Известия НАН Армении, Математика, том 54, н. 2, 2019, стр. 82 – 89

О ПОДМНОЖЕСТВАХ ЛИНЕЙНЫХ ПРОСТРАНСТВ НАД КОНЕЧНЫМ ПОЛЕМ, ОДНОЗНАЧНО ОПРЕДЕЛЯЕМЫХ НАБОРОМ ПОПАРНЫХ СУММ ИХ ЭЛЕМЕНТОВ

Д. САРГСЯН

Ереванский государственный университет
E-mail: *davit.sargsyan.1993@gmail.com*

Аннотация. Через F_3^n обозначим n-мерное линейное пространство над конечным полем F_3. Для подмножества $A = \{a_1, a_2, ..., a_N\}$ в F_3^n обозначим через $A + A$ совокупность сумм пар различных элементов A. Говорят, что A однозначно определяется набором $A+A$, если для любого $B \subseteq F_3^n$ с $|A| = |B|$ и $A+A = B+B$ следует, что $A = B$. В настоящей статье найдены все значения N, для которых всякое $A \subset F_3^n$, состоящее из N элементов однозначно определяется посредством $A + A$.

MSC2010 number: 11B75.

Ключевые слова: пары различных элементов; единственность.

1. Введение

Пусть F_3^n – n-мерное линейное пространство над конечным полем F_3. Набор элементов C из F_3^n записывается как $C = \{c_1^{[m_1]}, c_2^{[m_2]}, \dots, c_N^{[m_N]}\}$, где $c_i \in F_3^n, m_i > 0$. Кратность элемента $s \in F_3^n$ в C обозначается через

$$count_C(s) = \sum_{\substack{1 \le i \le N \\ s = c_i}} m_i.$$

Отметим, что не исключается возможность $c_i = c_j, i \neq j$. Мощность набора C обозначается через $|C| = m_1 + m_2 + \cdots + m_N$. Наборы A и B в F_3^n считаются равными тогда и только тогда, когда для всякого $s \in F_3^n$ имеет место равенство $count_A(s) = count_B(s)$. Основные операции над наборами понимаются следующим образом. Для любого $s \in F_3^n$

$$count_{A \cup B}(s) = count_A(s) + count_B(s)$$

$$count_{A \cap B}(s) = min\{count_A(s), count_B(s)\}$$

$$count_{A \setminus B}(s) = max\{count_A(s) - count_B(s), 0\}$$

Мы используем запись $C \subset F_3^n$ как для наборов, так и для подмножеств в F_3^n; каждая ситуация будет ясна из контекста. Определим $set(C)$ как

$$set(C) = \{s \mid s \in F_3^n, count_C(s) > 0\}$$

Пусть A, B - подмножества в F_3^n. Сумма A и B определяется как

$$A + B = \{(a+b)^{[1]} \mid a \in A, b \in B, a \neq b\}$$

Отметим, что каждая пара различных элементов в $A \times A$ рассматривается только один раз, и по определению $A + A$ - это набор сумм пар различных элементов A. Если $|A| = 1$, то $A + A = \emptyset$. Сходным образом, для набора $C = \{c_1^{[m_1]}, c_2^{[m_2]}, \ldots, c_N^{[m_N]}\}$ в F_3^n определяется

$$C + C = \{(c_i + c_j)^{[m_i \cdot m_j]} \mid 1 \leq i < j \leq N\} \cup \{2c_i^{[\binom{m_i}{2}]} \mid i = 1, \ldots, N\}$$

Для элемента $c \in F_3^n$ положим

$$c + C = \{c^{[1]}\} + C = \{(c + c_i)^{[m_i]} \mid 1 \leq i \leq N\}$$

Пример 1.1. Пусть $A, B \subseteq F_3^1 = F_3$ и $A = \{0, 1\}$, $B = \{1, 2\}$. Тогда $A + B = \{0^{[1]}, 1^{[1]}, 2^{[1]}\}, A + A = \{1^{[1]}\}, B + B = \{0^{[1]}\}$. Для $C = \{0^{[3]}, 1^{[3]}\}$ имеем $C + C = \{0^{[3]}, 1^{[9]}, 2^{[3]}\}$.

