' не получается выкидыванием рёбер из графа G. Про G' надо думать как про шаблон выкидывания, который указывает, какие рёбра выкинуть из графа G, а какие оставить.

2.4 Лемма об удалении гиперграфа

Существует несколько версий доказательства леммы об удалении гиперграфа, мы будем следовать работе [15]. Некоторые технические детали доказательств мы пропустим и приглашаем читателя ознакомиться с ними в указанной работе.

Определение 2.4.1. Пусть J — конечное множество, а $d \in [1..|J|]$. Символом $\binom{J}{d}$ обозначим множество всех подмножеств J мощности d. Любое подмножество $\binom{J}{d}$ назовём d-равномерным гиперграфом на множестве вершин J.

Естественно, классические графы без петель и кратных рёбер суть просто 2-равномерные гиперграфы.

Определение 2.4.2. Четвёрку $(J, \{V_j\}_{j\in J}, d, H)$, где J — конечное множество, $\{V_j\}$ — набор конечных множеств, проиндексированных элементами J, $d \in [1..|J|]$, а H — d-равномерный гиперграф на множестве J, назовём гиперграфовой системой.

Пример 2.4.3. *Система $(\{1,2,3\}, \{V_1, V_2, V_3\}, 2, \Delta)$ — главный герой второй версии леммы об удалении треугольника (лемма 2.3.3).*

Пример 2.4.4. *При помощи системы* $(\{1,2,3,4\},\{V_1,V_2,V_3,V_4\},3,\binom{\{1,2,3,4\}}{3})$ *можно сформулировать лемму об удалении симплекса.*

О гиперграфовой системе надо думать как о дополнительной структуре на вероятностном пространстве $V=\prod_{j\in J}V_j$ (как обычно, мы снабжаем это множество алгеброй всех множеств и равномерной вероятностной мерой). О множествах V_j полезно думать как о множествах значения j-ой координаты. С другой стороны, V_j — множество вершин j-ой доли гиперграфа.

Определение 2.4.5. Пусть $e\subset J$ — некоторое множество. Символом $\mathcal{A}_e$ будем обозначать алгебру подмножеств V, зависящих лишь от координат, номер которых принадлежит множеству e.

Как мы видели в предыдущих параграфах, удобно интерпретировать множество рёбер графа как случайное событие. Например, задать множество E_{12} рёбер между вершинами долей V_1 и V_2 — это то же самое, что задать произвольное подмножество множества $V_1\times V_2$. Однако, уже в лемме 2.3.3 у нас было три доли. Чтобы работать на одном вероятностном пространстве, удобно определить E_{12} как событие, не зависящее от третьей координаты (то есть, взять "старое" множество E_{12} и заменить его множеством $E_{12}\times V_3$ в случае леммы 2.3.3). Иными словами, множество рёбер между долями V_1 и V_2 есть событие на вероятностном пространстве $V_1\times V_2\times V_3$, измеримое относительно алгебры $\mathcal{A}_{12}$. Аналогичным образом, в примере 2.4.4 множества, измеримые относительно алгебры $\mathcal{A}_{\{1,2,3\}}$, можно понимать как множества гиперрёбер между вершинами первой, второй и третьей долей гиперграфа.

Лемма 2.4.6 (Лемма об удалении гиперграфа)**.** *Для всяких чисел* $|J|\in\mathbb{N}$ *и* $\varepsilon>0$*, существует число* δ *со следующим свойством. Для всякой гиперграфовой системы* $(J,\{V_j\}_{j\in J},d,H)$ *и для всякого выбора множеств* $E_e\in\mathcal{A}_e$*,* $e\in H$*, такого что* $\mathbb{E}\prod_e\chi_{E_e}<\delta$*, существуют множества* $E'_e\in\mathcal{A}_e$ *со следующими свойствами:*

1) *их пересечение пусто, то есть* $\cap_{e\in H}E'_e$*;*
2) *для всякого гиперребра* $e\in H$ *имеет место соотношение* $\mathbb{E}\chi_{E_e\setminus E'_e}\leqslant\varepsilon$*;*
3) *существуют алгебры* $\mathcal{B}_i\subset\mathcal{A}_i$*, пронумерованные подмножествами* J *мощности не более* $d-1$*, такие что* $E'_e\in\bigvee_{i\subset e}\mathcal{B}_i$ *и сложности алгебр* $\mathcal{B}_i$ *ограничены некоторым числом, зависящим лишь от* ε*.*

Определение 2.4.7. Сложностью алгебры назовём наименьшее число множеств, порождающих эту алгебру. Обозначать сложность алгебры $\mathcal{A}$ будем $\operatorname{compl}.A$.

Упражнение 2.4.1. *Докажите, что сложность алгебры* $\mathcal{A}$ *не превосходит* $\log_2\lceil\log_2|\mathcal{A}|\rceil+1$.

Следствие 2.4.8. *Пусть* $B\subset[1..N]^d$ *— конечное множество плотности хотя бы* $\nu>0$*. Если число* N *достаточно велико (в зависимости от* ν*), то множество* B *содержит прямоугольный симплекс вида*

$$\Big\{x,(x_1+k,x_2,x_3,\dots,x_d),(x_1,x_2+k,x_3,\dots,x_d),\dots,(x_1,x_2,\dots,x_d+k)\Big\}. \tag{2.4.1}$$

Доказательство этого следствия — почти точное повторение вывода теоремы Рота из леммы об удалении треугольника, приведённого в конце параграфа 2.1.

Доказательство. Построим гиперграфову систему. Положим $J:=[1..d+1]$, $d:=d$, $H:=\binom{\{1..d+1\}}{d}$ (то есть, H есть $(d+1)$-мерный симплекс). В качестве $V_1,V_2,\dots,V_d$ выберем гиперплоскости пространства $\mathbb{R}^d$, параллельные координатным:

$$V_j=\{v_{js}\mid s\in[1..N]\},\quad\text{где } v_{js}=\{x\in\mathbb{R}^d\mid x_j=s\}.$$

В качестве множества V_{d+1} выберем гиперплоскости, ортогональные вектору $(1,1,1,\dots,1)$:

$$V_{(d+1)s} = \{v_{(d+1)s} \mid s \in [1..dN]\}, \quad \text{где } v_{(d+1)s} = \Big\{x \in \mathbb{R}^d \,\Big|\, \sum_j x_j = s\Big\}.$$

Отметим, что произвольный выбор d гиперплоскостей из разных долей даст набор из d гиперплоскостей общего положения. Стало быть, они пересекаются по точке. Нетрудно видеть, что эта точка целочисленна. Таким образом, для всякого ребра $e_j \in H$, $e_j = \{1,2,\dots,(j-1),(j+1),\dots,d+1\}$, построим множество E_{e_j} согласно формуле

$$E_{e_j} = \left\{ \begin{pmatrix} v_{1s_1}, v_{2s_2}, \dots, v_{(j-1)s_{j-1}}, \\ v_{(j+1)s_{j+1}}, \dots, v_{(d+1)s_{d+1}} \end{pmatrix} \,\middle|\, \begin{array}{r} \text{общая точка гиперплоскостей } v_{1s_1}, v_{2s_2}, \dots, v_{(j-1)s_{j-1}}, \\ v_{(j+1)s_{j+1}}, \dots, v_{(d+1)s_{d+1}} \text{ лежит в множестве } B \end{array} \right\}.$$

Отметим, что $(d+1)$-мерный симплекс в таком случае соответствует как раз прямоугольному симплексу, который мы ищем, кроме случая вырожденного симплекса (случай $k=0$ в формуле (2.4.1)). Положим $\varepsilon < \frac{\nu}{d^2+d}$ и предположим противное, пусть в множестве A нет нетривиальных симплексов. Выберем число N большим, чем число δ^{-1}. Отметим, что в построенном гиперграфе число $(d+1)$-мерных симплексов равно мощности B и поэтому,

$$\mathbb{E}\prod_{e_j} \chi_{E_{e_j}} = \frac{|A|}{dN^{d+1}} \leqslant \frac{1}{dN} < \delta.$$

Применим лемму 2.4.6 и посмотрим на гиперграф с гиперрёбрами $E_{e_j} \setminus E'_{e_j}$. Отметим, что тривиальные $(d+1)$-мерные симплексы дизъюнктны по гиперрёбрам (так как любая точка задаётся однозначно проходящими через неё d гиперплоскостями общего положения). Стало быть, если $\cap_{e_j \in H} E'_{e_j} = \varnothing$, то мы удалили хотя бы $|A|$ различных гиперрёбер, и стало быть,

$$\sum_{j=1}^{d+1} \mathbb{E}\chi_{E_{e_j}\setminus E'_{e_j}} \geqslant \frac{|A|}{dN^d} \geqslant \frac{\nu}{d} > (d+1)\varepsilon.$$

Для какого-то j получилось противоречие. □

Упражнение 2.4.2. *Рассмотрев множество* $B = \{x \in [1..N]^d \mid x_1 + 2x_2 + 3x_3 + \ldots + dx_d \in A\}$, *выведите теорему Семереди 2.1.1 из следствия 2.4.8.*

12.11.2018

2.5 Лемма регулярности для гиперграфов

Основную сложность в доказательстве леммы 2.4.6 представляет нахождение удобной формулировки леммы регулярности: с одной стороны, она не может быть слишком сильной, а с другой стороны, должен найтись правильный аналог считающей леммы 2.3.1, который в комбинации с ней даст доказательство леммы об удалении гиперграфа. Формулировка леммы довольно громоздкая, мы будем приближаться к ней постепенно. Но сначала нам нужно определить понятие регулярного разбиения, или регулярной алгебры.

Определение 2.5.1. Пусть H есть d-равномерный гиперграф. Границей ∂e гиперребра $e \in H$ назовём множество всех подмножеств $f \subset e$, таких что $|f| = |e|-1$. Границей ∂H назовём объединение границ всех гиперрёбер H.

Отметим, что ∂H есть $(d-1)$-равномерный гиперграф.

Определение 2.5.2. Пусть $(J, \{V_j\}_{j\in J}, d, H)$ — гиперграфова система, $e \in H$ — гиперребро, $E \in \mathcal{A}_e$ — событие, $\mathcal{B}$ — некоторая алгебра. Определим e-искажение множества E согласно формуле

$$\Delta_e(E \mid \mathcal{B}) = \sup_{E_f \in \mathcal{A}_f} \Big|\mathbb{E}\Big(\big(\chi_E - \mathbb{E}(\chi_E \mid \mathcal{B})\big) \prod_{f\in\partial e} \chi_{E_f}\Big)\Big|.$$

В формуле для искажения супремум выбирается по всем наборам E_f множеств, таких что $E_f \in \mathcal{A}_f$. Параметр e-искажения измеряет, насколько гиперграф E регулярен относительно разбиения $\mathcal{B}$.

Пример 2.5.3. *Рассмотрим случай $d = 2$, $J = \{1, 2\}$, $e = \{1, 2\}$. Выбор множества $E \in \mathcal{A}_{\{1,2\}}$ задаёт граф $G(V_1, V_2, E)$. Рассмотрим сначала случай, когда $\mathcal{B}$ — тривиальная алгебра. В таком случае,*

$$\Delta_e(E \mid \mathcal{B}) = \sup_{\substack{\tilde V_1 \subset V_1\\ \tilde V_2 \subset V_2}} \Big|\mathbb{E}\Big(\big(\chi_E - \mathbb{E}(\chi_E \mid \mathcal{B})\big)\chi_{\tilde V_1}\chi_{\tilde V_2}\Big)\Big| = \sup_{\substack{\tilde V_1 \subset V_1\\ \tilde V_2 \subset V_2}} \frac{|\tilde V_1||\tilde V_2|}{|V_1||V_2|}\Big|d(V_1, V_2) - d(\tilde V_1, \tilde V_2)\Big|.$$

Из этой формулы следует, что искажение мало тогда и только тогда, когда пара (V_1, V_2) регулярна. А именно, если пара (V_1, V_2) ε-регулярна, то

$$\Delta_e(E \mid \mathcal{B}) \leqslant \varepsilon. \tag{2.5.1}$$

В обратную сторону, если выполнено неравенство (2.5.1), то пара (V_1, V_2) $\varepsilon^{\frac14}$-регулярна. Пусть теперь $\mathcal{B} = \mathfrak{X}^1 \times \mathfrak{X}^2$, где X^1 и X^2 — разбиения множеств V_1 и V_2. В таком случае,

$$\Delta_e(E \mid \mathcal{B}) \asymp \frac{1}{|V_1||V_2|} \sum_{i,j} |X^1_i||X^2_j| \sup_{\substack{\tilde V_1 \subset X^1_i\\ \tilde V_2 \subset X^2_j}} \Big|d(V_1, V_2) - d(\tilde V_1, \tilde V_2)\Big|,$$

(так как функция $\mathbb{E}(E \mid \mathfrak{X}^1 \times \mathfrak{X}^2)$ постоянна на множествах разбиения, оптимизировать выражение $\Big|\mathbb{E}\Big(\big(\chi_E - \mathbb{E}(\chi_E \mid \mathcal{B})\big)\chi_{\tilde V_1}\chi_{\tilde V_2}\Big)\Big|$ можно на каждой клетке разбиения индивидуально). Поэтому, малость искажения соответствует регулярности разбиения $X^1 \times X^2$.

Лемма 2.5.4 (Аналог леммы 2.2.7)**.** *Пусть $\varepsilon \in (0, 1)$, $(J, \{V_j\}_{j\in J}, d, H)$ — гиперграфова система, $e \in H$ — гиперребро, $E \in \mathcal{A}_e$ — событие, а алгебры $\mathcal{B}_f \subset \mathcal{A}_f, f \in \partial e$, таковы что*

$$\Delta_e\Big(E \Big| \bigvee_{f\in\partial e} \mathcal{B}_f\Big) > \varepsilon.$$

Тогда существуют алгебры $\mathcal{B}'_f$, такие что $\mathcal{B}_f \subset \mathcal{B}'_f \subset \mathcal{A}_f$, и

1) $\operatorname{compl}. \mathcal{B}'_f \leqslant \operatorname{compl}. \mathcal{B}_f + 1$*;*

2) выполнено неравенство

$$\mathbb{E}\Big(\mathbb{E}\Big(\chi_E \Big| \bigvee_{f\in\partial e} \mathcal{B}'_f\Big)\Big)^2 - \mathbb{E}\Big(\mathbb{E}\Big(\chi_E \Big| \bigvee_{f\in\partial e} \mathcal{B}_f\Big)\Big)^2 \geqslant \varepsilon. \tag{2.5.2}$$

Доказывать эту лемму мы не будем — её доказательство полностью аналогично доказательству леммы 2.2.7. Прежде чем итерировать эту лемму, мы её немного обобщим. В будущем нам надо будет вести индукцию по d, поэтому логично заменить единственное множество $E \in \mathcal{A}_e$ подалгеброй алгебры $\mathcal{A}_e$ ограниченной сложности.

Лемма 2.5.5. *Пусть $\varepsilon, \delta \in (0,1)$, $m, M \in \mathbb{N}$, $(J, \{V_j\}_{j\in J}, d, H)$ — гиперграфова система. Пусть для каждого гиперребра $e \in H$ выбрана алгебра $\mathcal{B}_e \subset \mathcal{A}_e$, такая что*

$$\operatorname{compl}\mathcal{B}_e \leqslant m.$$

Пусть также для всякого гиперребра $f \in \partial H$ задана алгебра $\mathcal{B}_f \subset \mathcal{A}_f$, такая что

$$\operatorname{compl}\mathcal{B}_f \leqslant M.$$

Тогда существует константа $C = C(|J|, m, \varepsilon, \delta)$ и алгебры $\mathcal{B}'_f$, $\mathcal{B}_f \subset \mathcal{B}'_f \subset \mathcal{A}_f$, такие что выполнен один из двух сценариев:

1) для всякого ребра $e \in H$ и всякого множества $E \in \mathcal{B}_e$

- *неравенство* (2.5.2) *не выполнено,*
- *имеет место неравенство*
$$\Delta_e\Big(E \,\Big|\, \bigvee_{f\in\partial e} \mathcal{B}'_f\Big) \leqslant \delta; \tag{2.5.3}$$

2) существуют гиперребро $e \in H$ и множество $E \in \mathcal{B}_e$, такие что

- *выполнено неравенство* (2.5.2),
- *верна оценка*
$$\operatorname{compl}\mathcal{B}'_f \leqslant M + C(|J|, m, \varepsilon, \delta).$$

Доказательство. Построение алгебр $\mathcal{B}'_f$ проведём алгоритмически. Сначала положим $\mathcal{B}'_f := \mathcal{B}_f$ для всех $f \in \partial H$.

