Math-Net.Ru

Общероссийский математический портал

С. В. Конягин, О теореме Фреймана в конечных полях,
Матем. заметки, 2008, том 84, выпуск 3, 472–474

DOI: <https://doi.org/10.4213/mzm5544>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением
<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 3.82.47.9

26 апреля 2023 г., 08:31:19

КРАТКИЕ СООБЩЕНИЯ

О теореме Фреймана в конечных полях

С. В. Конягин

Для подмножеств A, B аддитивной абелевой группы G обозначим

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

Пусть $|A|$ – мощность множества A . Для множества $A \subset G$, $0 < |A| < \infty$, рассмотрим его константу удвоения

$$\sigma(A) = \frac{|A + A|}{|A|}.$$

Теорема Фреймана [1] утверждает, что если константа удвоения множества $A \subset \mathbb{Z}$ мала, то A может быть покрыто небольшой обобщенной арифметической прогрессией. В данной работе рассматривается аналог теоремы Фреймана в линейном пространстве над полем порядка 2.

Пусть $\mathbb{F}_2$ – поле вычетов по модулю 2. Для любого конечного множества I рассмотрим группу по сложению

$$\mathbb{F}_2^I = \{(x_i)_{i \in I} : x_i \in \mathbb{F}_2 \text{ для всех } i \in I\}.$$

Для краткости будем писать $\mathbb{F}_2^n$ вместо $\mathbb{F}_2^{\{1, \dots, n\}}$. Если $J \subset I$, то мы имеем естественное вложение $\mathbb{F}_2^J$ в $\mathbb{F}_2^I$ (полагая $x_i = 0$ при $i \in I \setminus J$). В частности, при $m \leq n$ рассматриваем $\mathbb{F}_2^m$ как подмножество $\mathbb{F}_2^n$.

Пусть $K \geq 1$. Определим $F(K)$ как минимальную константу такую, что для любого конечного множества I и любого непустого $A \subset \mathbb{F}_2^I$ с константой удвоения $\sigma(A) \leq K$ найдется содержащее A аффинное подпространство $V \subset \mathbb{F}_2^I$ мощности $|V| \leq F(K)|A|$. Утверждение о конечности $F(K)$ для всех $K \geq 1$ называют теоремой Фреймана в $\mathbb{F}_2$. Ружи [2] доказал, что $F(K) \leq 2^{K^4}$ для всех $K \geq 1$. Верхние оценки для $F(K)$ улучшались в ряде работ (см. [3]–[5]). Недавно Грин и Тао [6] нашли асимптотику логарифма $F(K)$ при $K \rightarrow \infty$, установив, что

$$F(K) = 2^{2K + O(\sqrt{K} \log K)}, \quad K \geq 2. \quad (1)$$

Кроме того, в [6] отмечено, что

$$F(K) \geq 2^{2K - O(\log K)}, \quad K \geq 2. \quad (2)$$

Здесь и ниже $\log$ обозначает логарифм по основанию 2.

В данной заметке мы уточняем остаточный член в (1).

ТЕОРЕМА 1. Для $K \geq 2$ мы имеем

$$F(K) = 2^{2K + O(\log K)}.$$

Остается неясным, выполняется ли для достаточно больших K неравенство $F(K) \leq 2^{2K}$.

Для доказательства оценки сверху в неравенстве (1) авторы [6] сводят общий случай к рассмотрению множеств A специального вида: так называемых, SMD-множеств. Пусть $\{e^i\}_{i \in I}$ – стандартный базис в $\mathbb{F}_2^I$ (т.е. $e_j^i = \delta_{i,j}$, где $\delta_{i,j}$ – символ Кронекера). Мы говорим, что множество $A \subset \mathbb{F}_2^n$ является SMD-множеством, если выполнены следующие два условия:

- (а) если $i \in \{1, \dots, n\}$, $x \in A$, $x_i = 1$, то $x + e^i \in A$;
- (б) если $i, j \in \{1, \dots, n\}$, $i < j$, $x \in A$, $x_i = 0$, $x_j = 1$, то $x + e^i + e^j \in A$.

Для натуральных чисел $k \leq n$ через $H_k(n)$ обозначим шар в метрике Хемминга:

$$H_k(n) = \{x \in \mathbb{F}_2^n : |\{i : x_i = 1\}| \leq k\}.$$

Пусть $a, b, c \in \mathbb{F}_2^n$. Мы будем писать $ab = c$, если $a_i b_i = c_i$ для всех $i = 1, \dots, n$. Следующее предложение есть версия предложения 5.1 из [6] с улучшенным остаточным членом.

ПРЕДЛОЖЕНИЕ 1. *Предположим, что множества $A, B \subset \mathbb{F}_2^n$ удовлетворяют условиям $H_1(n) \subset A$, $B \subset A$ и $|A| \leq n^C$ для некоторого $C \geq 1$. Тогда*

$$|A + B| \geq \left(\frac{n}{2} - O(\log n)\right)|B|, \quad (3)$$

где константа в O зависит только от C .

Отметим, что при $C > 1$ остаточный член $O(\log n)$ в (3) имеет правильный порядок по n . В самом деле, пусть $k = \min(n - 1, [(C - 1) \log n])$,

$$A = B = \{x \in \mathbb{F}_2^n : |\{i > k : x_i = 1\}| \leq 1\}.$$

Тогда легко проверить, что множества A и B удовлетворяют условиям предложения 1 и $|A + B| \leq (n - k + 1)|B|/2$.