Замечание 1.1. *В выражениях, содержащих наборы или множества, типа $A + A \cup B + B$, операция $+$ имеет более высокий приоритет чем $\cup$ и $\cap$. Для непересекающихся подмножеств A, B в F_3^n верна следующая формула:*

$$(A \cup B) + (A \cup B) = A + A \cup A + B \cup B + B$$

Для наборов C, D, E в F_3^n из условия $C \cup D = C \cup E$ следует, что $D = E$.

2. Основная теорема

Пусть $A = \{a_1, a_2, ..., a_N\}$ - подмножество в F_3^n. A однозначно определяется набором $A + A$, если для всякого $B \subseteq F_3^n$, такого что $A + A = B + B$(очевидно с $|A| = |B|$) следует что $A = B$. В настоящей статье мы определяем значения параметра N, для которых все подмножества $A \subset F_3^n$ с N элементами однозначно определяются набором $A + A$. Аналогичная задача для натуральных чисел предложена Л. Мозером в [1] и содержтися в [2] как задача 15.12 на странице page 106. Случай алгебраически замкнутого поля характеристики 0 решен Селфриджем и Страусом в [3]. Рассмотренный нами случай также решает проблему над конечным полям характеристики 3. Обзор результатов по этой тематике можно найти в [4].

Теорема 2.1. *Для любого $N, 1 \leq N \leq 3^n - 1$, в F_3^n найдутся два разных подмножества A и B, такие что $|A| = |B| = N$ и $A + A = B + B$, тогда и только тогда, когда $N \not\equiv 0 mod 3$ и $N \neq 3^n - 1$.*

Предложение 2.1. *Если $1 \leq N \leq 3^n - 1$ и $N \not\equiv 0 mod 3, N \neq 3^n - 1$, то найдутся различные подмножества $A, B \subseteq F_3^n$, такие что $|A| = |B| = N$ и $A + A = B + B$.*

Доказательство. Применим индукцию по n. Если $n = 1$, тогда $N = 1$ и для $A = \{0\}, B = \{1\}$ имеем $A + A = B + B = \emptyset$. Пусть теперь $n > 1$ и утверждение верно для всех меньших значений. Ввиду $N \neq 0 mod 3$ рассмотрим следующие случаи:

Случай 1: $N < 3^{n-1} - 1$.

Согласно индуктивному предположению найдутся два разных подмножества $A, B \subset F_3^{n-1}$, такие что $|A| = |B| = N$ и $A + A = B + B$. Определим

$$C = \{(x_1, \ldots, x_{n-1}, 0) \mid (x_1, \ldots, x_{n-1}) \in A\}, \quad D = \{(x_1, \ldots, x_{n-1}, 0) \mid (x_1, \ldots, x_{n-1}) \in B\}.$$

Очевидно, что $|C| = |D| = N$ и $C + C = D + D$.

Случай 2: $N = 3^{n-1} - 1$.

Пусть L - это подпространство в F_3^n, состоящее из всех векторов с последней нулевой координатой. Положим $a = (0, 0, \ldots, 0, 0), b = (1, 0, \ldots, 0, 0), c = (2, 0, \ldots, 0, 0), M = L \setminus \{a, b, c\}, d = (2, 2, \ldots, 2, 1), e = (1, 2, \ldots, 2, 1)$. Рассмотрим множества $A = \{c, d\} \cup M$ и $B = \{a, e\} \cup M$. Имеем $|A| = |B| = 3^{n-1} - 1 = N$. Для $m \in M$ оба $b + m$ и $c + m \in M$. Следовательно, $c + M = M$ и $c + M = a + (c + M) = a + M$. Подобным образом, из $b + M = M$ получаем $d + M = (e + b) + M = c + (b + M) = e + M$. Поэтому, $c + d = a + e$, $c + M = a + M$, $d + M = e + M$, и $A + A = B + B$. Например, при $n = 3$

$$A = \{(2, 2, 1), (2, 0, 0), (0, 1, 0), (0, 2, 0), (1, 1.0), (1, 2.0), (2, 1.0), (2, 2, 0)\},$$

$$B = \{(1, 2, 1), (0, 0, 0), (0, 1, 0), (0, 2, 0), (1, 1, 0), (1, 2, 0), (2, 1, 0), (2, 2, 0)\}.$$

Случай 3: $3^{n-1} < N < 2 \cdot 3^{n-1} - 1$.