На каждом шаге алгоритм делает следующие действия. Если условие (2.5.3) выполнено для всех гиперрёбер $e \in H$ и всех множеств $E \in \mathcal{B}_e$, алгоритм останавливается. Если условие (2.5.2) выполнено для какого-то гиперребра $e \in H$ и какого-то множества $E \in \mathcal{B}_e$, то алгоритм тоже останавливается.

Если же условие (2.5.3) не выполнено для какого-то гиперребра $e \in H$ и какого-то множества $E \in \mathcal{B}_e$, то алгоритм при помощи леммы 2.5.4 с $\varepsilon := \delta$ (и алгебрами $\mathcal{B}'_f$ в роли алгебр $\mathcal{B}_f$) строит по алгебре $\mathcal{B}'_f$ алгебру $\mathcal{B}''_f$, такую что

$$\operatorname{compl}\mathcal{B}''_f \leqslant \operatorname{compl}\mathcal{B}'_f + 1,$$

и величина

$$\sum_{e\in H}\sum_{E\in\mathcal{A}_e} \mathbb{E}\Big(\mathbb{E}\Big(\chi_E \,\Big|\, \bigvee_{f\in\partial e} \mathcal{B}'_f\Big)\Big)^2 \tag{2.5.4}$$

увеличилась хотя бы на δ^2 при замене $\mathcal{B}'_f$ на $\mathcal{B}''_f$. После чего алгоритм полагает $\mathcal{B}'_f := \mathcal{B}''_f$ и переходит к следующему шагу.

Нетрудно видеть, что сумма (2.5.4) не превосходит $|H|2^{2^m}$, поэтому алгоритм совершит не более чем $C(|J|, m, \varepsilon, \delta)$ шагов. Ясно, что когда алгоритм остановится, будет выполнено одно из двух утверждений леммы. □

Замечание 2.5.6. *В этой лемме первая пара условий в двух сценариях, в некотором смысле, независима от второй. На первом месте можно ставить любое условие: в первом сценарии какой-то критерий выполнен для всех рёбер и всех множеств алгебры, а во втором сценарии для некоторого ребра и некоторого множества это условие не выполнено.*

Определение 2.5.7. Возрастающую функцию $F\colon \mathbb{R}_+ \to \mathbb{R}_+$ назовём функцией роста, если $F(x) \geqslant 1 + x$.

Лемма 2.5.8 (Предварительная лемма регулярности). *Пусть $\varepsilon \in (0,1)$, $m \in \mathbb{N}$, F — функция роста, а также зафиксирована гиперграфова система $(J, \{V_j\}_{j\in J}, d, H)$. Пусть для всех гиперрёбер $e \in H$ заданы алгебры $\mathcal{B}_e \subset \mathcal{A}_e$, такие что $\operatorname{compl}\mathcal{B}_e \leqslant m$. Существуют число M, константа $C = C(|J|, m, F, \varepsilon)$ и система пар алгебр $\mathcal{B}_f \subset \mathcal{B}'_f \subset \mathcal{A}_f$, $f \in \partial H$, такие что*

1) $F(m) \leqslant M \leqslant C(|J|, m, F, \varepsilon)$;

2) Для всякого гиперребра $f \in \partial H$ имеет место оценка $\operatorname{compl}\mathcal{B}_f \leqslant M$;

3) Для всякого гиперребра $e \in H$ и всякого множества $E \in \mathcal{B}_e$ неравенство (2.5.2) неверно;

4) Для всякого гиперребра $e \in H$ и всякого множества $E \in \mathcal{B}_e$ имеет место оценка

$$\Delta_e\Big(E \Big| \bigvee_{f\in\partial e} \mathcal{B}'_f\Big) \leqslant \frac{1}{F(M)}.$$

Замечание 2.5.9. *Классическая лемма регулярности находила нам алгебру ограниченной сложности $\log_2 M(\varepsilon)$, такую что разбиение по ней ε-регулярно. Лемма 2.5.8 строит нам пару алгебр, "расстояние" между которыми не превосходит ε^2, таких что вторая алгебра сверхрегулярна (т.к. функция F может расти очень быстро), а первая имеет ограниченную сложность. Оказывается, что такая конструкция более удобна для ведения индукции по параметру d, которая нам предстоит в следующей лемме.*

Доказательство леммы 2.5.8. Пары алгебр $\mathcal{B}_f, \mathcal{B}'_f$ будем строить при помощи алгоритма. Сначала положим $\mathcal{B}_f$ равными тривиальной алгебре.

На каждом шаге алгоритм получает набор алгебр $\mathcal{B}_f \subset \mathcal{A}_f$, $f \in \partial H$. Положим

$$M := \max(F(m), \{\operatorname{compl}\mathcal{B}_f\}_{f\in\partial H}); \quad \delta := \frac{1}{F(M)}$$

и применим лемму 2.5.5 к этому набору алгебр, ε и δ. Лемма построила нам набор алгебр $\mathcal{B}'_f$. Если они удовлетворяют первому сценарию, то алгоритм завершает свою работу. Если они удовлетворяют второй паре условий, то мы полагаем $\mathcal{B}_f := \mathcal{B}'_f$ для всякого $f \in \partial H$, и алгоритм переходит к следующему шагу.

Отметим, что на каждом шаге величина (2.5.4) (с алгебрами $\mathcal{B}_f$ вместо $\mathcal{B}'_f$) растёт хотя бы на ε^2. Поэтому алгоритм завершит свою работу за $C(|J|, m, \varepsilon)$ шагов. Нетрудно видеть, что набор пар алгебр $\mathcal{B}_f$, $\mathcal{B}'_f$, получившийся в результате работы алгоритма, удовлетворяет условиям леммы. □

Теперь мы готовы сформулировать полную лемму регулярности. Для этого определим j-равномерные графы H_j по правилу $H_d = H$ и $H_j = \partial H_{j+1}$.

Лемма 2.5.10 (Лемма регулярности для гиперграфов). *Пусть F — функция роста, $(J, \{V_j\}_{j\in J}, d, H)$ — гиперграфова система, $\{\mathcal{B}_e\}_{e\in H}$ — система алгебр сложности не более $M_d \in \mathbb{N}$. Существуют числа $M_0, M_1, \dots, M_{d-1}$, константа $C(|J|, M_d, F)$, а также системы алгебр $\mathcal{B}_f$, $\mathcal{B}'_f$, $f \in H_j$, такие что $\mathcal{B}_f \subset \mathcal{B}'_f \subset \mathcal{A}_f$ и*

1) $M_d \leqslant F(M_d) \leqslant M_{d-1} \leqslant F(M_{d-1}) \leqslant M_{d-2} \leqslant \dots \leqslant F(M_1) \leqslant M_0 \leqslant C(|J|, M_d, F)$;

2) Для всякого $j \in [0..d]$ и всех $f \in H_j$ имеет место оценка $\operatorname{compl}\mathcal{B}_f \leqslant M_j$;

3) Для всякого $j \in [0..d]$, всех гиперрёбер $e \in H_j$ и всех $E \in \mathcal{B}_e$ имеет место неравенство

$$\mathbb{E}\Big(\mathbb{E}\Big(\chi_E \Big| \bigvee_{f\in\partial e} \mathcal{B}'_f\Big)\Big)^2 - \mathbb{E}\Big(\mathbb{E}\Big(\chi_E \Big| \bigvee_{f\in\partial e} \mathcal{B}_f\Big)\Big)^2 \leqslant \frac{1}{F^2(M_j)};$$

4) Для всякого $j \in [0..d]$, всех гиперрёбер $e \in H_j$ и всех множеств $E \in \mathcal{B}_e$ имеет место неравенство

$$\Delta_e\Big(E \Big| \bigvee_{f \in \partial e} \mathcal{B}'_f\Big) \leqslant \frac{1}{F(M_0)}. \tag{2.5.5}$$

Доказательство. Будем вести индукцию по параметру d (не меняя множество J). Запасёмся функцией роста $\tilde{F}$, которую предстоит выбрать и применим лемму 2.5.8 с $m := M_d$, $\varepsilon := F(M_d)$ и $F := \tilde{F}$. Это даст нам набор пар алгебр $\mathcal{B}_f$, $\mathcal{B}'_f$, параметризованных $f \in H_{d-1}$, а также некоторое число M. Теперь к графу H_{d-1} и системе алгебр $\mathcal{B}_f$ применим предположение индукции с $M_{d-1} := M$. Это позволит построить числа M_j, $j = 0, 1, \ldots, d-1$, и соответствующие системы младших алгебр. Все утверждения будут выполнены по предположению индукции, кроме неравенств (2.5.5) в случае $j = d$. Однако, у нас имеются неравенства (обеспеченные леммой 2.5.8)

$$\Delta_e\Big(E \Big| \bigvee_{f \in \partial e} \mathcal{B}'_f\Big) \leqslant \frac{1}{\tilde{F}(M_{d-1})}, \quad e \in H_d, E \in \mathcal{B}_e.$$

Поэтому достаточно выбрать $\tilde{F}$ так, чтобы $\tilde{F}(M_{d-1}) \geqslant F(M_0)$. Определим функцию $\tilde{F}$ так, чтобы для всякого $M \in \mathbb{N}$ выполнялось неравенство $\tilde{F}(M) \geqslant F(M_0)$, где число M_0 определяется применением предположения индукции с $M_{d-1} := M$. Это позволит удовлетворить требуемому неравенству. Отметим, что $\tilde{F}$ зависит лишь от F и гиперграфа H, поэтому для всякого числа M_d число M_{d-1}, получающееся в результате применения леммы 2.5.8, будет ограничено некоторой абсолютной константой, зависящей лишь от M_d, H и F. А стало быть, и число M_0 тоже ограничено константой, зависящей от тех же параметров. □

19.11.2018

2.6 Форумлировка считающей леммы и доказательство леммы об удалении гиперграфа

В этом параграфе мы будем работать с гиперграфами, к которым уже применена лемма регулярности 2.5.10. Как обычно, мы будем черпать вдохновение из классического случая. При доказательстве леммы об удалении треугольника 2.1.4, мы "выбрасывали" из множества E те части, которые попали в "маленькие" или нерегулярные атомы алгебры $(\mathfrak{X} \times \mathfrak{X}) \bigvee \{\varnothing, V, E, \bar{E}\}$. В случае гиперграфов мы будем действовать точно также.

Рассмотрим "объемлющую" алгебру $\bigvee\limits_{\substack{0 \leqslant j \leqslant d \\ e \in H_j}} \mathcal{B}_e$. Нетрудно видеть, что любой её атом можно представить в виде

$$\bigcap_{\substack{0 \leqslant j \leqslant d \\ e \in H_j}} A_e, \quad A_e \text{ — атом алгебры } \mathcal{B}_e.$$

С другой стороны, для каждого набора атомов $\{A_e\}_{\substack{0 \leqslant j \leqslant d \\ e \in H_j}}$, их пересечение есть либо атом объемлющей алгебры, либо пустое множество.

Удобно ввести обозначение $\tilde{H}$ для "объемлющего" гиперграфа:

$$\tilde{H} = \bigcup_{0 \leqslant j \leqslant d} H_j.$$

Отметим, что гиперграф $\tilde{H}$ неоднороден.

Определение 2.6.1. Набор атомов $\{A_e\}_{e\in\tilde H}$ алгебр $\mathcal{B}_e$, $e\in\tilde H$, назовём хорошим, если выполнены два условия

$$\forall e\in\tilde H\qquad P\Big(A_e\cap\Big(\bigcap_{f\in\partial e}A_f\Big)\Big)\geqslant\frac{1}{\log F(M_j)}P\Big(\bigcap_{f\in\partial e}A_f\Big);\tag{2.6.1}$$

$$\forall e\in\tilde H,E\in\mathcal{B}_e\qquad\mathbb{E}\bigg(\Big[\mathbb{E}\Big(\chi_E\Big|\bigvee_{f\in\partial e}\mathcal{B}'_f\Big)-\mathbb{E}\Big(\chi_E\Big|\bigvee_{f\in\partial e}\mathcal{B}_f\Big)\Big]^2\prod_{f\subsetneq e}\chi_{A_f}\bigg)\leqslant\frac{1}{F(M_j)}P\Big(\bigcap_{f\subsetneq e}A_f\Big).\tag{2.6.2}$$

Замечание 2.6.2. *Появление логарифма* $\log F(M_j)$ *в формуле* (2.6.1) *весьма случайно. Важно лишь что эта величина много больше* M_j *(если функция* F *растёт достаточно быстро) и меньше, чем любая степень* $F(M_j)$*.*

Отметим также, что в формуле (2.6.2) *речь идёт о пересечении атомов всех алгебр, подчинённых ребру* e*.*

Пример 2.6.3. *Рассмотрим случай* $J=\{1,2\}$*,* $d=2$ *и сравним требование* (2.6.1) *с требованиями, которые мы предъявляли к хорошим атомам в классическом случае. В этом случае*

$$\mathcal{B}_{\{1,2\}}=\{\varnothing,V,E_{12},\bar E_{12}\},\quad\mathcal{B}_1=\mathfrak{X}_1\times\{\varnothing,V_2\},\mathcal{B}_2=\{\varnothing,V_1\}\times\mathfrak{X}_2,$$

где X_1 *и* X_2 *— разбиения множеств* V_1 *и* V_2 *соответственно. Атом объемлющей алгебры — это либо* (E,X_i^1,X_j^2)*, либо* $(\bar E,X_i^1,X_j^2)$*, где* X_i^1 *и* X_j^2 *— элементы разбиений* X_1 *и* X_2*, умноженные на* V_2 *и* V_1 *соответственно. Пусть наш атом —* (E,X_i^1,X_j^2)*. В таком случае, условие* (2.6.1) *переписывается в виде*

$$P\big(E\cap(X_i^1\times X_j^2)\big)\geqslant\frac{1}{\log F(M_2)}P(X_i^1\times X_j^2);$$
$$P(X_i^1\times V_2)\geqslant\frac{1}{\log F(M_1)},P(V_1\times X_j^2)\geqslant\frac{1}{\log F(M_1)}.$$

Вторая строчка следует из того, что граница точки — пустое множество. Отметим, что первая строчка соответствует требованию $d(X_i^1,X_j^2)\geqslant\frac{1}{\log F(M_2)}$*. Поэтому новые требования* (2.6.1) *соответствуют требованиям 2 и 3 доказательства леммы 2.1.4.*

Определение 2.6.4. Пусть $e\in\tilde H$ и A_e — атом алгебры $\mathcal{B}_e$. Рассмотрим множество "плохих" наборов атомов

$$\Pi_{e,A_e}=\Big\{\{A_f\}_{f\subsetneq e}\;\Big|\;\text{для этого набора }\{A_f\}\text{ не выполнено либо условие (2.6.1), либо условие (2.6.2)}\Big\}.$$

Определим теперь множество B_{e,A_e}:

$$B_{e,A_e}=\bigcup_{\{A_f\}\in\Pi_{e,A_e}}\Big(\bigcap_{f\subsetneq e}A_f\Big).$$

Отметим, что при определении множества Π_{e,A_e} мы проверяем условия (2.6.1) и (2.6.2) только с данным ребром e и атомом $A_e\in\mathcal{B}_e$, выбирая те наборы "младших" атомов, для которых одно из этих условий не выполнено. Также нетрудно видеть, что

$$B_{e,A_e}\in\bigvee_{f\subsetneq e}\mathcal{B}_f\tag{2.6.3}$$

Отметим, что набор $\{A_f\}_{f\in\tilde H}$ атомов хороший тогда и только тогда, когда для всякого $e\in\tilde H$ множество $\cap_{f\subsetneq e}A_f$ не лежит в множестве B_{e,A_e}. Следующая лемма, в некотором смысле, утверждает, что большинство наборов атомов — хорошие.

