Об ограничениях на накрытие конечных семейств натуральных чисел

П. С. Дергач (МГУ им. М. В. Ломоносова, Москва)

В работе рассматривается задача о накрытии семейства A натуральных чисел минимальным количеством арифметических прогрессий с запретом на накрытие элементов другого конечного семейства B. Более точно, нас интересует нахождение минимального количества $f(A)$ элементов в семействе B, которых достаточно, чтобы сделать накрытие семейства A наиболее сложным, то есть имеющим максимально возможное количество арифметических прогрессий. Приводятся соответствующие верхние и нижние оценки на $f(A)$ в зависимости от мощности семейства A.

Ключевые слова: арифметическая прогрессия, натуральный ряд, сложность накрытия.

Постановка задачи

Пусть A и B — непустые попарно непересекающиеся конечные подмножества натурального ряда:

$$A, B \subset \mathbb{N};\ |A|, |B| < \infty;\ A \cap B = \varnothing;$$
$$A = \{a_1, a_2, \ldots, a_n\},\ B = \{b_1, b_2, \ldots, b_m\}.$$

Пусть $a \in \mathbb{N}$ и $b \in \mathbb{N} \cup \{0\}$. Через (a, b) обозначаем множество

$$\{a + ib \mid i \in \mathbb{N} \cup \{0\}\}$$

и называем его *арифметической прогрессией с началом в a и шагом b*. Говорим, что конечная система арифметических прогрессий *пересекается в совокупности,* если общее пересечение этих прогрессий не пусто. Для произвольного $M \subseteq \mathbb{N}$ обозначаем через $\dim M$ минимальное количество попарно непересекающихся арифметических прогрессий, дающих в объединении M. В самой общей постановке задачи необходимо найти следующую величину:

$$f(A,B) = \operatorname{argmin}\{\dim M : A \subseteq M \subseteq \mathbb{N}/B\}.$$

В рамках данной курсовой работы была изучена следующая вспомогательная задача: по данному конечному множеству $A \subset \mathbb{N}$ необходимо найти минимальное число $m(A)$ элементов в множестве $B \subset \mathbb{N}$, которых все еще достаточно для выполнения условия $f(A,B) = |A|$.

Основные утверждения и их доказательства

Лемма 1. *Для любых $a, b, c, d \in \mathbb{N}$ верно*

$$(a,b) \cap (c,d) \neq \varnothing \iff a - c \equiv 0 \pmod{\text{НОД}(b,d)}.$$

Доказательство леммы см. в [1].

Утверждение 1. *Любая конечная система попарно пересекающихся арифметических прогрессий пересекается в совокупности.*

Доказательство проведем индукцией по количеству n арифметических прогрессий в системе. При $n = 1$ утверждение тривиально. Пусть для n прогрессий утверждение уже доказано. Рассмотрим систему из $n+1$ попарно пересекающихся арифметических прогрессий. Пусть это $\{(a_i, b_i)\}_{i=1}^{n+1}$. Так как все прогрессии попарно не пересекаются, то по предположению индукции пересечение первых n прогрессий $(a_1, b_1), \ldots, (a_n, b_n)$ непусто. Пусть x — минимальное число из этого пересечения. Очевидно, что тогда это пересечение само образует арифметическую прогрессию с началом в x и шагом $\text{НОК}(b_1, \ldots, b_n)$, который мы обозначим через y. Докажем от противного, что

$$(x, y) \cap (a_{n+1}, b_{n+1}) \neq \varnothing. \tag{1}$$

Если это не так, то по лемме 1 получили бы, что $x - a_{n+1}$ не делится на $\text{НОД}(y, b_{n+1})$. То есть, найдется такое простое число p и натуральная степень k, для которых y и b_{n+1} делятся на p^k, но

$$x - a_{n+1} \not\equiv 0 \pmod{p^k}. \tag{2}$$

Мы знаем, что

$$(a_i, b_i) \cap (a_{n+1}, b_{n+1}) \neq \varnothing$$

для всех $i = 1, \ldots, n$. Поэтому из леммы 1 получаем:

$$a_{n+1} - a_i \equiv 0 \pmod{\text{НОД}(b_i, b_{n+1})} \tag{3}$$

для всех $i = 1, \ldots, n$. Кроме того, при всех $i = 1, \ldots, n$ верно, что $x \in (a_i, b_i)$, то есть что

$$x - a_i \equiv 0 \pmod{b_i}. \tag{4}$$

Из (3) и (4) теперь выводим

$$x - a_{n+1} \equiv 0 \pmod{\text{НОД}(b_i, b_{n+1})} \tag{5}$$

для всех $i = 1, \ldots, n$. Далее, y делится на p^k и $y = \text{НОК}(b_1, \ldots, b_n)$. Значит для некоторого натурального $s \in \{1, \ldots, n\}$ обязательно b_s делится на p^k. Так как b_{n+1} делятся на p^k, то отсюда получаем, что $\text{НОД}(b_s, b_{n+1})$ делится на p^k. А это, в свою очередь, противоречит выполнению условий (2) и (5). Из выполнения условия (1) теперь тривиально следует, что все семейство $\{(a_i, b_i)\}_{i=1}^{n+1}$ арифметических прогрессий пересекается в совокупности. Утверждение доказано.