Пусть $M = N - 3^{n-1}, 0 < M < 3^{n-1} - 1$. Пусть L - подмножество в F_3^n, состоящее из всех векторов с последней координатой, равной 2. Согласно случаю 1 найдутся подмножества $C, D \subset F_3^n$, такие что $C \neq D, |C| = |D| = M, C + C = D + D$ и $x_n = 0$ для всех $(x_1, \ldots, x_n) \in C \cup D$. Положим $A = L \cup C, B = L \cup D$. Тогда $A \neq B$ и $|A| = |B| = N$. Для $c = (c_1, \ldots, c_n) \in C$ имеем $c_n = 0$, поэтому $c + L = L$ и $C + L = \{e^{[M]} \mid e \in L\}$. Аналогично $D + L = \{e^{[M]} \mid e \in L\}$ и $C + L = D + L$. Так как $A + A = C + C \cup L + L \cup C + L$ и $B + B = D + D \cup L + L \cup D + L$, получаем $A + A = B + B$.

Случай 4: $N = 2 \cdot 3^{n-1} - 1$.

Положим $M = 3^{n-1} - 1$. Пусть L - подмножество в F_3^n, состоящее из всех векторов с последней координатой, равной 2. Согласно случаю 2 найдутся подмножества $A = \{d\} \cup A_1, B = \{e\} \cup B_1 \subseteq F_3^n$, такие что $A \neq B, |A| = |B| = M, d = (d_1, \ldots, d_{n-1}, 1), e = (e_1, \ldots, e_{n-1}, 1)$, $x_n = 0$ для всех $(x_1, \ldots, x_n) \in A_1 \cup B_1$, и $A + A = B + B$. Положим $C = L \cup A, D = L \cup B$. Тогда $C \neq D$ и $|C| = |D| = N$.

Заметим также, что $d+L=e+L$. Для $a=(a_1,\ldots,a_n)\in A_1$ получаем $a+L=L$ и $A_1+L=\{e^{[M-1]}\mid e\in L\}$. Похожим образом, $B_1+L=\{e^{[M-1]}\mid e\in L\}$ и $A_1+L=B_1+L$. Теперь $C+C=D+D$ непосредственно следует из $A+A=B+B, d+L=e+L$, и $A_1+L=B_1+L$.

Случай 5: $2\cdot 3^{n-1}<N<3^n-1$.
Пусть L - это подмножество в F_3^n, состоящее из всех векторов с последней ненулевой координатой. Согласно случаю 1 найдутся подмножества $C,D\subseteq F_3^n$, такие что $C\neq D, |C|=|D|=N-2\cdot 3^{n-1}$, $x_n=0$ для всех $(x_1,\ldots,x_n)\in C\cup D$ и $C+C=D+D$. Положим $A=L\cup C, B=L\cup D$. Тогда $A\neq B, |A|=|B|=N$ и $A+A=B+B$ как и в предыдущих двух случаях. □

Лемма 2.1. *Если A,B - два разных набора в F_3, таких что $|A|=|B|=N$ и $A+A=B+B$, тогда $N\not\equiv 0 mod 3$.*

Доказательство. Обозначим $n_i=count_A(i), m_i=count_B(i), i\in F_3$. Из соображений симметрии следует рассмотреть следующие случаи:

Случай 1: $|set(A)|=|set(B)|=1$.
Если $set(A)=set(B)$ то $A=B$, что приводит к противоречию. Поэтому $set(A)\neq set(B)$. Пусть, к примеру, $A=\{0^{[N]}\}, B=\{1^{[N]}\}$. При $N=1$ все очевидно, в противном случае $A+A\neq B+B$ и получается противоречие.

Случай 2: $|set(A)|=1, |set(B)|\geq 2$.
Имеем $|set(A+A)|=1$. При $N=2$ все очевидно, в противном случае $|set(B+B)|\geq 2$ и потому $A+A\neq B+B$.