Лемма 2.6.5. *Для всякого $e \in \tilde{H}$ и всякого $A_e \in \mathcal{B}_e$, выполнено неравенство*

$$P(A_e \cap B_{e,A_e}) = O\Big(\frac{1}{\log F(M_j)}\Big).$$

Доказательство. Сначала оценив вклад в множество B_{e,A_e} тех наборов атомов, для которых не выполнено условие (2.6.1):

$$\sum_{\substack{\{A_f\}_{f\subsetneq e}\\ \text{(2.6.1) неверно}}} P\Big(A_e \cap \Big(\bigcap_{f\in\partial e} A_f\Big)\Big) \leqslant \frac{1}{\log F(M_j)} \sum_{\substack{\{A_f\}_{f\subsetneq e}\\ \text{(2.6.1) неверно}}} P\Big(\bigcap_{f\in\partial e} A_f\Big) \leqslant \frac{1}{\log F(M_j)},$$

так как множества $\bigcap_{f\in\partial e} A_f$ не пересекаются для разных наборов атомов (здесь надо быть аккуратным — мы суммируем по всем наборам $\{A_f\}_{f\in\partial e}$, для которых не выполнено условие (2.6.1), а вовсе не по всем плохим атомам, чтобы избежать многократного суммирования одного и того же). Теперь оценим вклад наборов атомов, нарушающих условие (2.6.2):

$$\sum_{\substack{\{A_f\}_{f\subsetneq e}\\ \text{(2.6.2) неверно}}} P\Big(A_e \cap \Big(\bigcap_{f\subsetneq e} A_f\Big)\Big) \leqslant$$

$$F(M_j) \sum_{\substack{\{A_f\}_{f\subsetneq e}\\ \text{(2.6.2) неверно}}} \mathbb{E}\Big(\Big[\mathbb{E}\Big(\chi_E \Big| \bigvee_{f\in\partial e} \mathcal{B}'_f\Big) - \mathbb{E}\Big(\chi_E \Big| \bigvee_{f\in\partial e} \mathcal{B}_f\Big)\Big]^2 \prod_{f\subsetneq e} \chi_{A_f}\Big) \leqslant$$

$$F(M_j)\mathbb{E}\Big[\mathbb{E}\Big(\chi_E \Big| \bigvee_{f\in\partial e} \mathcal{B}'_f\Big) - \mathbb{E}\Big(\chi_E \Big| \bigvee_{f\in\partial e} \mathcal{B}_f\Big)\Big]^2 \overset{\text{Лем. 2.5.10}}{\leqslant} \frac{1}{F(M_j)} \lesssim \frac{1}{\log F(M_j)}.$$

□

Наконец, мы готовы сформулировать аналог считающей леммы 2.3.1.

Лемма 2.6.6. *Пусть $(J, \{V_j\}_{j\in J}, d, H)$ — гиперграфова система, F — функция роста. Пусть к этой гиперграфовой системе и алгебрам $\mathcal{B}_e$ сложности не более M_d применена лемма 2.5.10. Пусть набор атомов $A_e \in \mathcal{B}_e$, $e \in \tilde{H}$ — хороший. Если функция F растёт достаточно быстро (в зависимости от параметра $|J|$), то*

$$P\Big(\bigcap_{e\in\tilde{H}} A_e\Big) = \Big(1 + o_{M_d\to\infty}(1)\Big) \prod_{e\in\tilde{H}} P\Big(A_e \Big| \bigcap_{f\in\partial e} A_f\Big) + O_{|J|,M_d}\Big(\frac{1}{F(M_0)}\Big). \tag{2.6.4}$$

Пример 2.6.7. *Посмотрим, что эта лемма означает в классическом случае $J = \{1,2,3\}$, $H = \Delta$, рассмотенном ранее в лемме 2.3.1. Символом E_{ij} будем обозначать подмножество V, полученное умножением множества рёбер между долями V_i и V_j (то есть, некоторого подмножества $V_i \times V_j$) и множества V_k (i,j,k здесь различны). Тогда мы можем сформировать "исходные" алгебры $\mathcal{B}_e$, где e — ребро треугольника:*

$$\mathcal{B}_{\{i,j\}} = \{\varnothing, V, E_{ij}, \bar{E}_{ij}\}.$$

Алгебры $\mathcal{B}_{\{1\}}$, $\mathcal{B}_{\{2\}}$ и $\mathcal{B}_{\{3\}}$ задаются разбиениями X_1, X_2, X_3 множеств V_1, V_2, V_3 соответственно. В этом случае атом объемлющей алгебры — это набор $(\tilde{E}_{12}, \tilde{E}_{13}, \tilde{E}_{23}, X_i^1, X_j^2, X_k^3)$, где $\tilde{E}_{ij}$ — либо E_{ij}, либо его дополнение, а X_i^1, X_j^2, X_k^3, — атомы разбиений X_1, X_2, X_3 соответственно. В таком случае, формула (2.6.4) *примет вид*

$$P\Big(E_{12} \cap E_{13} \cap E_{23} \cap \Big(X_i^1 \times X_j^2 \times X_k^3\Big)\Big) =$$
$$(1+o(1))P(E_{12} \mid X_i^1 \times X_j^2)P(E_{13} \mid X_i^1 \times X_k^3)P(E_{23} \mid X_j^2 \times X_k^3)|X_1||X_2||X_3| + O(\ldots) =$$
$$(1+o(1))d(X_1,X_2)d(X_1,X_3)d(X_2,X_3)|X_1||X_2||X_3| + O(\ldots).$$

Главный член в этой формуле совпадает с главным членов в оценке леммы 2.3.1.

Доказательство леммы 2.6.6 повторяет доказательство леммы 2.3.1, и мы отсылаем читателя к оригинальной статье [15]. Мы же выведем из этой леммы лемму об удалении гиперграфа.

Доказательство леммы 2.4.6. Выберем достаточно быструю функцию роста F, применим лемму 2.5.10 к нашей гиперграфовой системе и алгебрам $\mathcal{B}_e = \{\varnothing, V, E_e, \bar{E}_e\}$ и получим систему пар алгебр, удовлетворяющим выводам леммы.

Покажем, что если число δ достаточно мало (в зависимости от функции F), то в объемлющей алгебре $\bigvee_{f\in\tilde{H}} \mathcal{B}_f$ не будет наборов хороших атомов с $A_e = E_e$ для всех $e \in H$. Предположим противное, пусть нашёлся хороший набор атомов $\{A_e\}_{e\in\tilde{H}}$, $A_e \in \mathcal{B}_e$. В таком случае, согласно лемме 2.6.6,

$$P\Big(\bigcap_{e\in\tilde{H}} A_e\Big) = \Big(1 + o_{M_d\to\infty}(1)\Big)\prod_{e\in\tilde{H}} P\Big(A_e \;\Big|\; \bigcap_{f\in\partial e} A_f\Big) + O_{|J|,M_d}\Big(\frac{1}{F(M_0)}\Big) \overset{(2.6.1)}{\geqslant}$$
$$\Big(1 + o_{M_d\to\infty}(1)\Big)\prod_{0\leqslant j\leqslant d}\prod_{e\in H_j}\frac{1}{\log F(M_j)} + O_{|J|,M_d}\Big(\frac{1}{F(M_0)}\Big) \geqslant$$
$$\Big(1 + o_{M_d\to\infty}(1)\Big)\frac{1}{(\log F(M_0))^{O(|J|)}} + O_{|J|,M_d}\Big(\frac{1}{F(M_0)}\Big).$$

Поэтому можно взять число M_d настолько большим, чтобы первое слагаемое было строго положительно, и зафиксировать его. После чего взять функцию F достаточно быстрой, чтобы $M_0 \geqslant F(M_d)$ было столь велико, чтобы второе слагаемое было сильно меньше первого при любом выборе $F(M_0) \geqslant M_0$. Таким образом, при надлежащем выборе параметров, вероятность хорошего атома объемлющей алгебры отделена от нуля. Стало быть, если δ достаточно мало (в зависимости от M_d и F), то хороших наборов атомов, таких что $A_e = E_e$ для гиперрёбер $e \in H$, просто нет.

Для всякого гиперребра $e \in H$ определим множество E'_e согласно формуле

$$E'_e = V \setminus \Big(B_{e,E_e} \cup \Big(\bigcup_{\substack{f\subsetneq e\\ f\in\tilde{H}}} A_f \cap B_{f,A_f}\Big)\Big).$$

Первое требование леммы 2.4.6 следует из того, что при достаточно малом δ нет хороших атомов, таких что $A_e = E_e$ для гиперрёбер $e \in H$. Третье требование следует из формулы (2.6.3) и леммы 2.5.10. Осталось проверить второе требование:

$$P(E_e \setminus E'_e) \leqslant P(E_e \cap B_{e,E_e}) + \sum_{f\subsetneq e}\sum_{\substack{A_f\\ \text{атом }\mathcal{B}_f}} P(A_f \cap B_{f,A_f}) \overset{\text{Лем. 2.6.5}}{\leqslant}$$
$$\frac{1}{\log F(M_d)} + \sum_{j<d}\sum_{f\in H_j}\sum_{\substack{A_f\\ \text{атом }\mathcal{B}_f}}\frac{1}{\log F(M_j)} = \sum_j O(M_j)\frac{1}{\log F(M_j)},$$

поэтому при выборе достаточно шустрой функции F эта величина будет меньше ε. □

Глава 3

Эффективный поиск арифметических прогрессий

Рассуждения, опирающиеся на лемму регулярности, обычно дают очень плохие оценки. Оказывается, что если в случае с самой леммой регулярности это неизбежно, то в теореме Семереди, как показал Гауэрс, их можно существенно улучшить. Эта глава излагается по работе [8] (см. также [9]) и обзорам [13] и [14].

3.1 Нормы Гауэрса

21.4.2022

Символом $\mathcal{C}$ обозначим операцию комплексного сопряжения. Натуральные числа от 1 до 2^d нам будет удобно нумеровать вершинами двоичного куба $\{0,1\}^d$. Если $w \in \{0,1\}^d$, то пусть $|w| = \sum_1^d w_j$. Как обычно, N — большое простое число.

Определение 3.1.1. Пусть $\{f_w\}_{w\in\{0,1\}^d}$ — набор комплекснозначных функций на группе $\mathbb{Z}_N$. Мультилинейной формой (или скалярным произведением) Гауэрса степени d называется следующая форма:

$$\langle \{f_w\}_w \rangle_{U^d} = N^{-d-1} \sum_{\substack{x\in\mathbb{Z}_N \\ h\in\mathbb{Z}_N^d}} \prod_{w\in\{0,1\}^d} \mathcal{C}^{|w|} f_w(x + w\cdot h), \tag{3.1.1}$$

где $w \cdot h = \sum_{j=1}^d w_j h_j$.

Например, если $d = 1$, то

$$\langle \{f_0, f_1\} \rangle_{U^1} = N^{-2} \sum_{x,h\in\mathbb{Z}_N} f_0(x)\overline{f_1(x+h)} = N^{-2} \sum f_0 \sum \bar{f}_1. \tag{3.1.2}$$

В случае $d = 2$ формула становится сложнее:

$$\langle \{f_{00}, f_{10}, f_{01}, f_{11}\} \rangle_{U^2} = N^{-3} \sum_{x,h_1,h_2} f_{00}(x)\overline{f_{10}(x+h_1)f_{01}(x+h_2)}f_{11}(x+h_1+h_2). \tag{3.1.3}$$

Введём обозначение

$$\|f\|_{U^d} = \Big(\langle \underbrace{f, f, \dots, f}_{2^d \text{ раз}} \rangle_{U^d}\Big)^{2^{-d}}. \tag{3.1.4}$$

Мы докажем, что в случае $d \geqslant 2$ только что определённое выражение — действительно норма. Начнём с меньшего.

Предложение 3.1.2. *Формула* (3.1.4) *корректна: выражение в правой части, степень которого вычисляется, не отрицательно.*

Доказательство. Заметим, что сумму по переменной h_d можно вычислить:

$$\langle \underbrace{f, f, \dots, f}_{2^d \text{ раз}} \rangle_{U^d} = N^{-d-1} \sum_{h \in \mathbb{Z}_N^{d-1}} \Big| \sum_{x \in \mathbb{Z}_N} \prod_{w \in \{0,1\}^{d-1}} \mathcal{C}^{|w|} f(x + w \cdot h) \Big|^2, \tag{3.1.5}$$

это вычисление обобщает формулу (3.1.2). □

Выписав аналогичную формулу для различных функций f_w и применяя неравенство КБШ, получим

$$\Big| \langle \{f_w\}_w \rangle_{U^d} \Big| \leqslant \sqrt{\langle \{g_w\}_w \rangle_{U^d}} \sqrt{\langle \{h_w\}_w \rangle_{U^d}}, \tag{3.1.6}$$

где наборы функций $\{g_w\}_w$ и $\{h_w\}_w$ строятся по набору $\{f_w\}_w$ следующим образом:

$$g_w = f_{w'}; \qquad h_w = f_{w''}, \qquad w \in \{0, 1^d\}, \tag{3.1.7}$$

точка w' получается из точки w заменой последней координаты на 0, а точка w'' — заменой последней координаты на 1. Проводя аналогичные манипуляции для других координат, приходим к неравнству

$$\Big| \langle \{f_w\}_w \rangle_{U^d} \Big| \leqslant \prod_{w \in \{0,1\}^d} \|f_w\|_{U^d}. \tag{3.1.8}$$

Раскрывая скобки в выражениях

$$\langle \underbrace{f + g, f + g, \dots, f + g}_{2^d \text{ раз}} \rangle_{U^d} \qquad \text{и} \qquad \Big(\|f\|_{U^d} + \|g\|_{U^d} \Big)^{2^d} \tag{3.1.9}$$

и пользуясь неравенством (3.1.8), можно показать, что функция $\| \cdot \|_{U^d}$ — полунорма.

Применение КБШ к правой части формулы (3.1.5),

$$N^{-d-1} \sum_{h \in \mathbb{Z}_N^{d-1}} \Big| \sum_{x \in \mathbb{Z}_N} \prod_{w \in \{0,1\}^{d-1}} \mathcal{C}^{|w|} f(x + w \cdot h) \Big|^2 \geqslant \Big(N^{-d} \sum_{\substack{x \in \mathbb{Z}_N \\ h \in \mathbb{Z}_N^{d-1}}} \prod_{w \in \{0,1\}^{d-1}} \mathcal{C}^{|w|} f(x + w \cdot h) \Big)^2, \tag{3.1.10}$$

влечёт неравенство монотонности для норм Гауэрса

$$\|f\|_{U^d} \leqslant \|f\|_{U^{d+1}}. \tag{3.1.11}$$

Поэтому, если $\| \cdot \|_{U^2}$ — норма, то и при больших d функция $\| \cdot \|_{U^d}$ — норма. Запишем:

$$\|f\|_{U^2}^4 = N^{-3} \sum_h \Big| \sum_x f(x) \overline{f(x + h)} \Big|^2 = N^{-3} \sum_h \Big| f * \overline{f(-\cdot)}(-h) \Big|^2 = N^{-4} \sum_\zeta |\hat{f}(\zeta)|^4. \tag{3.1.12}$$

Если это выражение обратилось в ноль, то $\hat{f} \equiv 0$, а тогда и $f \equiv 0$. Следовательно, мы доказали, что функция $\| \cdot \|_{U^d}$ — действительно норма при $d \geqslant 2$.

Определение 3.1.3. Пусть $\eta \in [0, 1]$. Функция $f \colon \mathbb{Z}_N \to \mathbb{C}$ называется η-равномерной, если $\|f\|_{U^2} \leqslant \eta$ и квадратично η-равномерной, если $\|f\|_{U^3} \leqslant \eta$. Множество $A \subset \mathbb{Z}_N$ назовём (квадратично) η-равномерным, если его балансовая функция $f_A(\cdot) = \chi_A(\cdot) - |A|/N$ (квадратично) η-равномерна.

Следующая лемма является, в некотором роде, аналогом считающей леммы 2.3.1.

