СИБИРСКИЙ ЖУРНАЛ ИССЛЕДОВАНИЯ ОПЕРАЦИЙ
Апрель – июнь 1994. Том 1, № 2, 40–60

УДК 519.147

О СЛОЖНОСТИ ПОКРЫТИЙ ЧИСЛОВЫХ МНОЖЕСТВ АРИФМЕТИЧЕСКИМИ ПРОГРЕССИЯМИ*)

А. Д. Коршунов

Пусть $M_n = \{1, \dots, n\}$, R — произвольное подмножество из M_n и $A(R)$ — минимальное число арифметических прогрессий, теоретико-множественная сумма которых совпадает с R. Показывается, что для почти каждого подмножества $R \subseteq M_n$

$$n(\log_2 n)^{-1}(1 - \varepsilon(n)) < A(R) < 1,6n(\log_2 n)^{-1},$$

где $\varepsilon(n) \to 0$ при $n \to \infty$, т. е. сложность покрытия арифметическими прогрессиями почти каждого подмножества из M_n по порядку равна $n/\log_2 n$. Доказательство нижней оценки для $A(R)$ основано на использовании мощностных соображений, а верхняя оценка для $A(R)$ извлекается из предложенного алгоритма для получения покрытия (не обязательно наилучшего) произвольного подмножества из M_n арифметическими прогрессиями.

§ 1. Введение. Формулировка результатов

Наиболее известный вариант дискретных задач о покрытии состоит в следующем. Заданы конечное множество V и некоторая система W подмножеств из V такая, что для любого элемента $a \in V$ имеется по крайней мере один элемент из W, которому принадлежит a. Требуется найти наименьшую по числу подмножеств подсистему $P \subseteq W$, удовлетворяющую определенным условиям и такую, чтобы любой элемент из V принадлежал по крайней мере одному элементу из P.

Сформулированная задача о покрытии является важной дискретной экстремальной задачей: ряд известных проблем комбинаторного анализа, теории графов, теории дизъюнктивных нормальных форм для булевых функций, теории тестов и других областей может быть сформулирован как задачи о покрытии.

---

*) Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований (код проекта 93-011-1484) и Международного научного фонда (ISF).

Некоторые конкретные задачи о покрытии решаются довольно просто (например, задача о минимальной связывающей сети, задача о максимальном паросочетании в графе). Однако большинство задач о покрытии более сложны и им присущи трудности, характерные для многих дискретных экстремальных задач. Более подробные сведения о таких задачах имеются, например, в обзоре [1].

Поскольку надежды на отыскание эффективных алгоритмов для точного решения всех задач о покрытии весьма призрачны, естественно рассматривать простые в вычислительном отношении алгоритмы, посредством которых удается отыскивать хотя и не минимальные покрытия, но достаточно близкие к ним. К таким алгоритмам относятся так называемые жадные алгоритмы (иначе: градиентные алгоритмы, алгоритмы наискорейшего спуска). На каждом шаге жадный алгоритм выбирает элемент из R, покрывающий наибольшее число элементов из V, не покрытых на предыдущих шагах. Используя жадные алгоритмы, для ряда задач о покрытии удалось получить верхние оценки для сложности наилучших покрытий [1]. Однако эти оценки, как правило, существенно отличаются от имеющихся нижних оценок, часто получаемых мощностным методом. Есть основания полагать, что на самом деле для многих задач о покрытии жадные алгоритмы доставляют более экономные покрытия, чем получаемые верхние оценки. Однако к настоящему времени мы не располагаем методами для понижения этих оценок. Поэтому продвижение в решении конкретных задач о покрытии способствует прогрессу в решении и лучшем понимании задач дискретной оптимизации.

В [2, 3] нами были описаны новые алгоритмы построения дизъюнктивных нормальных форм (ДНФ) для булевых функций. Для большинства таких функций эти алгоритмы позволяют находить ДНФ, сложности которых по порядку совпадают со сложностями наилучших ДНФ.