Случай 3: $|set(A)|=|set(B)|=2$.
Из $|set(A)|=|set(B)|=2$ получаем, что $n_i=0$ только для одного $i\in\{0,1,2\}$, и $m_j=0$ только для одного $j\in\{0,1,2\}$. Пусть $i=j$. Без потери общности можем предположить, что $i=j=0$, то есть $A=\{1^{[n_1]},2^{[n_2]}\}, B=\{1^{[m_1]},2^{[m_2]}\}$. Из $A+A=B+B$ получается $\binom{n_1}{2}=\binom{m_1}{2}$ и $\binom{n_2}{2}=\binom{m_2}{2}$ (вычисляя кратности 1 и 2 в $A+A$ и $B+B$). Тогда $n_1=m_1, n_2=m_2$, и $A=B$ - противоречие. Следовательно $i\neq j$. Без потери общности можем предположить, что $i=2$ и $j=0$:

$$A=\{0^{[n_0]},1^{[n_1]}\}, B=\{1^{[m_1]},2^{[m_2]}\}$$

Вычисляя кратности 2 в $A+A$ и $B+B$ получаем $\binom{n_1}{2}=\binom{m_1}{2}$ и $n_1=m_1=n$. Из $|A|=|B|=N$ следует $n_0=m_2=m$. Поэтому,

$$A=\{0^{[m]},1^{[n]}\}, B=\{1^{[n]},2^{[m]}\}$$

Приравнивая кратности 1 в $A+A$ и $B+B$ получаем $mn=\binom{m}{2}$. Отсюда $m=2n+1$ и $N=3n+1\not\equiv 0 mod 3$.

Случай 4: $|set(A)| = 3, |set(B)| = 2$.

Без потери общности можем предположить, что $m_0 = 0$ и, тогда, $A = \{0^{[n_0]}, 1^{[n_1]}, 2^{[n_2]}\}$, $B = \{1^{[m_1]}, 2^{[m_2]}\}$ и

$$n_0 + n_1 + n_2 = m_1 + m_2 \tag{2.1}$$

Приравнивая кратности 1 и 2 в $A + A$ и $B + B$ получаем

$$\binom{n_2}{2} + n_0 n_1 = \binom{m_2}{2}, \qquad \binom{n_1}{2} + n_0 n_2 = \binom{m_1}{2}. \tag{2.2}$$

Покажем, что $(n_0 + n_1 + n_2) \not\equiv 0 mod 3$. Из (2.2) следует $m_2 > n_2$ и $m_1 > n_1$; поэтому, $m_2 = n_2 + y$, $m_1 = n_1 + x$, где x, y - натуральные числа.

Ввиду (2.1) $n_0 = x + y$. Подставим выражения для n_0, m_1, и m_2 в (2.2) и (??):

$$\begin{cases} n_1 x + n_1 y - n_2 y &= \binom{y}{2} \\ n_2 x + n_2 y - n_1 x &= \binom{x}{2} \end{cases}$$

Решив систему уравнений получаем:

$$2n_1 = y - \frac{2yx + y^2}{x^2 + yx + y^2}, \qquad 2n_2 = x - \frac{2yx + x^2}{x^2 + yx + y^2}.$$

Из натуральности $x, y \in N$ следует, что $x - 2n_2 \in (0, 2)$. Так как $x - 2n_2$ - целое, то $x = 2n_2 + 1$. Аналогично, $y = 2n_1 + 1$. Из $n_0 = x + y$ получаем, что $n_0 + n_1 + n_2 = 3(n_1 + n_2) + 2 \not\equiv 0 mod 3$.

Случай 5: $|set(A)| = |set(B)| = 3$.

Имеем $n_i > 0$ и $m_i > 0, i = 0, 1, 2$. Докажем, что для $C = A \setminus \{0^{[1]}, 1^{[1]}, 2^{[1]}\} = \{0^{[n_0-1]}, 1^{[n_1-1]}, 2^{[n_2-1]}\}$ и $D = B \setminus \{0^{[1]}, 1^{[1]}, 2^{[1]}\} = \{0^{[m_0-1]}, 1^{[m_1-1]}, 2^{[m_2-1]}\}$ верно $C + C = D + D$. Из

$$0 + C = \{0^{[n_0-1]}, 1^{[n_1-1]}, 2^{[n_2-1]}\}$$
$$1 + C = \{0^{[n_2-1]}, 1^{[n_0-1]}, 2^{[n_1-1]}\}$$
$$2 + C = \{0^{[n_1-1]}, 1^{[n_2-1]}, 2^{[n_0-1]}\}$$