Лемма 3.1.4. *Пусть A, B, C — подмножества группы $\mathbb{Z}_N$ плотностей α, β, γ соответственно. Если множество C является η-равномерным, то*

$$\Big| \sum_{r \in \mathbb{Z}_N} |A \cap (B + r) \cap (C + 2r)| - \alpha\beta\gamma N^2 \Big| \leqslant \eta N^2. \tag{3.1.13}$$

Доказательство. Перепишем интересующее нас выражение через балансовую функцию множества C:

$$|A \cap (B + r) \cap (C + 2r)| = \sum_{x \in \mathbb{Z}_N} \chi_A(x)\chi_B(x + r)\chi_C(x + 2r) = \sum_{x \in \mathbb{Z}_N} \chi_A(x)\chi_B(x + r)f_C(x + 2r) + \gamma \sum_{x \in \mathbb{Z}_N} \chi_A(x)\chi_B(x + r), \tag{3.1.14}$$

и поэтому, так как $\sum_{x,r} \chi_A(x)\chi_B(x + r) = \alpha\beta N^2$, достаточно доказать оценку

$$\Big| \sum_{x,r} \chi_A(x)\chi_B(x + r)f_C(x + 2r) \Big| \leqslant \eta N^2. \tag{3.1.15}$$

Сделаем замену $y = x+r$ и воспользуемся соотношением между свёрткой и преобразованием Фурье:

$$\sum_{x,y} \chi_A(x)\chi_B(y)f_C(2y - x) = \sum_y (\chi_A * f_C)(2y)\chi_B(y) = N^{-1} \sum_\zeta \hat{\chi}_A(\zeta/2)\hat{f}_C(\zeta/2)\overline{\hat{\chi}_B(\zeta)}. \tag{3.1.16}$$

Согласно формуле (3.1.12), $\|\hat{f}\|_{L_\infty} \leqslant \|\hat{f}\|_{L_4} = N\|f\|_{U_2}$. Применяя неравенство КБШ и теорему Планшереля, получаем

$$N^{-1}\Big| \sum_\zeta \hat{\chi}_A(\zeta/2)\hat{f}_C(\zeta/2)\overline{\hat{\chi}_B(\zeta)} \Big| \leqslant \eta N \Big(N^{-1} \sum_\zeta |\hat{\chi}_A(\zeta/2)|^2 \Big)^{\frac{1}{2}} \Big(N^{-1} \sum_\zeta |\hat{\chi}_B(\zeta)|^2 \Big)^{\frac{1}{2}} \leqslant \eta N\sqrt{\alpha N \beta N} \leqslant \eta N^2. \tag{3.1.17}$$

□

Следствие 3.1.5. *Пусть $\eta < \alpha^3/2$, а число N велико настолько, что $N < \alpha^3 N^2/2$. Всякое η-равномерное подмножество группы $\mathbb{Z}_N$ плотности α содержит нетривиальную арифметическую прогрессию длины 3.*

Лемма 3.1.6. *Пусть $D \subset \mathbb{Z}_N$ — квадратично η-равномерное множество плотности δ. Тогда для всех, кроме не более чем $\eta^2 N$, значений $k \in \mathbb{Z}_N$ справедливо неравенство*

$$||D \cap (D + k)| - \delta^2 N| \leqslant \eta N, \tag{3.1.18}$$

и для всех, кроме не более чем $2\eta^2 N$, значений $k \in \mathbb{Z}_N$, множество $D \cap (D + k)$ является 4η-равномерным.

Доказательство. Наши рассуждения будут основываться на тождестве

$$\chi_D(s)\chi_D(s + k) = \delta^2 + \delta f_D(s) + \delta f_D(s + k) + f_D(s)f_D(s + k), \qquad s, k \in \mathbb{Z}_N. \tag{3.1.19}$$

Согласно неравенству монотонности (3.1.11), $\|f\|_{U^2} \leqslant \eta$, то есть, ввиду формулы (3.1.5),

$$N^{-3} \sum_{k\in\mathbb{Z}_N} \Big| \sum_{x\in\mathbb{Z}_N} f_D(x) f_D(x+k)\Big|^2 \leqslant \eta^4. \tag{3.1.20}$$

Из формулы (3.1.19) следует, что

$$\Big||D\cap(D+k)| - \delta^2 N\Big| = \Big| \sum_{x\in\mathbb{Z}_N} f_D(x) f_D(x+k)\Big|, \tag{3.1.21}$$

и первое утверждение леммы следует из неравенства (3.1.20) от противного. Пусть теперь $\Delta(f;k)(x) = f(x)\overline{f(x+k)}$. Тогда

$$\|f\|_{U^3} = \Big(N^{-1} \sum_{k\in\mathbb{Z}_N} \|\Delta(f;k)\|_{U^2}^4\Big)^{1/8}. \tag{3.1.22}$$

Следовательно, для не более чем $\eta^4 N$ значений k нарушается неравенство $\|\Delta(f_D;k)\|_{U^2} \leqslant \eta$. Выкинем из рассмотрения те элементы $k \in \mathbb{Z}_N$, для которых не выполнено либо это неравенство, либо (3.1.18). Останется хотя бы $(1-2\eta^2)N$ индексов k (так как $\eta \leqslant 1$), и для них

$$\Big\|\chi_D(\cdot)\chi_D(\cdot+k) - \frac{|D\cap(D+k)|}{N}\Big\|_{U^2} \leqslant \eta + \Big\|\chi_D(\cdot)\chi_D(\cdot+k) - \delta^2\Big\|_{U^2} \overset{(3.1.19)}{\leqslant}$$
$$\eta + 2\|f_D\|_{U^2} + \|\Delta(f_D;k)\|_{U^2} \leqslant 4\eta. \tag{3.1.23}$$

□

Лемма 3.1.7. *Пусть A, B, C, D — подмножества группы $\mathbb{Z}_N$ плотностей α, β, γ и δ соответственно. Пусть множества C и D квадратично η-равномерны. Предположим, что $\eta \leqslant \beta\gamma\delta/2$. Тогда*

$$\Big| \sum_{r\in\mathbb{Z}_N} \big|A\cap(B+r)\cap(C+2r)\cap(D+3r)\big| - \alpha\beta\gamma\delta N^2\Big| \leqslant 13\sqrt{\eta} N^2. \tag{3.1.24}$$

При доказательстве леммы мы будем пользоваться следующим простым фактом, утверждающим, что функция, для которой неравенство Коши–Буняковского–Шварца почти обращается в равенство, близка к постоянной. Докажите его в качестве упражнения.

Факт 3.1.8. *Пусть $f\colon \mathbb{Z}_N \to \mathbb{R}_+$ — неотрицательная функция, пусть $\|f\|_{L_1} = \omega N$, а $\|f\|_{L_2}^2 \leqslant (1+\varepsilon)\omega^2 N$. Тогда для всякого множества $A \subset \mathbb{Z}_N$ верно неравенство*

$$\Big| \sum_{s\in A} f(s) - \omega|A|\Big| \leqslant \sqrt{\varepsilon|A|N}\,\omega. \tag{3.1.25}$$

Доказательство леммы 3.1.7. Рассмотрим функцию f:

$$f(s) = \sum_{r\in\mathbb{Z}_N} \chi_B(s-r)\chi_C(s-2r)\chi_D(s-3r). \tag{3.1.26}$$

Мы докажем, что введённая функция f «плоская» в смысле факта 3.1.8. С вычислением L_1-нормы справиться легко:

$$\|f\|_{L_1} = \sum_{s,r} \chi_B(s-r)\chi_C(s-2r)\chi_D(s-3r) =$$
$$\sum_{s,r} \chi_B(s)\chi_C(s-r)\chi_D(s-2r) = \sum_r |B\cap(C+r)\cap(D+2r)|. \tag{3.1.27}$$

Так как множество D квадратично η-равномерно, лемма 3.1.4 показывает, что

$$\Big|\|f\|_{L_1} - \beta\gamma\delta N^2\Big| \leqslant \eta N^2. \tag{3.1.28}$$

Оценка L_2 нормы функции f сложнее:

$$\|f\|_{L_2}^2 = \sum_{s,r_1,r_2} \chi_B(s-r_1)\chi_C(s-2r_1)\chi_D(s-3r_1)\chi_B(s-r_2)\chi_C(s-2r_2)\chi_D(s-3r_2) =$$
$$\sum_{s,r,p} \chi_B(s-r)\chi_C(s-2r)\chi_D(s-3r)\chi_B(s-r-p)\chi_C(s-2r-2p)\chi_D(s-3r-3p) =$$
$$\sum_{s,r,p} \chi_{B\cap(B+p)}(s)\chi_{C\cap(C+2p)}(s-r)\chi_{D\cap(D+3p)}(s-2r). \tag{3.1.29}$$

Лемма 3.1.6 утверждает, что множество $D\cap(D+3p)$ является 4η-равномерным для всех, кроме не более чем $2\eta^2 N$, индексов p. Для таких индексов p, по лемме 3.1.4, имеем

$$\sum_{s,r} \chi_{B\cap(B+p)}(s)\chi_{C\cap(C+2p)}(s-r)\chi_{D\cap(D+3p)}(s-2r) \leqslant$$
$$\frac{|B\cap(B+p)||C\cap(C+2p)||D\cap(D+3p)|}{N} + 4\eta N^2. \tag{3.1.30}$$

Следовательно, так как $\eta^2 \leqslant \eta$,

$$\sum_{s,r,p} \chi_{B\cap(B+p)}(s)\chi_{C\cap(C+2p)}(s-r)\chi_{D\cap(D+3p)}(s-2r) \leqslant$$
$$\sum_{p} \frac{|B\cap(B+p)||C\cap(C+2p)||D\cap(D+3p)|}{N} + 6\eta N^3. \tag{3.1.31}$$

Согласно лемме 3.1.6, для всех, кроме не более чем $4\eta^2 N$, индексов p верны оба соотношения

$$|C\cap(C+2p)| \leqslant (\gamma^2+\eta)N \qquad \text{и} \qquad |D\cap(D+2p)| \leqslant (\delta^2+\eta)N. \tag{3.1.32}$$

Значит, справедлива оценка

$$\|f\|_{L_2}^2 \leqslant \sum_p \frac{|B\cap(B+p)||C\cap(C+2p)||D\cap(D+3p)|}{N} + 6\eta N^3 \leqslant$$
$$\sum_p \frac{|B\cap(B+p)|}{N}(\gamma^2+\eta)(\delta^2+\eta)N^2 + 10\eta N^3 =$$
$$\beta^2(\gamma^2+\eta)(\delta^2+\eta)N^3 + 10\eta N^3 \leqslant (\beta^2\gamma^2\delta^2+14\eta)N^3. \tag{3.1.33}$$

Применим теперь факт 3.1.8. Для этого положим 28.4.2022

$$\omega = \frac{\|f\|_{L_1}}{N}, \quad \text{тогда} \quad |\omega - \beta\gamma\delta N| \leqslant \eta N \tag{3.1.34}$$

благодаря оценке (3.1.28). Определим значение параметра ε соотношением

$$1+\varepsilon = \frac{\|f\|_{L_2}^2}{\omega^2 N} \overset{(3.1.33)}{\leqslant} \frac{(\beta^2\gamma^2\delta^2+13\eta)N^3}{(\beta\gamma\delta-\eta)^2N^3} = \frac{1+13\frac{\eta}{\beta^2\gamma^2\delta^2}}{(1-\frac{\eta}{\beta\gamma\delta})^2} \overset{(*)}{\leqslant} \Big(1+13\frac{\eta}{\beta^2\gamma^2\delta^2}\Big)\Big(1+6\frac{\eta}{\beta\gamma\delta}\Big), \tag{3.1.35}$$

если $\eta/(\beta\gamma\delta) < 1/2$; переход $(*)$ следует из элементарного неравенства $(1-x)^{-1} \leqslant 1+2x$ при $x \in (0,1/2)$. Следовательно, $\varepsilon \leqslant 58\eta/(\beta\gamma\delta)^2$. Совмещая факт 3.1.8 с оценкой (3.1.35), получаем

$$\Big|\sum_{s\in A} f(s) - \alpha\beta\gamma\delta N^2\Big| \leqslant |\omega - \beta\gamma\delta N| + \sqrt{\varepsilon\alpha N^2}\omega \leqslant \alpha\eta N^2 + \sqrt{\frac{58\eta}{(\beta\gamma\delta)^2}\alpha N^2}(\beta\gamma\delta+\eta)N = \\ \Big(\alpha\eta + \sqrt{58\alpha\eta}\big(1+\frac{\eta}{\beta\gamma\delta}\big)\Big)N^2 \leqslant \sqrt{\eta}\big(\alpha + \frac{3}{2}\sqrt{58\alpha}\big) \leqslant 13\sqrt{\eta}, \quad (3.1.36)$$

и, вспоминая определение функции f, приходим к желаемой оценке (3.1.24). □

Следствие 3.1.9. *Пусть $F \subset [0\,..\,N]$ — квадратично η-равномерное множество плотности α. Пусть $\eta \leqslant 10^{-8}\alpha^8$. Если число N достаточно велико, то множество F содержит нетривиальную арифметическую прогрессию длины 4, причём арифметическую прогрессию в $\mathbb{Z}$, а не в $\mathbb{Z}_N$.*

Доказательство. Положим $A := F \cap [2N/5\,..\,3N/5]$, $B := F \cap [2N/5\,..\,3N/5]$, $C := F$ и $D := F$. Покажем, что плотности множеств A и B не меньше, чем $\alpha/200$. Для этого рассмотрим вспомогательную функцию φ (это сглаженная характеристическая функция интервала $[2N/5\,..\,3N/5]$):

$$\varphi(s) = \frac{1}{N}\chi_{[-N/20..N/20]} * \chi_{[-N/20..N/20]}\Big(s + \frac{N-1}{2}\Big), \quad s \in \mathbb{Z}_N. \quad (3.1.37)$$

Так как $\|\varphi\|_{L_\infty} \leqslant 1$, достаточно доказать неравенство $\sum_{s\in\mathbb{Z}_N} \chi_F(s)\varphi(s) \geqslant \alpha N/200$. Перепишем, используя балансовую функцию множества F,

$$\sum_{s\in\mathbb{Z}_N} \chi_F(s)\varphi(s) \geqslant \frac{\alpha N}{100} - \Big|\sum_{s\in\mathbb{Z}_N} f_F(s)\varphi(s)\Big|. \quad (3.1.38)$$

Оценим второе слагаемое, используя теорему Планшереля:

$$\Big|\sum_{s\in\mathbb{Z}_N} f_F(s)\varphi(s)\Big| = \Big|\frac{1}{N}\sum_{\zeta\in\mathbb{Z}_N} \hat{f}_F(\zeta)\overline{\hat{\varphi}(\zeta)}\Big| \leqslant \frac{1}{N}\|\hat{f}_F\|_{L_\infty}\sum_{\zeta}|\hat{\varphi}(\zeta)|. \quad (3.1.39)$$

Отметим, что, так как φ — сдвиг функции с положительным преобразованием Фурье,

$$\frac{1}{N}\sum_{\zeta}|\hat{\varphi}(\zeta)| = \varphi\Big(-\frac{N-1}{2}\Big) \leqslant \frac{1}{10}. \quad (3.1.40)$$

Кроме того, $\|\hat{f}_F\|_{L_\infty} \leqslant \|\hat{f}_F\|_{L_4} = N\|f_F\|_{U^2} \leqslant N\eta$ согласно формуле (3.1.12) и неравенству монотонности для норм Гауэрса (3.1.11). Собирая эти оценки воедино, получаем

$$\Big|\sum_{s\in\mathbb{Z}_N} f_F(s)\varphi(s)\Big| \leqslant \frac{\eta N}{10}. \quad (3.1.41)$$

Так как $\eta < \alpha/20$, мы показали, что плотности множеств A и B не менее $\alpha/200$. Применим лемму 3.1.7 к четвёрке множеств A, B, C и D. Получим

$$\sum_{r\in\mathbb{Z}_N} \big|A \cap (B+r) \cap (C+2r) \cap (D+3r)\big| \geqslant \frac{\alpha^4}{80000}N^2, \quad (3.1.42)$$

принимая во внимания малость числа η. Остаётся заметить, что тривиальных арифметических прогрессий (то есть таких, что $r=0$) не более αN. Следовательно, искомая нетривиальная арифметическая прогрессия найдётся, если

$$\frac{\alpha^4}{80000}N^2 > \alpha N \qquad \Longleftrightarrow \qquad N > \frac{80000}{\alpha^3}. \quad (3.1.43)$$

Остаётся отметить, что найденная арифметическая прогрессия будет прогрессией в $\mathbb{Z}$, а не по модулю N, так как её первый и второй члены лежат в отрезке $[2N/5\,..\,3N/5]$. □

3.2 Теорема Балога–Семереди–Гауэрса

Напомним определение аддитивной энергии (см. формулу (1.3.1))

$$E(A) = \Big|\Big\{(a_1, a_2, b_1, b_2) \in A \times A \times A \times A \;\Big|\; a_1 + b_1 = a_2 + b_2\Big\}\Big|. \tag{3.2.1}$$

Неравенство (1.3.3) показывает, что если константа удвоения множества A мала, то аддитивная энергия этого множества велика. Оказывается, это утверждение можно частично обратить.

Теорема 3.2.1 (Теорема Балога–Семереди–Гауэрса)**.** *Пусть A — непустое конечное подмножество абелевой группы Z. Предположим, что $E(A) \geqslant |A|^3/K$, где $K \geqslant 1$ — некоторое число. Тогда существует подмножество $A_* \subset A$, такое что*

$$|A_*| \geqslant \frac{|A|}{16K} \qquad \text{и} \qquad |A_* - A_*| \leqslant 2^{14}K^4|A_*|. \tag{3.2.2}$$

Оригинальное доказательство Балога и Семереди (см. [1]) опиралось на лемму регулярности, и поэтому давало плохие оценки. Гауэрс первым предложил хорошие оценки.