Оказывается, что основная идея этих алгоритмов применима и для решения других задач о покрытии. В настоящей статье рассматривается одна из них — задача о покрытии произвольного подмножества из отрезка натуральных чисел арифметическими прогрессиями [4]. Постановка этой задачи состоит в следующем.

Пусть $M_n = \{1, \ldots, n\}$, R — произвольное подмножество из M_n и $A(R)$ — минимальное число арифметических прогрессий, теоретико-множественная сумма которых совпадает с R. Тогда величина

$$A(n) = \max_{R \subseteq M_n} A(R)$$

объявляется сложностью «самого плохого» подмножества из M_n . Требуется найти величину $A(n)$.

Первые нетривиальные результаты по решению рассматриваемой задачи получили С. С. Кислицын и А. А. Сапоженко [4]. Они установили следующие факты:

а) при любом $n > 2$ справедливо неравенство (всюду в настоящей статье $\log$ обозначает логарифм по основанию 2):

$$A(n) \geqslant n/(3\log n); \tag{1.1}$$

б) для почти каждого подмножества $R \subseteq M_n$ справедливо неравенство

$$A(R) < n \ln 2 \log\log n (2\log n)^{-1}(1 + o(1)).$$

Оценка (1.1) была в последствии улучшена в работе [5]:

$$A(n) \geqslant n/(2\log n - 1).$$

В. В. Глаголев [6] рассматривал эту задачу со следующим дополнительным ограничением: все прогрессии, образующие покрытие, должны иметь одну и ту же разность. Им было показано, что для наилучшего покрытия «самого плохого» подмножества из M_n число требуемых прогрессий асимптотически равно $n/4$.

В настоящей статье доказываются следующие два утверждения.

Теорема 1.1. *Для почти каждого подмножества $R \subseteq M_n$*

$$A(R) \geqslant n(\log n)^{-1}(1 - \varepsilon(n)),$$

где $\varepsilon(n) \to 0$ при $n \to \infty$.

Теорема 1.2. *Для почти каждого подмножества $R \subseteq M_n$*

$$A(R) < 1,6n(\log n)^{-1}$$

при $n \to \infty$.

Следствие 1.1. *Сложность покрытия арифметическими прогрессиями почти каждого подмножества из M_n по порядку равна $n/\log n$.*

Поскольку в настоящей статье речь идет только об арифметических прогрессиях, начиная с этого места, прилагательное «арифметическая» будем опускать.

Теорема 1.1 доказывается в § 2. Основная же цель статьи состоит в доказательстве теоремы 1.2. Алгоритм выделения прогрессий, покрывающих произвольное $R \subseteq M_n$, описывается в § 3, а далее исследуется сложность получаемых покрытий.

§ 2. Доказательство теоремы 1.1

Для произвольного подмножества R из $M_n = \{1, \dots, n\}$ через $U(R, l)$ обозначим совокупность всех прогрессий длины l, содержащихся в R, а

через $S(R,l)$ — число элементов из R, каждый из которых принадлежит по крайней мере одной прогрессии из $U(R,l)$. Пусть $\overline{S}(n,l)$ есть среднее значение величины $S(R,l)$, взятое по всем подмножествам R из M_n, т. е.

$$\overline{S}(n,l) = 2^{-n} \sum_{R \subseteq M_n} S(R,l) < l2^{-n} \sum_{R \subseteq M_n} |U(R,l)|. \tag{2.1}$$

Пусть P_l обозначает произвольную прогрессию длины l в M_n. На множестве пар (R, P_l) рассмотрим предикат $B(R, P_l)$, задаваемый следующим образом:

$$B(R,P_l) = \begin{cases} 1, & \text{если } P_l \subseteq R; \\ 0 & \text{в противном случае.} \end{cases}$$

Тогда, очевидно, имеем

$$\sum_{R \subseteq M_n} |U(R,l)| = \sum_{R \subseteq M_n} \sum_{P_l \subseteq M_n} B(R,P_l) = \sum_{P_l \subseteq M_n} \sum_{R \subseteq M_n} B(R,P_l).$$

