

Некоторые задачи аддитивной комбинаторики

И. Д. Шкредов

Математический институт им. В.А. Стеклова

Введение

Пусть $\mathbf{G} = (\mathbf{G}, +)$ — (абелева) группа.

Тематика *аддитивной комбинаторики*: любые комбинаторные вопросы в формулировке которых присутствует групповая операция.

Сумма и разность множеств A, B

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

$$A - B = \{a - b : a \in A, b \in B\}.$$

Если $\mathcal{R} = (\mathcal{R}, +, *)$ — кольцо, то *произведение* множеств A, B

$$A * B = \{a * b : a \in A, b \in B\}.$$

Арифметическая комбинаторика (изучаются две операции одновременно).

Теорема Семереди, I

Теорема (Шур, 1916)

Пусть $h \in \mathbb{N}$. Для любой раскраски $\mathbb{N}$ в h цветов $C_1, \dots, C_h$ найдется цвет C_j и $x, y, z \in C_j$ такие, что

$$x + y = z.$$

Теорема (Ван дер Варден, 1927)

Пусть $h, k \in \mathbb{N}$. У любой раскраски $\mathbb{N}$ в h цветов найдется одноцветная прогрессия длины k .

Прогрессии длины три: $x + y = 2z$.

Теорема Семереди, II

Теорема (Семереди, 1969)

Пусть $A \subseteq \{1, 2, \dots, N\}$ — множество без прогрессий длины k .
Тогда

$$|A| = o(N), \quad N \rightarrow \infty.$$

Теорема Семереди влечет теорему Ван дер Вардена.

Графы: Атья, Семереди, Ружа.

Гиперграфы: Редл, Тао, Гауэрс.

Эргодический подход: Фюрстенберг, Орнштейн, Бергельсон, Лейбман, Тао, Аустин.

Аналитика: Гауэрс, Грин, Тао.

Теорема Семереди, III

Т. (Атья–Семереди, 1974, Фюрстенберг–Кацнельсон, 1978)

Пусть $A \subseteq \{1, 2, \dots, N\}^2$ — множество без конфигураций

$$\{(x, y), (x + d, y), (x, y + d)\}, \quad d \neq 0.$$

Тогда

$$|A| = o(N^2), \quad N \rightarrow \infty.$$

Теорема эквивалентна возвращаемости под действием двух коммутирующих операторов на пространстве с общей сохраняемой конечной мерой.

Теорема Семереди, IV

Теорема (Рот, 1953)

Пусть $A \subseteq \{1, 2, \dots, N\}$ — множество без прогрессий длины три.
Тогда

$$|A| = O\left(\frac{N}{\log \log N}\right).$$

Хиф–Браун (1987), Семереди (1990), Бурган (1999, 2008),
Сандерс (2011, 2012), Блум (2014).

Теорема (Гауэрс, 1998)

Пусть $A \subseteq \{1, 2, \dots, N\}$ — множество без прогрессий длины k .
Тогда

$$|A| = O\left(\frac{N}{(\log \log N)^{c_k}}\right), \quad c_k > 0.$$

Теорема Семереди, V

Теорема (Шкредов, 2006–2009)

Пусть $A \subseteq \{1, 2, \dots, N\}^2$ — множество без конфигураций

$$\{(x, y), (x + d, y), (x, y + d)\}, \quad d \neq 0.$$

Тогда

$$|A| = O\left(\frac{N^2}{(\log \log N)^C}\right), \quad C > 0.$$

Это двумерный аналог теоремы Рота.

Линейные уравнения, I

Теорема Ван дер Вардена:

$$x + y = 2z, \quad x, y, z \in A.$$

Теорема Шура:

$$x + y = z, \quad x, y, z \in A.$$

Общее аффинное линейное уравнение :

$$c_1 x_1 + \cdots + c_k x_k = 0,$$

где $c_1 + \cdots + c_k = 0$ и $x_j \in A$.

Теорема (Мешулам, 1995, Блум, 2014)

Пусть $A \subseteq \{1, 2, \dots, N\}$ — произвольное множество без решений уравнения

$$c_1 x_1 + \dots + c_k x_k = 0,$$

где $c_1 + \dots + c_k = 0$ и $x_j \in A$. Тогда для любого $\varepsilon > 0$

$$|A| = O\left(\frac{N}{(\log N)^{k-2+\varepsilon}}\right).$$

Теорема (Беренд, 1946)

Пусть $k \geq 2$. Найдется множество $A \subseteq \{1, 2, \dots, N\}$ такое, что

$$|A| \gg N \cdot \exp(-\sqrt{\log N})$$

и A не содержит нетривиальных решений уравнения

$$a_1 x_1 + \dots + a_k x_k = (a_1 + \dots + a_k) y.$$

Теорема (Шкредов–Шоен, 2014)

Пусть $A \subseteq \{1, 2, \dots, N\}$ — произвольное множество, не содержащее решений уравнения

$$c_1 x_1 + \dots + c_k x_k = 0,$$

где $c_1 + \dots + c_k = 0$ и $x_j \in A$. Тогда

$$|A| \ll N \cdot \exp(-(\log N)^{1/7}).$$

Снизу (Беренд) : $|A| \gg N \cdot \exp(-(\log N)^{1/2})$.