Замечание 3.2.2. *Мы формулируем теорему Балога–Семереди–Гауэрса для произвольной абелевой группы, потому что применять её будем к группе $\mathbb{Z}^2$, а не $\mathbb{Z}$ или $\mathbb{Z}_N$.*

Доказательство. Введём обозначения $a = |A|$ и $A_s = A \cap (A - s)$. Тогда

$$E(A) = \sum_{s \in Z} |A_s|^2 = \sum_{s,x,y} \chi_{A_s}(x)\chi_{A_s}(y) = \sum_{s,x,y} \chi_A(x)\chi_A(y)\chi_A(x+s)\chi_A(y+s). \tag{3.2.3}$$

Пусть ε — некоторое малое число (мы потом выберем $\varepsilon = 1/8$, но пока удобнее обозначать это число отдельным символом). Рассмотрим множество P_ε:

$$P_\varepsilon = \Big\{s \in Z \;\Big|\; |A_s| \geqslant \frac{\varepsilon a}{2K}\Big\}. \tag{3.2.4}$$

Имеем

$$\sum_s \sum_{x-y \notin P_\varepsilon} \chi_{A_s}(x)\chi_{A_s}(y) = \sum_s \sum_{x-y \notin P_\varepsilon} \chi_A(x)\chi_A(y)\chi_{A_{x-y}}(s) \leqslant \frac{\varepsilon a}{2K} \sum_{x,y} \chi_A(x)\chi_A(y) = \frac{\varepsilon a^3}{2K}. \tag{3.2.5}$$

Кроме того,

$$\sum_{s:\ |A_s| \leqslant \frac{a}{2K}} |A_s|^2 \leqslant \frac{a}{2K} \sum_s |A_s| = \frac{a^3}{2K}. \tag{3.2.6}$$

Собирая оценки $E(A) \geqslant a^3/K$, (3.2.3), (3.2.5) и (3.2.6) воедино, получаем

$$\sum_{s:\ |A_s| \geqslant \frac{a}{2K}} \sum_{x,y} \chi_{A_s}(x)\chi_{A_s}(y) - \varepsilon^{-1} \sum_{s:\ |A_s| \geqslant \frac{a}{2K}} \sum_{x-y \notin P_\varepsilon} \chi_{A_s}(x)\chi_{A_s}(y) \geqslant 0. \tag{3.2.7}$$

Значит, найдётся такой индекс $s \in Z$, что $|A_s| \geqslant \frac{a}{2K}$ и

$$\sum_{x,y} \chi_{A_s}(x)\chi_{A_s}(y) - \varepsilon^{-1} \sum_{x-y \notin P_\varepsilon} \chi_{A_s}(x)\chi_{A_s}(y) \geqslant 0, \tag{3.2.8}$$

что равносильно неравенству

$$\sum_{x-y \in P_\varepsilon} \chi_{A_s}(x)\chi_{A_s}(y) \geqslant (1-\varepsilon)|A_s|^2. \tag{3.2.9}$$

Зафиксируем элемент s и построим граф $G = (V, E)$ на множестве A_s (то есть, $V = A_s$). Две вершины $u, v \in A_s$ соединим ребром, если $u - v \in P_\varepsilon$ (будем смотреть на наш граф как на ориентированный, он содержит петли и кратные рёбра). Оценка (3.2.9) показывает, что в нашем графе хотя бы $(1-\varepsilon)|V|^2$ ребер, откуда следует, что $|A_*| \geqslant \varepsilon|V|$, где

$$A_* = \{v \in V \mid \deg_G v \geqslant (1-2\varepsilon)|V|\}. \tag{3.2.10}$$

В частности, вспоминая, что $\varepsilon = 1/8$ и $|A_s| \geqslant a/(2K)$, получаем искомую оценку $|A_*| \geqslant a/(16K)$. Поэтому нам остаётся оценить мощность множества $|A_* - A_*|$. Согласно условию, наложенному на степени вершин множества A_*, у любых двух вершин есть хотя бы $|V|/2$ общих соседей. Это значит, что для любых $a, b \in A_*$ представление

$$a - b = (a - x) + (x - b), \quad a - x, x - b \in P_\varepsilon \tag{3.2.11}$$

справедливо для хотя бы $|V|/2$ элементов x. Значит, для элемента $a - b \in A_* - A_*$ существует хотя бы $(a/(16K))^2|V|/2$ различных представлений

$$a - b = a_1 + a_2 - b_1 - b_2, \qquad a_1, a_2, b_1, b_2 \in A. \tag{3.2.12}$$

Всего таких представлений не более a^4. Следовательно, получаем оценку

$$|A_* - A_*|(a/(16K))^2|V|/2 \leqslant a^4, \tag{3.2.13}$$

что влечёт

$$|A_* - A_*| \leqslant 2^9 K^2 a^2 |A_s|^{-1} \leqslant 2^{14} K^4 |A_*|. \tag{3.2.14}$$

□

5.5.2022

Следствие 3.2.3. *Пусть $c_0 \in (0,1)$. Существуют такие постоянные d и c, зависящие лишь от числа c_0, что если $A \subset \mathbb{Z}^2$ — такое множество мощности m, что $E(A) \geqslant c_0 m^3$, то найдётся обобщённая арифметическая прогрессия Q размерности d и мощности не более $c^{-1}m$, такая что $|Q \cap A| \geqslant cm$.*

Доказательство. Согласно теореме 3.2.1, найдётся множество $A_* \subset A$, удовлетворяющее оценкам $|A_*| \geqslant c_0 m/16$ и $\sigma[A_*] \leqslant 2^{28} c_0^{-8}$ (мы воспользовались следствием 1.1.11). Мы хотим применить к множеству A_* теорему Фреймана, однако для этого нужно перенести множество A_* на решётку $\mathbb{Z}$. Пусть p — настолько большое простое число, что $A_* \subset [-p/4, p/4]^2$. Рассмотрим проекцию $\varphi_p \colon \mathbb{Z}^2 \to \mathbb{Z}$, действующую по правилу

$$\varphi_p(a, b) = pa + b, \qquad (a, b) \in \mathbb{Z}^2. \tag{3.2.15}$$

Эта проекция — групповой гомоморфизм. Покажем, что $\varphi_p|_{A_*}$ —2-изоморфизм Фреймана. Действительно, если $(a_i, c_i), (b_i, d_i) \in A_*$ для $i = 1, 2$, то равенства

$$\begin{cases} a_1 + b_1 = a_2 + b_2; \\ c_1 + d_1 = c_2 + d_2 \end{cases} \qquad \text{и} \qquad p(a_1 + b_1) + c_1 + d_1 = p(a_2 + b_2) + c_2 + d_2 \tag{3.2.16}$$

равносильны (потому что $|c_i + d_i| < p/2$). Применим теорему 1.5.7 к множеству $\varphi_p(A^*)$, получим обобщённую арифметическую прогрессию $\tilde{Q}$ размерности $d = 2^{20} C^2 (\log C)^2$ и мощности не более $\exp(2^{20} C^2 (\log C)^2) m$, где $C = 2^{28} c_0^8$. Остаётся положить $Q = \varphi_p^{-1}(\tilde{Q})$ и воспользоваться тем фактом, что 2-изоморфизм Фреймана переводит обобщённые арифметические прогрессии в обобщённые арифметические прогрессии. □

Определение 3.2.4. Пусть $B \subset \mathbb{Z}_N$, а $\psi\colon B \to \mathbb{Z}_N$ — некоторое отображение. Будем говорить, что четвёрка $(a,b,c,d) \in B^4$ аддитивна, если $a+b=c+d$ и $\psi(a)+\psi(b)=\psi(c)+\psi(d)$.

В следующем следствии мы считаем число N достаточно большим (настолько большим, что $N^\gamma \geqslant 2$).

Следствие 3.2.5. *Для всяких чисел $\beta \in (0,1)$ и $c_0 \in (0,1)$ существуют постоянные $\gamma, \eta \in (0,1)$ со следующим свойством. Пусть $B \subset \mathbb{Z}_N$ — подмножество плотности β, $\varphi\colon B \to Z_N$ — отображение, график которого содержит хотя бы c_0N^3 аддитивных четвёрок. Существует арифметическая прогрессия P мощности хотя бы N^γ и линейная функция $\psi\colon P \to \mathbb{Z}_N$, такая что $\varphi|_{B\cap P}$ совпадает с ψ хотя бы в $\eta|P|$ точках.*

Доказательство. Пусть A — образ при естественном вложении в решётку $\mathbb{Z}^2$ графика $\Gamma \subset \mathbb{Z}_N^2$ отображения φ. Нетрудно видеть, что тогда $E(A) \geqslant E(\Gamma)/16$ (для этого нужно воспользоваться формулой (1.3.2) и подметить, что число решений $a,b \in \Gamma$ уравнения $a+b=x$ равно суммарному числу решений $c,d \in A$ уравнений $c+d=x$, $c+d=(x+(0,N))$, $c+d=x+(N,0)$ и $c+d=x+(N,N)$, здесь $x \in \mathbb{Z}_N^2$ отождествлён со своим вложением в $\mathbb{Z}^2$), а последняя величина не менее $c_0N^3/16$. Применим к множеству A следствие 3.2.3, пусть Q — соответствующая обобщённая арифметическая прогрессия, что $|A\cap Q| \geqslant \eta|A|$. Пусть $Q = P_1 \times P_2 \times \ldots \times P_d$, где P_j — отрезки арифметических прогрессий. Пусть, не умаляя общности, P_1 — самый длинный из них, в таком случае $|P_1| \geqslant |Q|^{1/d} \gtrsim N^{1/d}$; положим $\gamma = (2d)^{-1}$. Заметим, что множество Q — объединение сдвигов прогрессии P_1, и поэтому, для какого-то сдвига будет справедливо неравенство $|(P_1+z)\cap A| \geqslant \eta|P_1|$. Положим $P = \pi_1[P_1+z]$, где π_1 — проекция решётки $\mathbb{Z}^2$ на первую координату. Остаётся заметить, что, так как множество A — график некоторого отображения, $\pi_1|_{P_1+z}$ — биекция (потому что иначе $|(P_1+z)\cap A| \leqslant 1$, что противоречит нашему предположению $N^\gamma \geqslant 2$). Поэтому справедливо неравенство $|P| \geqslant N^\gamma$ (если число N достаточно велико), а сужение графика отображения φ на $P\cap B$ линейно. $\square$

3.3 Структура неравномерных множеств и функций

Пусть функция $f\colon \mathbb{Z}_N \to \mathbb{D} = \{z \in \mathbb{C} \mid |z| \leqslant 1\}$ не является квадратично η-равномерной. Согласно формуле (3.1.22), это, в частности, означает, что для хотя бы $\eta^8N/2$ значений параметра k функция $\Delta(f;k)$ не является $\eta^2/2$-равномерной. Ввиду формулы (3.1.12) это означает, что существует такие множество B мощности $\eta^8N/2$ и отображение $\varphi\colon B \to \mathbb{Z}_N$, что

$$\left|\Delta(f;k)\hat{}(\varphi(k))\right| \geqslant \frac{\eta^4}{4}N, \qquad k \in B. \tag{3.3.1}$$

Следовательно,

$$\sum_{k\in B}\left|\Delta(f;k)\hat{}(\varphi(k))\right|^2 \geqslant c_0N^3, \tag{3.3.2}$$

где $c_0 = \eta^{16}/32$. Следующая лемма гласит, что это простое неравенство позволяет сделать вывод о геометрии графика отображения φ.

Предложение 3.3.1. *Пусть $\alpha > 0$, $f\colon \mathbb{Z}_N \to \mathbb{D}$ — функция, $B \subset \mathbb{Z}_N$ — множество, а $\varphi\colon B \to \mathbb{Z}_N$ — отображение. Если*

$$\sum_{k\in B}\left|\Delta(f;k)\hat{}(\varphi(k))\right|^2 \geqslant \alpha N^3, \tag{3.3.3}$$

то график отображения φ содержит хотя бы α^4N^3 аддитивных четвёрок.

Доказательство. Запишем по определению,

$$\sum_{k\in B}\sum_{s,t\in\mathbb{Z}_N} f(s)\overline{f(s-k)f(t)}f(t-k)e^{2\pi i\frac{\varphi(k)(s-t)}{N}} \geqslant \alpha N^3 \tag{3.3.4}$$

и заменим переменную $u=s-t$

$$\sum_{k\in B}\sum_{s,u\in\mathbb{Z}_N} f(s)\overline{f(s-k)f(s-u)}f(s-u-k)e^{2\pi i\frac{\varphi(k)u}{N}} \geqslant \alpha N^3. \tag{3.3.5}$$

Воспользуемся неравенством треугольника:

$$\sum_{s,u}\Big|\sum_{k\in B}\overline{f(s-k)}f(s-u-k)e^{2\pi i\frac{\varphi(k)u}{N}}\Big| \geqslant \alpha N^3, \tag{3.3.6}$$

а потом — неравенством КБШ:

$$\sum_{s,u}\Big|\sum_{k\in B}\overline{f(s-k)}f(s-u-k)e^{2\pi i\frac{\varphi(k)u}{N}}\Big|^2 \geqslant \alpha^2 N^4. \tag{3.3.7}$$

Пусть

$$\sum_{s}\Big|\sum_{k\in B}\overline{f(s-k)}f(s-u-k)e^{2\pi i\frac{\varphi(k)u}{N}}\Big|^2 = \gamma(u)N^3. \tag{3.3.8}$$

Докажем неравенство

$$\sum_{r\in\mathbb{Z}_N}\Big|\sum_{k\in B}e^{2\pi i\frac{\varphi(k)u+rk}{N}}\Big|^4 \geqslant \gamma^2(u)N^4, \qquad u\in\mathbb{Z}_N. \tag{3.3.9}$$

Для этого определим функции F и G по правилам

$$F(k)=\overline{\Delta(f;-u)}(k), \qquad G(k)=\chi_B(k)e^{2\pi i\frac{\varphi(k)u}{N}}, \qquad k\in\mathbb{Z}_N. \tag{3.3.10}$$

Неравенство (3.3.8) гласит:

$$\sum_{s\in\mathbb{Z}_N}|F*G(s)|^2=\gamma(u)N^3. \tag{3.3.11}$$

Запишем цепочку неравенств:

$$\sum_{s\in\mathbb{Z}_N}|F*G(s)|^2=\frac{1}{N}\sum_{\zeta\in\mathbb{Z}_N}|\hat{F}(\zeta)|^2|\hat{G}(\zeta)|^2 \leqslant \frac{1}{N}\Big(\sum_{\zeta}|\hat{F}(\zeta)|^4\Big)^{\frac12}\Big(\sum_{\zeta}|\hat{G}(\zeta)|^4\Big)^{\frac12}$$
$$\overset{|f|\leqslant 1}{\leqslant}\Big(\sum_{\zeta}|\hat{F}(\zeta)|^2\Big)^{\frac12}\Big(\sum_{\zeta}|\hat{G}(\zeta)|^4\Big)^{\frac12}\overset{|f|\leqslant 1}{\leqslant}N\Big(\sum_{\zeta}|\hat{G}(\zeta)|^4\Big)^{\frac12}, \tag{3.3.12}$$

что и даёт неравенство (3.3.9). Благодаря оценке (3.3.7), имеем $\sum_u\gamma(u)\geqslant\alpha^2N$, что влечёт $\sum_u\gamma^2(u)\geqslant\alpha^4N$. Значит, из неравенства (3.3.9) следует оценка

$$\sum_u\sum_r\Big|\sum_{k\in B}e^{2\pi i\frac{\varphi(k)u+rk}{N}}\Big|^4\geqslant\alpha^4N^5. \tag{3.3.13}$$

Раскрывая скобки, получаем

$$\sum_{a,b,c,d\in B}\sum_{u,r}e^{2\pi i\frac{\varphi(a)+\varphi(b)-\varphi(c)-\varphi(d)}{N}u}e^{2\pi i\frac{a+b-c-d}{N}r}\geqslant\alpha^4N^5. \tag{3.3.14}$$

Остаётся заметить, что сумма в левой части этого неравенства есть ни что иное, как количество аддитивных четвёрок графика отображения φ, умноженное на N^2. □

Следовательно, если множество A — не квадратично η-равномерно, то, совмещая следствие 3.2.5 и предложение 3.3.1, находим арифметическую прогрессию P мощности хотя бы N^γ (число γ довольно просто зависит от числа η) и числа $\lambda, \mu \in \mathbb{Z}_N$, такие что

$$\sum_{k\in P} \Big|(\Delta(f_A; k))\hat{}\ (\lambda k + \mu)\Big|^2 \geqslant cN^2|P|, \tag{3.3.15}$$