ДОКАЗАТЕЛЬСТВО ПРЕДЛОЖЕНИЯ 1. Следуя аргументам [6], легко показать, что достаточно ограничиться случаем, когда A и B являются SMD-множествами. Далее можно считать n достаточно большим. На протяжении доказательства будем считать эти условия выполненными. Предположим, что

$$|A + B| < \frac{n}{2}|B|. \quad (4)$$

Обозначим

$$K = [C \log n], \quad L = 4(K + 1), \quad M = [10C\sqrt{n} \log n], \quad N = M + \left\lceil \frac{n}{3} \right\rceil.$$

Заметим, что $K < L < M < N$. При указанных выше предположениях в [6] установлены следующие факты.

ЛЕММА 1. *Имеем $A \subset H_K(n)$.*

ЛЕММА 2. *Если $x \in A$, то имеется не более одного такого $i \geq M$, что $x_i = 1$.*

Мы докажем следующее утверждение.

ЛЕММА 3. *Для $x \in A$ не существует различных $i \geq L$ и $j \geq N$ таких, что $x_i = x_j = 1$.*

ДОКАЗАТЕЛЬСТВО. Предположим, что найдутся $x \in A$ и различные i, j такие, что $i \geq L$, $j \geq N$ и $x_i = x_j = 1$. Так как A является SMD-множеством, то оно содержит множество D , состоящее из элементов вида

$$e_i + e_j, \quad i \leq L, \quad M \leq j \leq N.$$

Оценим снизу количество различных элементов $z = a + b$ таких, что $a \in D$, $b \in B$ и $ab = 0$.

С одной стороны, количество допустимых пар (a, b) не меньше $|B|(L - K)(N - M)$. С другой стороны, в силу лемм 1 и 2 для фиксированного z количество допустимых a не превосходит $2(K + 1)$. Сопоставляя эти оценки, выводим

$$|A + B| \geq |B| \frac{(L - K)(N - M)}{2(K + 1)} \geq |B| \frac{n}{2},$$

что противоречит (4). Лемма 3 доказана.

Для $x \in \mathbb{F}_2^n$ обозначим

$$\nu(x) = |\{i : i \geq L, x_i = 1\}|.$$

Каждому элементу $b \in B$ сопоставим множество

$$I_b = \begin{cases} \{i : i \geq L, b_i = 0\}, & \text{если } \nu(b) \leq 1, \\ \{i : i \geq N\}, & \text{если } \nu(b) \geq 2. \end{cases}$$

Отметим, что в силу леммы 3 $b_i = 0$ при $i \in I_b$. Пусть

$$Z = \{b + e_i : b \in B, i \in I_b\}.$$

Для любого $z = b + e_i \in Z$ справедливо равенство $\nu(z) = \nu(b) + 1$. Для $z \in Z$ через $\mu(z)$ обозначим количество представлений $z = b + e_i$, $b \in B$, $i \in I_b$. Оценим снизу $A + B$:

$$|A + B| \geq |Z| \geq \sum_{b \in B} \sum_{i \in I_b} \frac{1}{\mu(b + e_i)}.$$

Если $\nu(b) \leq 1$, то

$$\sum_{i \in I_b} \frac{1}{\mu(b + e_i)} \geq \sum_{i \in I_b} \frac{1}{\nu(b + e_i)} \geq \sum_{i \in I_b} \frac{1}{2} \geq \frac{n - L}{2}.$$

Если $\nu(b) \geq 2$, то в силу леммы 3 снова

$$\sum_{i \in I_b} \frac{1}{\mu(b + e_i)} = \sum_{i \in I_b} 1 = n - N + 1 \geq \frac{n - L}{2}.$$

Следовательно,

$$|A + B| \geq |B| \frac{n - L}{2}.$$

Тем самым предложение 1 доказано.

Доказательство теоремы 1 проводится точно так же, как вывод (1) в [6], с заменой предложения 5.1 из [6] на предложение 1.

Работа выполнена во время визита автора в Институт высших исследований в Принстоне. Автор благодарит институт за гостеприимство и превосходные условия для работы и Oswald Veblen Fund за финансовую поддержку.

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

- [1] Г. А. Фрейман, *Основания структурной теории сложения множеств*, Казанский гос. пед. ин-т, Казань, 1966. [2] I. Ruzsa, *Structure Theory of Set Addition*, Astérisque, **258**, Soc. Math. France, Paris, 1999, 323–326. [3] J. M. Deshouillers, F. Hennecart, A. Plagne, *Combinatorica*, **24**:1 (2004), 53–68. [4] B. J. Green, I. Z. Ruzsa, *Bull. London Math. Soc.*, **38**:1 (2006), 43–52. [5] T. Sanders, *A note of Freiman's theorem in vector spaces*, [arXiv: math/0605523](https://arxiv.org/abs/math/0605523). [6] B. Green, T. Tao, *Freiman's theorem in finite fields via extremal set theory*, [arXiv: math/0703668](https://arxiv.org/abs/math/0703668).

С. В. Конягин

Московский государственный
университет им М. В. Ломоносова

E-mail: konyagin@ok.ru

Поступило

09.01.2008