Утверждение 2. *Для любого $n \in \mathbb{N}$ существует такое $A \subset \mathbb{N}$, что $|A| = n$ и $m(A) = 1$.*

Доказательство. Определим рекурсивно бесконечную последовательность $\{x_n\}$ натуральных чисел. Пусть $x_1 = 1$, $x_2 = 2$. Если мы уже построили n первых чисел последовательности, то возьмем по определению

$$x_{n+1} := x_n + \text{НОК}(x_i - x_j), \text{ где НОК берется по всем } 1 \leqslant i < j \leqslant n.$$

Так как для любых $i < j < k$, $i, j, k \in \mathbb{N}$ верно, что $x_k - x_j$ делится нацело на $x_j - x_i$, то

$$x_k \in (x_i, x_j - x_i) \text{ для всех } i < j < k,\ i, j, k \in \mathbb{N}. \tag{6}$$

Положим теперь

$$A := \{x_1, x_2, \ldots, x_n\},\ B := \{x_{n+1}\}.$$

Тогда из (6) следует, что любая арифметическая прогрессия, содержащая более одного числа из множества A, обязательно включает в себя элемент из множества B. Поэтому

$$f(A, B) \geqslant |A| = n.$$

Достижимость оценки тривиально следует из того, что

$$A = (x_1, 0) \cup (x_2, 0) \cup \ldots \cup (x_n, 0).$$

Утверждение доказано.

Утверждение 3. *Для любого $n \in \mathbb{N}$ существует такое $A \subset \mathbb{N}$, что $|A| = n$ и $m(A) \geqslant \left[\frac{n}{2}\right]$.*

Доказательство. Если n четно, то в качестве A можно взять множество

$$A := \{1, 2, \ldots, \frac{n}{2}, 1 + n, 2 + n, \ldots, \frac{n}{2} + n\}.$$

Если же n нечетно, то в качестве A можно взять множество

$$A := \{1, 2, \ldots, \frac{n-1}{2}, n, 1 + n, 2 + n, \ldots, \frac{n-1}{2} + n\}.$$

И в том, и в другом случае для выполнения условия

$$f(A, B) = n \tag{7}$$

необходимо, чтобы в B было хотя бы по одному элементу из прогрессий $(1, n), (2, n), \ldots, (\left[\frac{n}{2}\right], n)$, так как иначе можно было бы одним элементом из B «накрыть» сразу два элемента из A. Так как эти прогрессии попарно не пересекаются, то для любого множества B, удовлетворяющего условию (7), будет обязательно верно, что $|B| \geqslant \left[\frac{n}{2}\right]$. Значит $m(A) \geqslant \left[\frac{n}{2}\right]$. Утверждение доказано.

Утверждение 4. *Для любого конечного $A \subset \mathbb{N}$ верно, что $m(A) \leqslant |A| - 2$.*

Доказательство. Упорядочим элементы множества A в порядке возрастания и обозначим их через $a_1, a_2, a_3, \ldots, a_n$, где n — мощность A. Заметим, что прогрессии

$$(a_1, a_2 - a_1), (a_1, a_3 - a_1), (a_2, a_3 - a_2) \tag{8}$$

попарно пересекаются. Из утверждения 1 следует существование такого числа b_1, которое лежит в каждой из прогрессий в (8). Очевидно, можно выбрать b_1 так, чтобы оно не лежало в A. Далее, для каждого натурального $i = \overline{4, n}$ рассмотрим семейство прогрессий

$$T_i := \{(a_1, a_i - a_1), (a_2, a_i - a_2), \ldots, (a_{i-1}, a_i - a_{i-1}),$$
$$(a_{i+1}, a_{i+1} - a_i), \ldots, (a_n, a_n - a_i)\}.$$

Все прогрессии этого семейства имеют общую точку пересечения a_i. Поэтому для всех $i = \overline{4, n}$ существует число b_i, лежащее в каждой из прогрессий семейства T_i. Очевидно, можно подобрать эти числа так, чтобы они не лежали в A. Таким образом, если взять в качестве B множество $\{b_1\} \cup \{b_4\} \cup \{b_5\} \ldots \cup \{b_n\}$, то оно обязательно «перекроет» все возможные способы «закрыть» одной прогрессией более одного элемента из A. То есть, будет выполнено условие $f(A, B) = n$. Осталось заметить, что $|B| \leqslant n - 2$. Строгое неравенство здесь возможно, если некоторые из чисел b_i совпадают. Значит $m(A) \leqslant n - 2 = |A| - 2$. Утверждение доказано.

Список литературы

[1] Дергач П. С. О каноническом регулярном представлении S-тонких языков // Интеллектуальные системы. — 2014. — Т. 18, вып. 1. — С. 211–242.