где c — некоторая зависящая лишь от η постоянная. 12.5.2022

Лемма 3.3.2. *Пусть $T \in N$, $T \geqslant 2$. Пусть $f_1, f_2, f_3 \colon [1\,..\,2T] \to \mathbb{D}$ — функции, удовлетворяющие неравенству*

$$\Big|\sum_{p=1}^{T}\sum_{q=1}^{T} f_1(p)f_2(q)f_3(p+q)e^{-2\pi i(ap+bq-2cpq)}\Big| \geqslant cT^2. \tag{3.3.16}$$

Существует такой квадратный трёхчлен ψ, что

$$\Big|\sum_{p=1}^{T} f_1(p)e^{-2\pi i\psi(p)}\Big| \geqslant \frac{cT}{\sqrt{2}}. \tag{3.3.17}$$

Доказательство. Преобразуем фазу в условии

$$ap + bq - 2cpq = ap + cp^2 + bq + cq^2 - c(p+q)^2. \tag{3.3.18}$$

Введём в рассмотрение функции g_1, g_2 и g_3, заданные формулами

$$g_1(p) = f_1(p)e^{-2\pi i(ap+cp^2)}, \quad p \in [0..T]; \tag{3.3.19}$$

$$g_2(q) = f_2(-q)e^{-2\pi i(-bq+cq^2)}, \quad q \in [0..T]; \tag{3.3.20}$$

$$g_3(s) = f_3(s)e^{2\pi ics^2}, \quad s \in [0..2T], \tag{3.3.21}$$

и доопределим функции g_1 и g_2 нулём при других значениях параметров. В таком случае, условие (3.3.16) перепишется в виде

$$\Big|\sum_{s=0}^{T} g_1(s)(g_2 * g_3)(s)\Big| \geqslant cT^2. \tag{3.3.22}$$

Оценим левую часть величиной (работаем в группе $\mathbb{Z}_{2T}$) $\|\hat{g}_1\|_\infty\|g_2\|_2\|g_3\|_2 \leqslant \sqrt{2}T\|\hat{g}_1\|_\infty$. Следовательно, найдётся такое число $r \in [0..2T]$, что

$$\Big|\sum_{p=1}^{T} g_1(p)e^{-2\pi i\frac{rp}{2T}}\Big| \geqslant \frac{c}{\sqrt{2}}T. \tag{3.3.23}$$

□

Замечание 3.3.3. *Коэффициенты многочлена ψ — c и $a + r/(2T)$. На самом деле, если N — большее $2T$ число, то, проведя то же самое рассуждение, но вкладывая естественным образом отрезок $[0\,..\,2T]$ в группу $\mathbb{Z}_N$ и пользуясь преобразованием Фурье на этой группе, можно заменить коэффициент $r/(2T)$ на $\tilde{r}/N$, где $\tilde{r} \in [0\,..\,N]$.*

Предложение 3.3.4. *Пусть P — арифметическая прогрессия в отрезке $[0\,..\,N]$ мощности T, а $f\colon \mathbb{Z}_N \to \mathbb{D}$ — функция. Пусть нашлись такие числа $\lambda, \mu \in \mathbb{Z}$, что*

$$\sum_{k\in P} \Big|\Delta(f;k)(\lambda k+\mu)\Big|^2 \geqslant \beta N^2 T. \tag{3.3.24}$$

Тогда существуют такие квадратные трёхчлены $\psi_0, \psi_1, \dots, \psi_{N-1}$ с целыми коэффициентами, что

$$\sum_s \Big|\sum_{z\in P+s} f(z)e^{-2\pi i\frac{\psi_s(z)}{N}}\Big| \geqslant \frac{\beta NT}{\sqrt{2}}. \tag{3.3.25}$$

Доказательство. Расшифруем неравенство (3.3.24):

$$\sum_{k\in P}\sum_{s,t} f(s)f(s-k)f(t)f(t-k)e^{-2\pi i\frac{(s-t)(\lambda k+\mu)}{N}} \geqslant \beta N^2 T \tag{3.3.26}$$

и сделаем традиционную замену переменных $u = s - t$:

$$\sum_{k\in P}\sum_{s,u} f(s)f(s-k)f(s-u)f(s-u-k)e^{-2\pi i\frac{(\lambda k+\mu)u}{N}} \geqslant \beta N^2 T. \tag{3.3.27}$$

Пусть $P = \{x+d, x+2d, \dots, x+Nd\}$, перепишем, используя эти обозначения:

$$\sum_{p=1}^{T}\sum_{s,u} f(s)f(s-x-pd)f(s-u)f(s-u-x-pd)e^{-2\pi i\frac{(\lambda(x+pd)+\mu)u}{N}} \geqslant \beta N^2 T. \tag{3.3.28}$$

Для всякого элемента $u \in \mathbb{Z}_N$ существует ровно T способов представить его в виде $u = y + jd$, $j = 1, 2, \dots, T$, поэтому,

$$\frac{1}{T}\sum_{p,j=1}^{T}\sum_{s,y} f(s)f(s-x-pd)f(s-y-jd)f(s-y-x-(p+j)d)e^{-2\pi i\frac{(\lambda(x+pd)+\mu)(y+jd)}{N}}$$

$$\geqslant \beta N^2 T \tag{3.3.29}$$

Воспользовавшись неравенством треугольника и оценкой $|f| \leqslant 1$, получаем

$$\frac{1}{T}\sum_{s,y}\Big|\sum_{p,j=1}^{T} f(s-x-pd)f(s-y-jd)f(s-y-x-(p+j)d)e^{-2\pi i\frac{(\lambda(x+pd)+\mu)(y+jd)}{N}}\Big| \geqslant \beta N^2 T \tag{3.3.30}$$

Введём обозначение

$$\gamma(s,y) = T^{-2}\Big|\sum_{p,j=1}^{T} f(s-x-pd)f(s-y-jd)f(s-y-x-(p+j)d)e^{-2\pi i\frac{(\lambda(x+pd)+\mu)(y+jd)}{N}}\Big|, \tag{3.3.31}$$

тогда $\sum_{s,y}\gamma(s,y) \geqslant \beta N^2$. Применив лемму 3.3.2 (с учётом замечания 3.3.3) при фиксированных s, y, получим, что существует такой целочисленный квадратный трёхчлен $\psi_{s,y}$, что

$$\Big|\sum_{p=1}^{T} f(s-x-pd)e^{-2\pi i\frac{\psi_{s,y}(p)}{N}}\Big| \geqslant \frac{\gamma(s,y)T}{\sqrt{2}}. \tag{3.3.32}$$

В качестве квадратного трёхчлена ψ_s выберем тот трёхчлен $\psi_{s,y}$, для которого число $\gamma(s,y)$ наибольшее. Получаем

$$\sum_s \Big| \sum_{z\in P+s} f(z)e^{-2\pi i\frac{\psi_s(z)}{N}}\Big| \geqslant \frac{T}{\sqrt{2}N}\sum_{s,y}\gamma(s,y) = \frac{\beta NT}{\sqrt{2}}. \tag{3.3.33}$$

□

Следующая лемма является следствием неравенства Вейля (количественной версии того факта, что последовательность $\{\alpha n^2\}$ равномерно распределена на единичной окружности, если число α иррационально). Оставим её без доказательства (его можно посмотреть в пятой главе работы [9]).

Лемма 3.3.5. *Существует абсолютная постоянная C со следующим свойством. Пусть $\psi\colon \mathbb{Z}_N \to \mathbb{Z}_N$ — квадратный трёхчлен, а $r \leqslant N$. Существует такое число $m \leqslant Cr^{127/128}$, что множество $[0\,..\,r-1]$ можно разбить на арифметические прогрессии $P_1, P_2, \dots, P_m$, длины которых отличаются не более чем на единицу, и для всякого j диаметр множества $\psi(P_j)$ не превосходит $Cr^{-1/128}N$.*

Следствие 3.3.6. *Пусть $\psi\colon \mathbb{Z}_N \to \mathbb{Z}_N$ — квадратный трёхчлен и $r \leqslant N$. Пусть $\alpha \gtrsim r^{-1/128}$. Существует число $m \leqslant Cr^{127/128}$ и разбиение множества $[0\,..\,r-1]$ на арифметические прогрессии $P_1, P_2, \dots, P_m$, длины которых отличаются не более чем на один, такие что если для некоторой функции $f\colon \mathbb{Z}_N \to \mathbb{D}$ выполнено условие*

$$\Big|\sum_{x=0}^{r-1} f(x)e^{-2\pi i\frac{\psi(x)}{N}}\Big| \geqslant \alpha r, \tag{3.3.34}$$

то $\sum_{j=1}^m |\sum_{x\in P_i} f(x)| \geqslant \alpha r/2$.

Доказательство. Построим арифметические прогрессии P_i при помощи леммы 3.3.5. По неравенству треугольника,

$$\sum_{j=1}^m \Big|\sum_{x\in P_j} f(x)e^{-2\pi i\frac{\psi(x)}{N}}\Big| \geqslant \alpha r. \tag{3.3.35}$$

Так как для любых двух $x, y \in P_i$ верно неравенство $|\psi(x)-\psi(y)| \leqslant Cr^{-1/128} \leqslant \alpha/20$, выполнена и оценка

$$\Big|e^{-2\pi i\frac{\psi(x)}{N}} - e^{-2\pi i\frac{\psi(y)}{N}}\Big| \leqslant \alpha/2. \tag{3.3.36}$$

Поэтому

$$\Big|\sum_{x\in P_i} f(x)\Big| \geqslant \frac{1}{2}\Big|\sum_{x\in P_i} f(x)e^{-2\pi i\frac{\psi(x)}{N}}\Big| \geqslant \frac{\alpha r}{2}. \tag{3.3.37}$$

□

Доказательство теоремы 2.1.1 для случая $k=4$. Пусть $A \subset [0..N]$ — подмножество плотности δ. Если множество A квадратично η-равномерно (пусть $\eta = 10^{-8}\delta^8$), то оно содержит нетривиальную арифметическую прогрессию длины 4 согласно следствию 3.1.9. В противном же случае найдутся такие множество $B \subset \mathbb{Z}_N$ и отображение $\varphi\colon B \to \mathbb{Z}_N$, что

$$\sum_{k\in B}\Big|\Delta(f;k)\hat{}(\varphi(k))\Big|^2 \geqslant \eta^6N^3/8, \tag{3.3.38}$$

см. формулу (3.3.2). Благодаря предложению 3.3.1, это значит, что график отображения φ содержит хотя бы $(\eta^6/8)^4$ аддитивных четвёрок. Значит, по следствию 3.2.5, существует арифметическая прогрессия P, где $|P| \geqslant N^\gamma$ и γ зависит от параметра η полиномиальным образом, такая что

$$\sum_{k\in P} \Big|\Delta(f_A;k)(\lambda k+\mu)\Big|^2 \geqslant cN^2|P|, \tag{3.3.39}$$

для некоторых чисел $\lambda, \mu \in \mathbb{Z}$. Тогда, по предложению 3.3.4

$$\sum_{s\in\mathbb{Z}_N} \Big|\sum_{z\in P+s} f_A(z)e^{-2\pi i\frac{\psi_s(z)}{N}}\Big| \geqslant \beta NT, \tag{3.3.40}$$

где ψ_s — целочисленные квадратные трёхчлены, а β — некоторое число, зависящее от параметра η экспонента многочлена. Следствие 3.3.6 позволяет разбить каждую прогрессию $P+s$ на подпрогресии $P_{s1}, P_{s2}, \dots, P_{sm_s}$ почти равной длины, не слишком короткие, $m_s \geqslant N^{\gamma/128}$, и такие что

$$\sum_s \sum_{j=1}^{m_s} \Big|\sum_{z\in P_{sj}} f_A(z)\Big| \geqslant \frac{\beta NT}{2}. \tag{3.3.41}$$

Заметим, что

$$\sum_s \sum_{j=1}^{m_s} \sum_{z\in P_{sj}} f_A(z) = \sum f_A(x) = 0, \tag{3.3.42}$$

поэтому, если мы оставим в сумме по параметрам j и z лишь неотрицательные слагаемые, то сумма будет не менее $\beta NT/4$. Следовательно, для некоторого выбора j и m_s справедлива оценка

$$\sum_{z\in P_{sj}} f_A(z) \geqslant \frac{\beta T}{4m}, \tag{3.3.43}$$

что влечёт неравенство $|A\cap P_{sj}| \geqslant (\delta+\beta/4)|P_{sj}|$. Это значит, что если множество A не является квадратично η-равномерным, то такая найдётся арифметическая прогрессия длины N^θ, где θ зависит лишь от η (причём полиномиальным образом), что плотность A в этой прогрессии хотя бы $\delta+\delta_0$, где δ_0 зависит лишь от η. Итерируя это утверждение, завершаем доказательство. $\square$

Глава 4

Задачи об иголках

26.11.2018

4.1 Множество Безиковича на плоскости

Определение 4.1.1. Множество $X \subset \mathbb{R}^d$ назовём множеством Безиковича если для всякого вектора $e \in \mathbb{R}^d$, $|e| = 1$, найдётся $x \in X$, такой что

$$\{x + te \mid t \in [0,1]\} \subset X.$$

Иными словами, множество Безиковича обязано содержать отрезок единичной длины произвольного направления. Конечно, существует очень много множеств Безиковича — например, единичный шар, или единичный куб. Вполне естественный вопрос, некоторые неполные ответы на который мы дадим в этой главе, это насколько малым может быть множество Безиковича.

Теорема 4.1.2 (Теорема Безиковича)**.** *Существует компактное множество Безиковича на плоскости, имеющее нулевую лебегову меру.*

Наше изложение доказательства будет следовать [17]. Однако, мы дадим геометрическое описание построения, за арифметическим описанием той же конструкции читатель может обратиться к книге [17].

Определение 4.1.3. Компактное подмножество F полосы $\{(x,y) \in \mathbb{R} \mid 0 \leqslant x \leqslant 1\}$ назовём хорошим, если для всякого числа $m \in [0,1]$, множество F содержит отрезок наклона m, соединяющий края полосы. Иными словами, для всякого $m \in [0,1]$ найдётся число b, такое что

$$\{(x, mx + b) \mid x \in [0,1]\} \subset F.$$

Предложение 4.1.4. *Для всякого числа $\varepsilon > 0$ существует хорошее множество $F \subset [0,1] \times [-1,1]$, такое что для всякого $x_0 \in [0,1]$ имеет место неравенство*

$$\big|F \cap \{(x_0, y) \mid y \in \mathbb{R}\}\big| \leqslant \varepsilon.$$

Модуль обозначает меру Лебега на прямой. Естественно, двумерная мера Лебега построенного множества не превосходит ε.

Доказательство. Построение множество F удобно будет задать в несколько шагов. Но сначала мы опишем общую структуру множества F. Зафиксируем большое натуральное число N, которое выберем впоследствии. Рассмотрим треугольник T_1 с вершинами $(0,0)$, $(0,-1)$ и $(1,0)$. Конечно, этот треугольник хороший. Разделим его основание $\{(0,y) \mid y \in [-1,0]\}$ на N^N равных отрезков. Это

индуцирует разбиение треугольника T_1 на N^N треугольников с равными основаниями, а именно, каждый треугольник разбиения имеет своими вершинами точки $(1,0)$, $(0,-\frac{k}{N^N})$ и $(0,-\frac{k+1}{N^N})$, где $k = 0,1,\ldots,N^N-1$. Множество F будет объединением некоторых сдвигов по вертикали треугольников разбиения. Отсюда следует, что множество F будет хорошим. Двигать треугольники будет удобно группами, поэтому мы будем резать треугольники и двигать поэтапно.

На k-м шаге алгоритм получает набор из N^{k-1} треугольников T_k^j, $j = 1,2,\ldots,N^{k-1}$. У каждого из этих треугольников основание имеет длину N^{1-k} и лежит на оси игрек, а ещё одна вершина лежит на прямой $x = 1$. Кроме того, множество $F_k = \cup_j T_k^j$ удовлетворяет следующим двум свойствам:

1) $F_k \cap \{(x,y) \mid x \leqslant \frac{k-1}{N}\} \subset F_{k-1}$;

2) Множество $F_k \cap \{(x_0,y) \mid y \in \mathbb{R}\}$, где $x_0 \in [\frac{k-1}{N}, \frac{k}{N}]$, можно покрыть N^{k-1} отрезками длины $2N^{-k}$.