Ясно, что при фиксированной прогрессии P_l имеет место равенство

$$\sum_{R \subseteq M_n} B(R,P_l) = 2^{n-l}.$$

Пользуясь этим фактом и тем, что каждая прогрессия длины l задается первым членом (не более n возможностей) и разностью (не более n/l возможностей), имеем

$$\sum_{R \subseteq M_n} |U(R,l)| = \sum_{P_l \subseteq M_n} 2^{n-l} < n^2 l^{-1} 2^{n-l}. \tag{2.2}$$

Подставляя (2.2) в (2.1), получаем $\overline{S}(n,l) < n^2 2^{-l}$. Пусть $l_1 = \lceil \log n + 2\log\log n \rceil$. Тогда при больших n имеем

$$\sum_{l \geqslant l_1} \overline{S}(n,l) < n^2 \sum_{l \geqslant l_1} 2^{-l} < 2n(\log n)^{-2}. \tag{2.3}$$

Из (2.3) и неравенства Чебышева [7] следует, что при $n \to \infty$ почти каждое подмножество R из M_n обладает следующим свойством: не более чем $n/\log n$ элементов из R принадлежат прогрессиям, длины которых не меньше величины l_1.

Обозначим через $V(n)$ совокупность подмножеств $R \subseteq M_n$ таких, что R может быть покрыто не более чем

$$v_0 = \lfloor n(\log n)^{-1}(1 - 3\log\log n/\log n) \rfloor \tag{2.4}$$

прогрессиями, причем не более чем $\lfloor n/\log n\rfloor$ элементов из R покрываются прогрессиями длины не менее l_1. Поскольку каждая совокупность прогрессий из M_n однозначно задает покрываемое множество, то все подмножества из M_n можно получить следующим способом.

1. Из M_n выбирается такое r-элементное подмножество, которое можно покрыть прогрессиями длины не менее l_1, где $r \leqslant n/\log n$. При больших n имеется не более $\sum_{r=0}^{n/\log n}\binom{n}{r} = o(2^n)$ возможностей.

2. Из множества тех прогрессий на множестве M_n, каждая из которых имеет менее l_1 членов, выбирается v прогрессий, $1 \leqslant v \leqslant v_0$. Поскольку каждая прогрессия однозначно задается первым членом (не более n возможностей), разностью (менее n возможностей) и числом членов (менее l_1 возможностей), то при больших n в M_n имеется менее $n^2 l_1 < 2n^2\log n$ прогрессий длины менее l_1. Поэтому при больших n число возможностей не превосходит величины

$$\sum_{v=0}^{v_0}\binom{\lfloor 2n^2\log n\rfloor}{v} < \binom{\lfloor 2n^2\log n\rfloor}{v_0} < 2(en^2\log n/v_0)^{v_0}$$
$$< (\text{ см. } (2.4)) < (3n\log^2 n)^{v_0} = o(2^n).$$

Следовательно, при $n\to\infty$ имеем $|V(n)| = o(2^n)$. Таким образом, для покрытия почти каждого подмножества $R \subseteq M_n$ требуется использовать более v_0 прогрессий. Теорема 1.1 доказана.

§ 3. Алгоритм построения покрытия

Введем следующие обозначения:

$$l_0 = \lfloor \log n - 4\log\log n\rfloor, \tag{3.1}$$
$$z = \lfloor \log\log\log n\rfloor + 2, \tag{3.2}$$
$$l^* = \lfloor l_0 2^{-z}\rfloor. \tag{3.3}$$

Пусть R — произвольное подмножество из M_n.

- Прогрессия P называется *тупиковой в* R, если P не является собственной частью другой прогресии в R с той же разностью, что и P.

Покрытие множества R будем осуществлять только подходящими тупиковыми прогрессиями длины от l^* до l_0 и прогрессиями длины 2. Делается это так.