следует $0 + C \cup 1 + C \cup 2 + C = \{0^{[N-3]}, 1^{[N-3]}, 2^{[N-3]}\}$. Набор $0 + C \cup 1 + C \cup 2 + C$ не зависит от элементов C, а зависит только от мощности C. Ввиду $A = C \cup \{0^{[1]}, 1^{[1]}, 2^{[1]}\}$, получаем

$$A + A = C + C \cup 0 + C \cup 1 + C \cup 2 + C \cup \{0^{[1]}, 1^{[1]}, 2^{[1]}\} + \{0^{[1]}, 1^{[1]}, 2^{[1]}\}$$
$$= C + C \cup \{0^{[N-3]}, 1^{[N-3]}, 2^{[N-3]}\} \cup \{0^{[1]}, 1^{[1]}, 2^{[1]}\} = C + C \cup \{0^{[N-2]}, 1^{[N-2]}, 2^{[N-2]}\}$$

Аналогично, $B + B = D + D \cup \{0^{[N-2]}, 1^{[N-2]}, 2^{[N-2]}\}$. Теперь уже $C + C = D + D$ следует из $A + A = B + B$.

Таким образом, мы всегда можем предположить, без потери общности, что либо

$|set(A)| < 3$, либо $|set(B)| < 3$; ибо в противном случае положив $k = min\{n_0, n_1, n_2, m_0, m_1, m_2\}$ рассмотрим наборы $C = A \setminus \{0^{[k]}, 1^{[k]}, 2^{[k]}\}, D = B \setminus \{0^{[k]}, 1^{[k]}, 2^{[k]}\}$, для которых $C + C = D + D, C \neq D$, либо $|set(C)| < 3$, либо $|set(D)| < 3$, и $|C| = |D| \equiv N mod 3$. Так, что этот случай сводится к рассмотренным выше. □

Лемма 2.2. *Пусть A, B - разные наборы в $F_3^n, n > 1$, такие что $|A| - |B| - N$ и $A + A = B + B$. Найдутся разные наборы $A_L, B_L \subseteq F_3^{n-1}$, такие что $|A_L| = |B_L| = N$ и $A_L + A_L = B_L + B_L$.*

Доказательство. Положим $A = \{a_1^{[m_1]}, a_2^{[m_2]}, \ldots, a_M^{[m_M]}\}$, $B = \{b_1^{[n_1]}, b_2^{[n_2]}, \ldots, b_N^{[n_N]}\}$. Пусть L какое-либо 1-мерное подпространство в F_3^n. Фактор-пространство F_3^n/L изоморфно F_3^{n-1}. Имея это ввиду, построим два набора в F_3^{n-1} заменяя каждый элемент в A и B на содержащий его смежный класс по подпространству L:

$$A_L = \{(a_1 + L)^{[m_1]}, (a_2 + L)^{[m_2]}, \ldots, (a_M + L)^{[m_M]}\}$$

$$B_L = \{(b_1 + L)^{[n_1]}, (b_2 + L)^{[n_2]}, \ldots, (b_N + L)^{[n_N]}\}$$

Из $A+A = B+B$ следует, что $A_L+A_L = B_L+B_L$. Для завершения доказательства покажем, что L может быть выбрано так, чтобы $A_L \neq B_L$.
Положим $C = A \cap B, D = A \setminus C, E = B \setminus C$, тогда $D \cap E = \emptyset$ и $|D| = |E|$. В самом деле, для любого $s \in F_3^n$

$$count_D(s) = max\{count_A(s) - count_C(s), 0\}$$

$$count_E(s) = max\{count_B(s) - count_C(s), 0\}$$

Из $C = A \cap B$ следует $count_C(s) \leq count_A(s)$ и $count_C(s) \leq count_B(s)$. Далее,

$$count_D(s) = count_A(s) - count_C(s)$$

$$count_E(s) = count_B(s) - count_C(s)$$

Окончательно,

$$|D| = \sum_{s \in F_3^n} count_D(s) = \sum_{s \in F_3^n} count_A(s) - count_C(s)$$

$$= \sum_{s \in F_3^n} count_A(s) - \sum_{s \in F_3^n} count_C(s) = |A| - |C|$$

Аналогично, $|E| = |B| - |C|$ и $|D| = |E|$ следует из $|A| = |B|$.

Из соображений симметрии следует рассмотреть следующие случаи:

Случай 1: $|set(D)| = |set(E)| = 1$.
То есть, $A = \{d^{[k]}\} \cup C, B = \{e^{[k]}\} \cup C$, и $d \neq e$. Выберем L таким образом, чтобы d и e принадлежали бы разным смежным классам по L. Ясно, что A_L и B_L будут разными.