С каждым треугольником T_k^j проделаем следующие действия. Разобъём его основание (то есть, сторону, лежащую на оси y) на N равных частей, это индуцирует разбиение T_k^j на N треугольников $\tilde{T}_{k+1}^{(j-1)N+i}$, $i = 1,2,\ldots,N$. После этого посмотрим на отрезки, высекаемые этими треугольниками на прямой $x = \frac{k-1}{N}$. Передвинем каждый треугольник $\tilde{T}_{k+1}^{(j-1)N+i}$ параллельно оси y так, чтобы отрезок, высекаемый им на прямой $x = \frac{k-1}{N}$ совпал с отрезком, высекаемым на оной прямой верхним из треугольников $\tilde{T}_{k+1}^{(j-1)N+i}$, $i = 1,2,\ldots,N$. Такой сдвиг треугольника $\tilde{T}_k^{(j-1)+i}$ и назовём $T_k^{(j-1)+i}$. Пример этой процедуры изображён на рисунке 4.1. Новые треугольники построены, и алгоритм может переходить к следующему шагу.

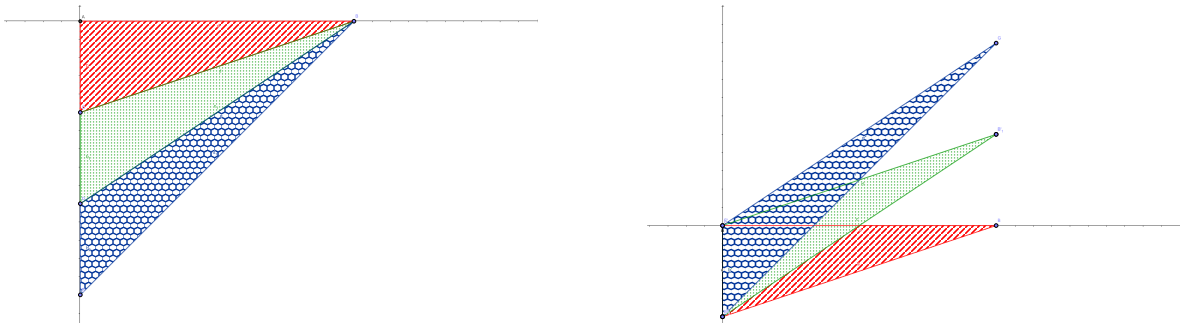

Рис. 4.1: Пример преобразования множества F_1 в множество F_2 при $N = 3$.

Надо показать, что построенная таким образом последовательность множеств F_k удовлетворяет двум требуемым свойствам. Первое свойство легко вывести из того факта, что

$$T_{k+1}^{(j-1)N+i} \cap \left\{(x,y) \;\middle|\; x \leqslant \frac{k-1}{N}\right\} \subset T_k^j.$$

Второй факт несколько сложнее. В случае $x_0 = \frac{k-1}{N}$ он следует из построения новых треугольников. Общий случай нетрудно вывести из рассмотренного и того факта, что наклоны сторон треугольников $T_{k+1}^{(j-1)N+i}$, $i = 1,2,\ldots,N$ отличаются не более, чем на N^{1-k}, при фиксированном j.

Нетрудно видеть, что в качестве множества F можно взять F_N, если $N \geqslant \frac{1}{2\varepsilon}$. □

Упражнение 4.1.1. *Докажите, что конструкция, приведённая в доказательстве предложения 4.1.4, допускает следующую переформлировку. Положим $\delta = 0.1N^{-N}$. Существует набор дизъюнктных прямоугольников T_j вида $1 \times \delta$, таких что мера обеединения их сдвигов на расстояние d_j, $5 \leqslant d_j \leqslant 10$, вдоль главных осей, имеет меру не более N^{-1}.*

Лемма 4.1.5. *Для всяких положительных чисел δ и ε и всякого хорошего множества G существует хорошее множество E меры не более ε, лежащее в δ-окрестности G.*

Доказательство. Пусть ℓ_j, $j = 0, 1, \dots, [\delta^{-1}]$, — отрезок в множестве G наклона $j\delta$, соединяющий ось игрек с прямой $x = 1$. Построим параллелограммы P_j:

$$P_j = \{(x, y) \mid \exists (x, \tilde{y}) \in \ell_j, |y - \tilde{y}| \leqslant \delta\}.$$

Пусть F — множество, построенное в предложении 4.1.4. Сделаем аффинное преобразование, переводящее прямоугольник $[0, 1] \times [-1, 1]$ в параллелограмм P_j, пусть F_j — образ множества F при этом отображении. В таком случае, F_j содержит отрезки направлений $[\delta j, \delta j + \delta]$, соединяющие края полосы. Положим $E = \cup_j F_j$. Отметим, что это хорошее множество. Его меру тоже легко оценить:

$$|E| \leqslant \sum_{j=0}^{[\delta^{-1}]} |F_j| \leqslant ([\delta^{-1}] + 1)\varepsilon\delta \leqslant 2\varepsilon,$$

(мы предположили $\delta < 1$, что, разумеется, не ограничительно). Поэтому надо лишь уменьшить ε в два раза. □

Лемма 4.1.6. *Существует хорошее множество меры нуль.*

Эта лемма влечёт теорему 4.1.2: надо просто объединить повороты хорошего множества меры нуль на углы $\frac{k\pi}{4}$, $k = 0..4$, объединение будет множеством Безиковича нулевой меры.

Доказательство леммы 4.1.6. Построим последовательность хороших множеств $\{F_n\}$ и убывающую к нулю последовательность чисел $\{\varepsilon_n\}$ со следующими свойствами:

1) $\overline{B_{\varepsilon_n}(F_n)} \subset B_{\varepsilon_{n-1}}(F_{n-1})$;

2) $|\overline{B_{\varepsilon_n}(F_n)}| \leqslant 2^{-n}$.

Строить эту последовательность надо так: пользуясь леммой 4.1.5 с $\varepsilon := 2^{-n}$, $\delta := \frac{1}{2}\varepsilon_{n-1}$ и $G := F_{n-1}$, строить множество $F_n := E$. После чего, выбирать ε_n столь малым, чтобы выполнилось второе условие (это можно сделать по регулярности меры Лебега).

Искомое множество есть ни что иное как $\cap_n \overline{B_{\varepsilon_n}(F_n)}$. □

Маленькие множества Безиковича встречаются в задачах гармонического анализа, нелинейных уравнениях в частных производных и даже в задачах классической механики. Например, конструкция упражнения 4.1.1 сыграла ключевую роль в построении Ч. Фефферманом контрпримера к задаче о шаровом мультипликаторе. Эта задача была очень знаменитой гипотезой в гармоническом анализе в 1960-х годах. Гипотеза состояла в том, что неравенство

$$\|(\hat{f}\chi_{B_1(0)})^{\check{}}\|_{L_p(\mathbb{R}^2)} \lesssim \|f\|_{L_p(\mathbb{R}^2)}$$

верно при $p \in (\frac{4}{3}, 4)$. Оказалось, что контрпример строится из множества Безиковича и единственное возможное значение параметра p — это 2, при этом показателе неравенство следует из теоремы Планшереля.

В 1970-х годах выяснилось, что оценки размерности множеств Безиковича почти равносильны некоторым важным в гармоническом анализе неравенствам. Об этих оценках мы расскажем в следующей главе.

4.2 Гипотеза Какейя

Гипотеза 4.2.1 (Гипотеза Какейя)**.** *Любое множество Безиковича в $\mathbb{R}^d$ имеет полную размерность Хаусдорфа.*

Отметим, что Какейя интересовался задачами, схожими с теоремой Безиковича, но вряд ли ставил эту гипотезу. Она поставлена в 1950-х годах. В размерности 2 её доказал Дэвис в 1971 году. В размерностях $d = 3$ и выше гипотеза открыта. Методами гармонического анализа (или классическими методами геометрической теории меры) можно добиться оценки $\dim_{\mathrm{Haus}} F \geqslant \frac{d}{2} + 1$, где F — множество Безиковича в $\mathbb{R}^d$. Это доказательство читатель может найти в [17]. В конце 1990-х годов Бургейн доказал оценку $\dim_{\mathrm{Haus}} F \geqslant \frac{13}{25}d - c$, где c — некоторая абсолютная константа, не зависящая от параметра d. Его доказательство опиралось на теоремы аддитивной комбинаторики. Мы изложим теорему Каца и Тао, доказательство которой хоть и не использует результаты предыдущих глав, но по духу — аддитивно комбинаторное. На самом деле, этот результат — лишь предварительная ступень к более сильной оценке, которую читатель может изучить по оригинальной работе [11].

Теорема 4.2.2 (Кац–Тао, 2002)**.** *Размерность Минковского любого множества Безиковича в $\mathbb{R}^d$ не менее $\frac{4}{7}(d-1)$.*

Напомним определение размерности Минковского.

Определение 4.2.3. Пусть $F \subset \mathbb{R}^d$, $\delta > 0$. Символом $\mathcal{N}_\delta$ обозначим наименьшее число шаров радиуса δ, требуемое, чтобы покрыть множество F. Определим нижнюю размерность Минковского множества F согласно формуле

$$\dim_{\mathrm{Mink}} F = \varliminf_{\delta \to 0} \frac{\log \mathcal{N}_\delta(F)}{|\log \delta|}.$$

Упражнение 4.2.1. *Докажите, что для всякого числа $\lambda > 0$ существует константа $C = C(d, \lambda)$, такая что*

$$\mathcal{N}_\delta(G) \leqslant C\mathcal{N}_{\lambda\delta}(G).$$

Упражнение 4.2.2. *Докажите, что размерность Хаудорфа не меньше размерности Минковского. Постройте пример множества ненулевой размерности Минковского и нулевой размерности Хаусдорфа.*

3.12.2018

Определение 4.2.4. Пусть Z — коммутативная группа, $r \in \mathbb{Z}$. Символом $\pi_r \colon Z \times Z \to Z$ обозначим проекцию

$$\pi_r(z_1, z_2) = z_1 + rz_2.$$

Символ π_∞ обозначает отображение $(z_1, z_2) \mapsto z_2$.

Доказательство теоремы 4.2.2 опирается на следующий результат аддитивной комбинаторики.

Теорема 4.2.5. *Пусть Z — абелева группа, $G \subset Z \times Z$ — конечное множество, такое что $\pi_{-1}|_G$ — инъективное отображение (иными словами все элементы $b - a$ различны когда $(a, b) \in G$). Имеет место неравенство (константы в неравенстве не зависят от множества G и группы Z)*

$$|G| \lesssim \Big(\max_{r=0,1,2,\infty} |\pi_r(G)| \Big)^{\frac{7}{4}}.$$

Следствие 4.2.6. *Пусть $G \subset \mathbb{R}^d \times \mathbb{R}^d$. Тогда*

$$\mathcal{N}_\delta(\pi_{-1}(G)) \lesssim \Big(\max_{r=0,1,2,\infty} \mathcal{N}_\delta(\pi_r(G)) \Big)^{\frac{7}{4}}.$$

Вывод следствия 4.2.6 из теоремы 4.2.5. Для всякого числа δ рассмотрим множество G_δ:

$$G_\delta = \Big\{ x \in \delta(\mathbb{Z}^d \times \mathbb{Z}^d) \;\Big|\; \operatorname{dist}(x, G) \leqslant \sqrt{2d}\delta \Big\}.$$

Докажем, что $\mathcal{N}_\delta(G) \asymp |G_\delta|$. Константы в этом соотношении, разумеется, могут зависеть от размерности d. На время доказательства этого соотношения введём обозначение $D = 2d$, то есть, всё происходит в пространстве $\mathbb{R}^D$.

Сначала получим неравенство $\mathcal{N}_\delta(G) \lesssim |G_\delta|$. Отметим, что множество G содержится в $\sqrt{D}\delta$-окрестности множества G_δ, так как в замкнутой $\sqrt{D}\delta$-окрестности каждой точки пространства $\mathbb{R}^D$ лежит какая-то точка решётки $\delta\mathbb{Z}^D$. Стало быть, множество G можно покрыть $|G_\delta|$ шарами радиуса $\sqrt{D}\delta$. Следовательно, $N_{\sqrt{D}\delta}(G) \leqslant |G_\delta|$ и результат следует из упражнения 4.2.1.

Теперь докажем обратное неравенство $|G_\delta| \lesssim \mathcal{N}_\delta(G)$. Пусть $B_\delta(x_j), j = 1, 2, \ldots, \mathcal{N}_\delta(G)$, — покрытие множества G шарами радиуса δ. Нетрудно видеть, что

$$G_\delta \subset \Big\{ x \in \delta\mathbb{Z}^D \;\Big|\; \operatorname{dist}(x, \cup_j B_\delta(x_j)) \leqslant \sqrt{D}\delta \Big\} = \bigcup_{j=1}^{\mathcal{N}_\delta(G)} \Big\{ x \in \delta\mathbb{Z}^D \;\Big|\; \operatorname{dist}(x, B_\delta(x_j)) \leqslant \sqrt{D}\delta \Big\}.$$

Следовательно, осталось доказать оценку

$$\Big| \Big\{ x \in \delta\mathbb{Z}^D \;\Big|\; \operatorname{dist}(x, B_\delta(y)) \leqslant \sqrt{D}\delta \Big\} \Big| \lesssim 1$$

независимо от положения точки y и значения параметра δ. Во-первых, избавимся от параметра δ, пользуясь растяжениями и произвольностью точки y:

$$\Big| \Big\{ x \in \delta\mathbb{Z}^D \;\Big|\; \operatorname{dist}(x, B_\delta(y)) \leqslant \sqrt{D}\delta \Big\} \Big| = \Big| \Big\{ \tilde{x} \in \mathbb{Z}^D \;\Big|\; \operatorname{dist}(\tilde{x}, B_1(\tilde{y})) \leqslant \sqrt{D} \Big\} \Big|, \quad \tilde{y} = \frac{y}{\delta}.$$

Во-вторых, избавимся от шара:

$$\Big| \Big\{ \tilde{x} \in \mathbb{Z}^D \;\Big|\; \operatorname{dist}(\tilde{x}, B_1(\tilde{y})) \leqslant \sqrt{D} \Big\} \Big| = \Big| \Big\{ \tilde{x} \in \mathbb{Z}^D \;\Big|\; \operatorname{dist}(\tilde{x}, \tilde{y}) \leqslant (1 + \sqrt{D}) \Big\} \Big|.$$

Теперь остаётся отметить, что для всякой точки $\tilde{x}$ из этого множества, шарик $B_{\frac{1}{2}}(\tilde{x})$ лежит в шаре $B_{\frac{3}{2}+\sqrt{D}}(y)$, и такие маленькие шарики дизъюнктны. Стало быть,

$$\Big| \Big\{ \tilde{x} \in \mathbb{Z}^D \;\Big|\; \operatorname{dist}(\tilde{x}, \tilde{y}) \leqslant (1 + \sqrt{D}) \Big\} \Big| \leqslant 2^D \Big(\frac{3}{2} + \sqrt{D} \Big)^D.$$

Таким образом, мы доказали соотношение $\mathcal{N}_\delta(G) \asymp |G_\delta|$ и можем приступить собственно к выводу следствия 4.2.6 из теоремы 4.2.5.