1. Пусть $H_{0,1}(n)$ — множество первых $h_{0,1}$ натуральных чисел, где

$$h_{0,1} = \lfloor l_0^{-1}2^{l_0+1}\ln 2\rfloor. \tag{3.4}$$

С множеством $H_{0,1}(n)$ связывается совокупность $S_{0,1}(n)$ возрастающих прогрессий $P \subseteq M_n$ длины l_0 таких, что P принадлежит $S_{0,1}(n)$ тогда и только тогда, когда разность прогрессии P принадлежит $H_{0,1}(n)$. Прогрессия P из $S_{0,1}(n)$ включается в покрытие множества R тогда и только тогда, когда P принадлежит R и является тупиковой в R.

2. Пусть $l_1 = \lfloor l_0/2 \rfloor$ и $H_{1,1}(n)$ — множество натуральных чисел, начиная с $h_{0,1}+1$ и кончая $h_{1,1}$, где

$$h_{1,1} - h_{0,1} = \lfloor l_1^{-1} 2^{2l_1} \ln 2 \rfloor. \tag{3.5}$$

С множеством $H_{1,1}(n)$ связывается совокупность $S_{1,1}(n)$ возрастающих прогрессий $P \subseteq M_n$ длины l_1 таких, что $P \in S_{1,1}(n)$ тогда и только тогда, когда разность прогрессии P принадлежит $H_{1,1}(n)$. Прогрессия P из $S_{1,1}(n)$ включается в покрытие множества R тогда и только тогда, когда $P \subseteq R$, P является тупиковой в R и не пересекается ни с одной прогрессией из $S_{0,1}(n)$, уже включенной в покрытие множества R.

3. Пусть $l_2 = \lfloor l_0/4 \rfloor$ и $H_{2,1}(n)$ — множество натуральных чисел, начиная с $h_{1,1}+1$ и кончая $h_{2,1}$, где

$$h_{2,1} - h_{1,1} = \lfloor l_2^{-1} 2^{3l_2-1} \ln 2 \rfloor.$$

Аналогично пусть $H_{2,2}(n)$ — множество натуральных чисел, начиная с $h_{2,1}+1$ и кончая $h_{2,2}$, где

$$h_{2,2} - h_{2,1} = \lfloor l_2^{-1} 2^{4l_2-2} \ln 2 \rfloor.$$

С множествами $H_{2,1}(n)$, $H_{2,2}(n)$ соответственно связываются множества $S_{2,1}(n)$, $S_{2,2}(n)$ возрастающих прогрессий $P \subseteq M_n$ длины l_2 таких, что $P \in S_{2,1}(n)$ тогда и только тогда, когда разность прогрессии P принадлежит $H_{2,1}(n)$, и $P \in S_{2,2}(n)$ тогда и только тогда, когда разность прогрессии P принадлежит $H_{2,2}(n)$.

4. Прогрессия P из $S_{2,1}(n)$ включается в покрытие множества R тогда и только тогда, когда $P \subseteq R$, P является тупиковой в R и не пересекается с теми прогрессиями из $S_{0,1}(n)$, $S_{1,1}(n)$, которые уже включены в покрытие множества R.

5. Прогрессия P из $S_{2,2}(n)$ включается в покрытие множества R тогда и только тогда, когда $P \subseteq R$, P является тупиковой в R и не пересекается с теми прогрессиями из $S_{0,1}(n)$, $S_{1,1}(n)$, $S_{2,1}(n)$, которые уже включены в покрытие множества R.