Случай 2: $|set(D)| = 2, |set(E)| = 1$.
Пусть $D = \{d_1^{[p]}, d_2^{[l]}\}$ и $E = \{e^{[k]}\}, k = p + l$. Рассмотрим $L = \{0, d_1 - d_2, -d_1 + d_2\}$. Имеем $d_1 + L = d_2 + L = H = \{d_1, d_2, -d_1 - d_2\}$. Предположим, что $A_L = B_L$. Это означает, что $D_L \cup C_L = E_L \cup C_L$, что влечет $D_L = E_L$ и $e + L = d_1 + L = H$. Ввиду $D \cap E = \emptyset$, получаем $e = -d_1 - d_2$. Теперь, если $d_1 \neq 0$ и $d_2 \neq 0$, то для $L_1 = \{0, -d_1 - d_2, d_1 + d_2\}$ получается $d_1 + L_1 \neq e + L_1$ и $A_{L_1} \neq B_{L_1}$. В противном случае, если один из d_1, d_2 равен нулю, скажем $d_1 = 0$, получим $e = -d_2$. Выбрав $c \in F_3^n \setminus \{0, d_2, -d_2\}$, и положив $L_2 = \{0, c, -c\}$, получим $d_1 + L_2 \neq e + L_2$ и $A_{L_2} \neq B_{L_2}$.

Случай 3: $|set(D)| = |set(E)| = 2$.
Пусть $D = \{d_1^{[m]}, d_2^{[n]}\}, E = \{e_1^{[p]}, e_2^{[k]}\}, m + n = p + k$, и $L = \{0, d_1 - d_2, -d_1 + d_2\}$. Тогда $d_1 + L = d_2 + L = H = \{d_1, d_2, -d_1 - d_2\}$. Если $A_L = B_L$, то $e_1 + L = e_2 + L = H$. Тогда все d_1, d_2, e_1, e_2 лежат в H, и, ввиду $D \cap E = \emptyset$, это противоречит тому, что $|H| = 3$. Поэтому $A_L \neq B_L$.

Случай 4: $|set(D)| > 2$.
Пусть $|set(D)| = P > 2$ и $D = \{d_1^{[k_1]}, d_2^{[k_2]}, \dots d_P^{[k_P]}\}, d_i \neq d_j, 1 \leq i, j \leq P$. Положим $L_1 = \{0, d_1 - d_2, -d_1 + d_2\}$. Предположим, что $A_{L_1} = B_{L_1}$. Из $d_1 + L_1 = d_2 + L_1 = H = \{d_1, d_2, -d_1 - d_2\}$ и $A_{L_1} = B_{L_1}$, следует, что найдется $e_1 \in E$ такое что $e_1 + L_1 = H$. Из $D \cap E = \emptyset$ следует $e_1 = -d_1 - d_2$ и $-d_1 - d_2 \notin D$. Так как $d_i + L_1 \neq H, i > 2$, и $e + L_1 \neq H, e \in E, e \neq e_1$, получаем $count_E(e_1) = k_1 + k_2$. Аналогично, если для $L_2 = \{0, d_1 - d_3, -d_1 + d_3\}$ имеет место $A_{L_2} = B_{L_2}$, тогда $e_2 = -d_1 - d_3 \in E$ и $count_E(e_2) = k_1 + k_3$. Продолжая получим $L_1 = \{0, d_1 - d_2, -d_1 + d_2\}, L_2 = \{0, d_1 - d_3, -d_1 + d_3\}, \dots, L_{P-1} = \{0, d_1 - d_P, -d_1 + d_P\}$, для которых $e_1 = -d_1 - d_2, e_2 = -d_1 - d_3, \dots, e_{P-1} = -d_1 - d_P$, и $count_E(e_1) = k_1 + k_2, count_E(e_2) = k_1 + k_3, \dots, count_E(e_{P-1}) = k_1 + k_P$. Ясно, что

$$\begin{aligned} |E| &\geq count_E(e_1) + count_E(e_2) + \cdots + count_E(e_{P-1}) \\ &= (k_1 + k_2) + (k_1 + k_3) \cdots + (k_1 + k_P) \\ &= (P-2) \cdot k_1 + k_1 + \cdots + k_P = (P-2) \cdot k_1 + |D| \end{aligned}$$