Рассмотрим теперь множество G_δ и выкинем из него, если надо, некоторые точки так, чтобы отображение $\pi_{-1}|_{G_\delta}$ стало инъективным, а множество $\pi_{-1}[G_\delta]$ не поменялось. Полученное множество назовём $\tilde{G}_\delta$. Рассуждая так же, как и при доказательстве неравенства $\mathcal{N}_\delta(G) \lesssim |G_\delta|$ (замечая, что каждая точка множества $\pi_{-1}(G)$ лежит в $\sqrt{2d}\delta$-окрестности множества $\pi_{-1}(G_\delta)$), запишем цепочку неравенств:

$$\mathcal{N}_\delta(\pi_{-1}(G)) \lesssim |\pi_{-1}(G_\delta)| = |\tilde{G}_\delta| \overset{\text{Теор.4.2.5}}{\lesssim} \Big(\max_{r=0,1,2,\infty} |\pi_r(\tilde{G}_\delta)| \Big)^{\frac{7}{4}}.$$

Стало быть, для завершения доказательства достаточно проверить неравенство

$$|\pi_r(\tilde{G}_\delta)| \lesssim \mathcal{N}_\delta(\pi_r(G))$$

для всякого $r = 0, 1, 2, \infty$. Вывод аналогичен доказательству неравенства $|G_\delta| \lesssim \mathcal{N}_\delta(G)$, приведённому выше. А именно, пусть $B_\delta(y_j)$, $j = 1, 2, \ldots, \mathcal{N}_\delta(\pi_r(G))$, — покрытие множества $\pi_r(G)$ шарами радиуса δ (в $\mathbb{R}^d$). Нетрудно видеть, что

$$\pi_r(\tilde{G}_\delta) \subset \pi_r(G_\delta) \subset \bigcup_{j=1}^{\mathcal{N}_\delta(\pi_r(G))} \Big\{ x \in \delta\pi_r[\mathbb{Z}^D] \;\Big|\; \operatorname{dist}(x, B_\delta(y_j)) \leqslant 2\sqrt{D}\delta \Big\},$$

поэтому результат будет следовать из оценки

$$\Big| \{ \tilde{x} \in \pi_r[\mathbb{Z}^D] \;\Big|\; \operatorname{dist}(\tilde{x}, \tilde{y}) \leqslant 1 + 2\sqrt{D} \Big\} \Big| \lesssim 1.$$

Это следует из того факта, что $\pi_r[\mathbb{Z}^D]$ — решётка. □

Вывод теоремы 4.2.2 из следствия 4.2.6. Пусть K — множество Безиковича в $\mathbb{R}^d$. Для всякой точки $\xi \in S^{d-1}$, выберем точки a_ξ, b_ξ, такие что $|b_\xi - a_\xi| = 1$, $b_\xi - a_\xi \parallel \xi$ и отрезок $[a_\xi, b_\xi]$ целиком содержится в множестве K. Рассмотрим множество $G \subset \mathbb{R}^{2d}$:

$$G = \{ (a_\xi, b_\xi) \mid \xi \in S^{d-1} \}$$

и применим к нему следствие 4.2.6. Заметим, что $\pi_0(G) \subset K$, $\pi_\infty(G) \subset K$, $\pi_1(G) \subset 2K$ и $\pi_2(G) \subset 3K$, где множества nK определяются как растяжения множества K в n раз (в частности, $\mathcal{N}_\delta(nK) \leqslant n^d \mathcal{N}_\delta(K)$). Поэтому,

$$\max_{r=0,1,2,\infty} \mathcal{N}_\delta(\pi_r(G)) \lesssim \mathcal{N}_\delta(K).$$

С другой стороны, по свойству построения точек a_ξ, b_ξ, имеет место равенство $\pi_{-1}(G) = S^{d-1}$ и поэтому $\mathcal{N}_\delta(\pi_{-1}(G)) \gtrsim \delta^{1-d}$. По следствию 4.2.6,

$$\mathcal{N}_\delta(K) \gtrsim \delta^{\frac{4}{7}(1-d)},$$

что и даёт оценку размерности:

$$\dim_{\text{Mink}} K = \varlimsup_{\delta \to 0} \frac{\log \mathcal{N}_\delta(K)}{|\log \delta|} \geqslant \frac{4}{7}(d-1).$$

□

Таким образом, нам осталось доказать теорему 4.2.5. Для этого нам будет удобно ввести несколько определений.

Определение 4.2.7. Пусть $f\colon X \to Y$ — отображение. Введём отношение эквивалентности на множестве X:

$$x_1 \sim x_2 \quad \Longleftrightarrow \quad f(x_1) = f(x_2).$$

Символом $[x]_f^X$ будем обозначать класс смежности элемента x относительно этого отношения эквивалентности.

Замечание 4.2.8. *Отметим простое, но очень важное неравенство*

$$\Big| \Big\{ x \in X \;\Big|\; |[x]_f^X| \geqslant \frac{|X|}{2|Y|} \Big\} \Big| \geqslant \frac{|X|}{2}.$$

Действительно, различных классов смежности не более Y, стало быть, объединение тех из них, мощность которых не превосходит $\frac{|X|}{2|Y|}$, покрывает не более половины множества X.

Определение 4.2.9. Улучшением множества X при помощи отображения f назовём множество

$$\left\{x \in X \;\middle|\; |[x]_f^X| \geqslant \frac{|X|}{2|Y|}\right\}.$$

В доказательстве теоремы 4.2.5 важную роль будет играть множество V:

$$V = \{((a,b_1),(a,b_2)) \in Z^4 \mid (a,b_1),(a,b_2) \in G\}.$$

Его можно интерпретировать как множество вертикальных отрезков с концами в множестве G.

Лемма 4.2.10. *Пусть* $N = \max_{r=0,1,2,\infty} |\pi_r(G)|$. *Тогда* $|V| \geqslant \frac{|G|^2}{N}$.

Доказательство. Пусть $a_1, a_2, \ldots, a_{\tilde{N}}$ — всевозможные значения первой координаты точек множества G (в частности, $\tilde{N} \leqslant N$), пусть

$$A_i = \{g \in G \mid \pi_0[g] = a_i\}, \quad i = 1, 2, \ldots, \tilde{N}.$$

Тогда $|V| = \sum_{i=1}^{\tilde{N}} |A_i|^2$, $|G|^2 = (\sum_{i=1}^{\tilde{N}} |A_i|)^2$ и утверждение леммы следует из неравенства Коши–Буняковского–Шварца. □

Лемма 4.2.11. *В условиях теоремы 4.2.5 и обозначении* $N = \max_{r=0,1,2,\infty} |\pi_r(G)|$, *имеет место оценка* $|V| \lesssim N^{\frac{5}{2}}$.

Замечание 4.2.12. *Теорема 4.2.5 есть прямой следствие лемм 4.2.10 и 4.2.11.*

Доказательство леммы 4.2.11. Рассмотрим функцию $\nu\colon V \to Z$, заданную по правилу

$$\nu((a,b_1),(a,b_2)) = a + 2b_1 - b_2.$$

Сначала покажем, что для всякого $w \in V$ имеет место неравенство

$$|[w]_\nu^V| \leqslant N. \tag{4.2.1}$$

Действительно, рассмотрим все пары $((a,b_1),(a,b_2))$, такие что

$$\nu((a,b_1),(a,b_2)) = (a - b_2) + 2b_1 = z$$

для некоторого фиксированного элемента $z \in Z$, определяющего класс эквивалентности. Отметим, что переменная b_1 пробегает не более чем N различных значений. Из инъективности π_{-1} следует, что для каждого значения b_1 существует не более одной пары (a,b_2), решающей уравнение. Стало быть, при фиксированном z всего решений не более N, что и доказывает неравенство (4.2.1).

Согласно неравенству (4.2.1), чтобы доказать лемму, достаточно найти элемент $w_0 \in V$, такой что

$$\left|[w_0]_\nu^V\right| \gtrsim \frac{|V|^2}{N^4}. \tag{4.2.2}$$

Рассмотрим ещё две функции, отображающие V в $Z \times Z$:

$$\pi_1 \otimes \pi_1[(a,b_1),(a,b_2)] = (a + b_1, a + b_2);$$
$$\pi_2 \otimes \pi_\infty[(a,b_1),(a,b_2)] = (a + 2b_1, b_2).$$

Отметим, что ν есть функция от каждой из этих функций (то есть, может быть представлена как композиция пары проекций и ещё какого-то отображения). Поэтому для всякого $w \in V$ и всякого множества $\tilde{V} \subset V$ имеют место вложения

$$[w]_\nu^{\tilde{V}} \supset [w]_{\pi_1\otimes\pi_1}^{\tilde{V}}; \quad [w]_\nu^{\tilde{V}} \supset [w]_{\pi_2\otimes\pi_\infty}^{\tilde{V}}. \tag{4.2.3}$$

Отметим также, что функции $\pi_1 \otimes \pi_1$ и $\pi_2 \otimes \pi_\infty$ порождают "трансверсальные разбиения" в том смысле, что если $\pi_1 \otimes \pi_1(v_1) = \pi_1 \otimes \pi_1(v_2)$ и $\pi_2 \otimes \pi_\infty(v_1) = \pi_2 \otimes \pi_\infty(v_2)$, то $v_1 = v_2$. Этот факт легко установить, решив линейную систему уравнений.

Теперь пришло время улучшений! Пусть W — улучшение множества V при помощи отображения $\pi_1 \otimes \pi_1$, а W_0 — улучшение множества W при помощи отображения $\pi_2 \otimes \pi_\infty$. Согласно замечанию 4.2.8, множество W_0 непусто (мы конечно же предположили $|V| \geqslant 4$, в противном случае нечего доказывать). Пусть $w_0 \in W_0$. В таком случае, вложения (4.2.3) позволяют заключить

$$\bigcup_{w \in [w_0]^W_{\pi_2 \otimes \pi_\infty}} [w]^V_{\pi_1 \otimes \pi_1} \subset [w_0]^V_\nu .$$

С другой стороны, по "трансверсальности" отображений $\pi_1 \otimes \pi_1$ и $\pi_2 \otimes \pi_\infty$, множества $[w]^V_{\pi_1 \otimes \pi_1}$, которые мы объединяем, дизъюнктны. Мощность каждого из них хотя бы $\frac{|V|}{2N^2}$, и всего их хотя бы $\frac{|V|}{4N^2}$, что и доказывает неравенство (4.2.2), а с ним и всю лемму. □

10.12.2018

4.3 Гипотеза Какейя в конечных полях

Зачастую в анализе для решения непрерывной задачи (про функции на евклидовом пространстве) строят дискретную модель (например, про функции на конечном или счётном множестве). Решают задачу в дискретной модели, после чего переносят решение на непрерывный случай. В случае гипотезы Какейя, дискретную постановку предложил Вольф.

Пусть $\mathbb{F}_q$ — конечное поле из q элементов, $\mathbb{F}_q^d$ есть d-мерное линейное пространство над ним.

Определение 4.3.1. Множество $K \subset \mathbb{F}_q^d$ назовём множеством Какейя, если для всякого элемента $y \in \mathbb{F}_q^d$ найдётся элемент $x \in \mathbb{F}_q^d$, такой что прямая

$$L_{y,x} = \{x + ay \mid a \in \mathbb{F}_q\} \tag{4.3.1}$$

целиком содержится в множестве K.

Дискретный аналог гипотезы Какейя таков: существует константа $C = C(d)$, такая что для всякого множества Какейя в $\mathbb{F}_q^d$ имеет место оценка $|K| \geqslant C(d)q^d$. В 2008 году З. Двир ([3]) доказал дискретную гипотезу Какейя.

Определение 4.3.2. Пусть $\delta, \gamma \in (0,1)$. Множество K назовём (δ,γ)-Какейя, если для хотя бы δq^d векторов $y \in \mathbb{F}_q^d$ существуют точки $x \in \mathbb{F}_q^d$, такие что прямая (4.3.1) пересекает множество K по хотя бы γq точкам.

Теорема 4.3.3. *Пусть множество K есть (δ,γ)-Какейя. Тогда*

$$|K| \geqslant C^{d-1}_{n+d-1}, \quad n = [q \min(\delta,\gamma)] - 2.$$

Следствие 4.3.4. *Если K — множество Какейя, то $|K| \geqslant C(d)q^{d-1}$.*

Следствие 4.3.5. *Для всякого числа $\varepsilon > 0$ существует константа $C = C(d,\varepsilon)$, такая что $|K| \geqslant Cq^{d-\varepsilon}$, если K — множество Какейя.*

Доказательство. Пусть число $r \in \mathbb{N}$ таково, что $\frac{1}{r} \leqslant \varepsilon$. Рассмотрим множество

$$\underbrace{K \times K \times \ldots \times K}_{r \text{ раз}} \subset \mathbb{F}_q^{dr}$$

и заметим, что это множество есть множество Какейя в $\mathbb{F}_q^{dr}$. Применив к нему следствие 4.3.4, получим оценку

$$|K|^r \geqslant Cq^{dr-1},$$

что после извлечения корня r-ой степени и даст требуемое неравенство. □

Припомним полезную лемму. Доказательство остаётся читателю в качестве упражнения.

Лемма 4.3.6 (Лемма Шварца–Зиппеля)**.** *Любой многочлен $f \in \mathbb{F}_q[x_1, x_2, \ldots, x_d]$ степени D, обнуляющийся в более чем Dq^{d-1} точках, тождественно равен нулю.*

Замечание 4.3.7. *Леммой Шварца–Зиппеля зачастую называют более общее утверждение.*

Доказательство теоремы 4.3.3. Предположим противное, пусть $|K| < C_{n+d-1}^{d-1}$. Иными словами, мощность множества K меньше, чем число различных мономов степени n в $\mathbb{F}_q[x_1, x_2, \ldots, x_d]$. Следовательно, существует однородный многочлен g степени n, такой что $g \neq 0$, но $g|_K = 0$. Мы хотим придти к противоречию с леммой Шварца–Зиппеля, доказав, что в таком случае у многочлена g более чем nq^{d-1} корень.

Пусть $\mathfrak{L} \subset \mathbb{F}_q^d$ есть множество хороших направлений:

$$\mathfrak{L} = \{y \mid \exists x \in \mathbb{F}_q^d \quad |K \cap L_{y,x}| \geqslant \gamma q\}.$$

Покажем, что $g(y) = 0$ если $y \in \mathfrak{L}$. В случае $y = 0$ всё и так ясно, так как многочлен g однороден, поэтому будем считать $y \neq 0$. Степень многочлена $a \mapsto g(x+ay)$ одной переменной не больше n. При этом он обнуляется хотя бы в $\gamma q \geqslant n + 2$ точках. Значит, он тождественно равен нулю. Посмотрим теперь на многочлен $b \mapsto g(bx + y)$. Достаточно доказать, что он тождественно равен нулю (тогда его значение в нуле равно нулю, а это и есть $g(y)$). Но по однородности $g(bx + y) = b^n g(x + b^{-1}y)$, если $y \neq 0$, а это выражение обнуляется при всех b^{-1}. Так как рассматриваемый многочлен тоже имеет степень не более n и обнуляется хотя бы в $\gamma q - 1 \geqslant n + 1$ точках, он тоже тождественно равен нулю.

Остаётся заметить, что $|\mathfrak{L}| \geqslant \delta q^d > nq^{d-1}$, что и даёт противоречие с леммой Шварца–Зиппеля. □

Упражнение 4.3.1. *Докажите, что множество Какейя в $\mathbb{F}_q^d$ удовлетворяет неравенству*

$$|K| \geqslant C_{q+d-1}^d \gtrsim q^d,$$

несколько изменив пространство многочленов в доказательстве теоремы 4.3.3.

Литература

[1] A. Balog, A. Szemerédi, *A statistical theorem of set addition*, Combinatorica **14**:3 (1994), 263–268.

[2] M. C. Chang, *A polynomial bound in Freiman's theorem*, Duke Math. J. **113** (2002), 289–311.

[3] Z. Dvir, *On the size of Kakeya sets in finite fields*, J. Amer. Math. Soc. **22** (2009), 1093–1097.

[4] Г. А. Фрейман, *Начала структурной теории сложения множеств*, Казань 1966.

[5] A. Geroldinger, I. Rusza, *Combinatorial number theory and additive group theory*, Advanced courses in Mathematics, CRM Barcelona, 2009.

[6] B. J. Green, *Structure theory of set addition*, Edinburgh lecture notes.

[7] W. T. Gowers, *Lower bounds of tower type for Szemeredi's regularity lemma*, Geom. Funct. Anal. **7** (1997), 322–337.

[8] W. T. Gowers, *A new proof of Szemerédi's theorem for arithmetic progressions of length four*, Geom. Funct. Anal., **8**:3 (1998), 529–551.

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

[10] K. Gyarmati, S. Konyagin, I. Z. Ruzsa, *Double and triple sums modulo a prime*, Additive Combinatorics, CRM Proceedings and Lecture Notes **43** (2007), 271–277.

[11] N. H. Katz, T. Tao, *New bounds for Kakeya problems*, J. d'Anal. Math. **87**:1 (2002), 231–263.

[12] G. Petridis, *Plunnecke's inequality*, Comb. Prob. Comt. **20**:6 (2011), 921–938.

[13] И. Д. Шкредов, *Теорема Семереди и задачи об арифметических прогрессиях*, УМН, **61**:6 (372) (2006), 111–178.

[14] И. Д. Шкредов, *Структурные теоремы в аддитивной комбинаторике*, УМН, **70**:1(421) (2015), 123–178.

[15] T. Tao, *A variant of the hypergraph removal lemma*, J. of Comb. Theory, ser. A **113**:7 (2006), 1257–1280.

[16] T. Tao, V. Vu, *Additive combinatorics*, Camb. Stud. Adv. Math., Camb. Univ. Press, 2010.

[17] T. Wolff, *Recent work connected with the Kakeya problem*, lecture notes.