Задача Кахана, I

Пусть $\mathbb{T} = \mathbb{R}/(2\pi\mathbb{Z})$ и $A(\mathbb{T})$ — банахова алгебра непрерывных комплексных функций f с нормой

$$\|f\|_{A(\mathbb{T})} := \sum_{k \in \mathbb{Z}} |\hat{f}(k)| < \infty.$$

Здесь

$$\hat{f}(k) = (2\pi)^{-1} \int_{\mathbb{T}} f(t) e^{-ikt} dt, \quad k \in \mathbb{Z}.$$

Теорема (Берлинг–Хелсон, 1953)

Все эндоморфизмы алгебры $A(\mathbb{T})$ — тривиальны, то есть имеют вид

$$f(t) \rightarrow f(\nu t + t_0),$$

где $\nu \in \mathbb{Z}$.

Задача Кахана, II

Теорема (Берлинг–Хелсон, эквивалентная формулировка)

Пусть $\varphi : \mathbb{T} \rightarrow \mathbb{T}$ — непрерывное отображение со свойством

$$\|e^{in\varphi}\|_{A(\mathbb{T})} = O(1), \quad |n| \rightarrow \infty.$$

Тогда φ — линейно.

Гипотеза (Кахан, 1962)

Пусть $\varphi : \mathbb{T} \rightarrow \mathbb{T}$ — непрерывное отображение со свойством

$$\|e^{in\varphi}\|_{A(\mathbb{T})} = o(\log |n|), \quad |n| \rightarrow \infty.$$

Тогда φ — линейно.

Задача Кахана, III

Теорема (Лебедев, 2012)

Пусть $\varphi : \mathbb{T} \rightarrow \mathbb{T}$ — непрерывное отображение. Предположим, что

$$\|e^{in\varphi}\|_{A(\mathbb{T})} = o\left(\left(\frac{\log \log |n|}{(\log \log \log |n|)}\right)^{1/12}\right), \quad |n| \rightarrow \infty.$$

Тогда для некоторого $\nu \in \mathbb{Z}$ выполнено $\varphi(t) = \nu t + \varphi(0)$.

В доказательстве существенно использовались методы аддитивной комбинаторики.

Задача Кахана, IV

Теорема (Конягин–Шкрёдов, 2015)

Пусть $\varphi : \mathbb{T} \rightarrow \mathbb{T}$ — непрерывное отображение. Предположим, что

$$\|e^{in\varphi}\|_{A(\mathbb{T})} = o\left(\frac{\log^{1/22}|n|}{(\log \log |n|)^{3/11}}\right), \quad n \in \mathbb{Z}, \quad |n| \rightarrow \infty.$$

Тогда для некоторого $\nu \in \mathbb{Z}$ выполнено $\varphi(t) = \nu t + \varphi(0)$.

Таким образом, наш результат отличается от гипотезы Кахана

$$\|e^{in\varphi}\|_{A(\mathbb{T})} = o(\log |n|), \quad |n| \rightarrow \infty$$

лишь степенью $1/22$.

Задача Кахана и гипотеза Литтлвуда в $\mathbb{F}_p$

Теорема (Конягин–Шкредов, 2015)

Пусть p — простое число, $A \subset \mathbb{F}_p$ и

$$2 \leq |A| \leq \exp((\log p / \log \log p)^{1/3}).$$

Тогда

$$\|\chi_A\|_{A(\mathbb{F}_p)} \gg \log |A|.$$

Если же

$$\exp((\log p / \log \log p)^{1/3}) \leq |A| \leq p/3,$$

то при $p/|A| \rightarrow \infty$ выполнено

$$\|\chi_A\|_{A(\mathbb{F}_p)} \gg (\log(p/|A|))^{1/3} (\log \log(p/|A|))^{-1+o(1)}.$$

Это аналог гипотезы Литтлвуда в $\mathbb{F}_p$.

Общий принцип

Если $A \subseteq \mathcal{R}(+, *)$ и

$$|A + A|, |A * A| \leq |A|^{1+\epsilon},$$

то A имеет "большое" пересечение с подкольцом.

Исследователи: Эрдеш, Семереди, Элекеш, Бурган, Катц, Тао, Конягин, Глибичук, Гараев, Руднев, Чанг, Шоймоши,

Приложения: теория чисел, аддитивная комбинаторика, криптография, теоретическая информатика, динамические системы.

Суммы произведений, II

Теорема (Эрдеш–Семереди, 1983)

Пусть $A \subset \mathbb{Z}$, $|A| < \infty$. Тогда

$$\max\{|A + A|, |AA|\} \gg |A|^{1+c}, \quad |A| \rightarrow \infty,$$

где $c > 0$ — некоторая абсолютная константа.

Теорема (Бурган–Катц–Тао, 2004)

Пусть $A \subset \mathbb{F}_p$, $p^\delta < |A| < p^{1-\delta}$. Тогда

$$\max\{|A + A|, |AA|\} \gg |A|^{1+\varepsilon(\delta)},$$

где $\varepsilon(\delta) > 0$.

Суммы произведений, III

Теорема (Конягин–Шкредов, 2016)

Пусть $A \subset \mathbb{R}$. Тогда

$$\max\{|A + A|, |AA|\} \gg |A|^{4/3+c}, \quad |A| \rightarrow \infty,$$

где $c > 0$ — некоторая абсолютная константа.

Теорема (Роше-Ньютон–Руднев–Шкредов, 2016 и Языцы–Мерфи–Руднев–Шкредов, 2017)

Пусть $A \subset \mathbb{F}_p$, $|A| < p^{5/8}$. Тогда

$$\max\{|A + A|, |AA|\} \gg |A|^{1+1/5}.$$

Приложения: новые триг. суммы, распределение элементов мультипликативных подгрупп, аддитивная неприводимость и т.д.

Спасибо за внимание!