Ввиду $P > 2$, получаем $|D| < |E|$, что противоречит тому, что $|D| = |E|$. Следовательно, $A_{L_i} \neq B_{L_i}$ для некоторого $i, 1 \leq i \leq P - 1$. □

Лемма 2.3. *Если существуют разные подмножества $A, B \subset F_3^n$, такие что $|A| = |B| = N$ и $A + A = B + B$, тогда $N \not\equiv 0 mod 3$.*

Доказательство. Пусть $A = \{a_1, \dots, a_N\}, B = \{b_1, \dots, b_N\}$. Так как множества могут быть рассмотрены в качестве наборов, из леммы 2 следует, что найдутся

разные наборы $A_L, B_L \subseteq F_3^{n-1}$ такие что $|A_L| = |B_L| = N$ и $A_L + A_L = B_L + B_L$. Если $n-1 > 1$, применив лемму 2 к A_L и B_L получим разные наборы $A_{L_1}, B_{L_1} \subseteq F_3^{n-2}$, такие что $|A_{L_1}| = |B_{L_1}| = N$ и $A_{L_1} + A_{L_1} = B_{L_1} + B_{L_1}$. Продолжим применять лемму 2 пока не получим разные наборы $C, D \subseteq F_3^1 = F_3$, такие что $|C| = |D| = N$ и $C + C = D + D$. Условие $N \not\equiv 0 mod 3$ последует из леммы 2.1. □

Лемма 2.4. *Если существуют разные подмножества $A, B \subseteq F_3^n$, такие что $|A| = |B| = N$ и $A + A = B + B$, тогда $N \neq 3^n - 1$.*

Доказательство. Предположим, что $A = F_3^n \setminus \{e_1\}$ и $B = F_3^n \setminus \{e_2\}, e_1 \neq e_2$. Пусть $C = F_3^n \setminus \{e_1, e_2\}$. Тогда, $A + A = e_2 + C \cup C + C = B + B = e_1 + C \cup C + C$ и

$$e_1 + C = e_2 + C \tag{2.3}$$

Множество $e_1 + C$ является сдвигом C. Поэтому $|e_1 + C| = |C| = |F_3^n| - 2$. Из $e_2 \notin C$ следует $e_1 + e_2 \notin e_1 + C$. Если $-e_1 \in e_1 + C$, то $-e_1 - e_1 = -2e_1 = e_1 \in C$, что противоречит $e_1 \notin C$. Следовательно, $e_1 + C = F_3^n \setminus \{e_1 + e_2, -e_1\}$. Аналогично, $e_2 + C = F_3^n \setminus \{e_1 + e_2, -e_2\}$. Из $e_1 \neq e_2$ получается $e_1 + C \neq e_2 + C$, что противоречит (2.3). □

Из лемм 2.3 и 2.4 следует следующее утверждение.

Предложение 2.2. *Если существуют разные подмножества $A, B \subseteq F_3^n$, такие что $|A| = |B| = N$ и $A + A = B + B$, тогда $N \not\equiv 0 mod 3$ и $N \neq 3^n - 1$.*

Комбинируя предложения 2.1 и 2.2 получаем доказательство основной теоремы.

Abstract. Let F_3^n be an n-dimensional linear space over the finite field F_3. Let $A = \{a_1, a_2, ..., a_N\}$ be a set in F_3^n and $A + A$ be the collection of sums of pairs of distinct elements in A. It is said, that A is uniquely determined by $A + A$ if for any $B \subseteq F_3^n$ such that $|A| = |B|$ and $A + A = B + B$ it follows that $A = B$. In this paper, we find those values of N for which any set $A \subset F_3^n$ containing N elements is determined uniquely by $A + A$.

Список литературы

[1] L. Moser, Problem E 1248, Amer. Math. Monthly, 507 pages, (1957).
[2] László Lovász, Combinatorial Problems and Exercises, American Mathematical Soc. (1979).
[3] J. Selfridge and E. G. Straus, Pac. J. Math. 8, 847 – 856 (1958).
[4] D. Fomin, "Is Multiset of n Integers Uniquely Determined by the Multiset of its s-sums"? arXiv:1709.06046v3 [math.NT] 16 Nov 2017.

Поступила 26 января 2018
После доработки 21 июля 2018
Принята к публикации 15 сентября 2018