6. Пусть необходимые прогрессии длин $l_0, l_1, l_2, \ldots, l_{i-1}$ включены в покрытие множества R, $i \leqslant z$. Тогда рассматриваются 2^{i-1} множеств $H_{i,1}(n), \ldots, H_{i,2^{i-1}}(n)$. Множество $H_{i,1}(n)$ состоит из натуральных чисел, начиная с $h_{i-1,2^{i-2}}+1$ и кончая $h_{i,1}$, где

$$h_{i,1} - h_{i-1,2^{i-2}} = \lfloor l_i^{-1} 2^{(l_i-1)(2^{i-1}+1)+2} \ln 2 \rfloor, \quad l_i = \lfloor l_0 2^{-i} \rfloor. \tag{3.6}$$

Множество $H_{i,2}(n)$ состоит из натуральных чисел, начиная с $h_{i,1}+1$ и кончая $h_{i,2}$, где

$$h_{i,2}-h_{i,1}=\lfloor l_i^{-1}2^{(l_i-1)(2^{i-1}+2)+2}\ln 2\rfloor,$$

и т. д. Вообще, при $1<j\leqslant 2^{n-1}$ в $H_{i,j}(n)$ входит $h_{i,j}-h_{i,j-1}$ натуральных чисел, начиная с $h_{i,j-1}+1$ и кончая $h_{i,j}$, где

$$h_{i,j}-h_{i,j-1}=\lfloor l_i^{-1}2^{(l_i-1)(2^{i-1}+j)+2}\ln 2\rfloor. \tag{3.7}$$

С каждым множеством $H_{i,j}(n)$, $1\leqslant j\leqslant 2^{i-1}$, связывается совокупность $S_{i,j}(n)$ возрастающих прогрессий $P\subseteq M_n$ длины l_i таких, что $P\in S_{i,j}(n)$ тогда и только тогда, когда разность прогрессии P принадлежит множеству $H_{i,j}(n)$.

7. Последовательно из каждого $S_{i,j}(n)$ некоторые прогрессии отбираются в покрытие множества R следующим способом. Прогрессия P из $S_{i,1}(n)$ включается в покрытие множества R тогда и только тогда, когда $P\subseteq R$, P является тупиковой в R и не пересекается с теми прогрессиями длины более l_i, которые уже включены в покрытие множества R. Отбор прогрессий из $S_{i,2}(n),\dots,S_{i,2^{i-1}}(n)$ осуществляется индуктивно. Если все необходимые прогрессии из $S_{i,1}(n),\dots,S_{i,j-1}(n)$ уже включены в покрытие множества R, то прогрессия P из $S_{i,j}(n)$ включается в покрытие множества R тогда и только тогда, когда $P\subseteq R$, P является тупиковой в R и не пересекается как с отобранными прогрессиями длины более l_i, так и с уже отобранными прогрессиями из $S_{i,1}(n),\dots,S_{i,j-1}(n)$.

8. Элементы из R, которые не принадлежат объединению отобранных прогрессий, покрываются прогрессиями длины 2. В результате получается искомое покрытие множества R прогрессиями.

Убедимся, что при рассматриваемых i и j из множества M_n можно выбирать подмножества $H_{i,j}(n)$ указанных мощностей. Для этого достаточно показать, что при больших n

$$|H_{0,1}(n)|+\sum_{i=1}^{z}\sum_{j=1}^{2^{i-1}}|H_{i,j}(n)|<n(\log n)^{-3}. \tag{3.8}$$

Справедливость (3.8) вытекает из следующих соотношений:

$$|H_{0,1}(n)|<(\text{ см. (3.4)})<2^{l_0}/l_0<(\text{ см. (3.1)})<n(\log n)^{-4},$$

при любом i, $1\leqslant i\leqslant z$,

$$|H_{i,1}(n)|+|H_{i,2}(n)|+\ldots+|H_{i,2^{i-1}}(n)|<(\text{ см. (3.7)})$$
$$<2|H_{i,2^{i-1}}(n)|<l_i^{-1}2^{(l_i-1)2^i+2^{i-1}+2}<l_i^{-1}2^{l_0-2^{i-1}+2}.$$

Следовательно,

$$\sum_{i=1}^{z}\sum_{j=1}^{2^{i-1}} |H_{i,j}(n)| < 2^{l_0+2}\sum_{i=1}^{z} l_i^{-1} < n(\log n)^{-3}.$$

Доказательство того, что с помощью описанного алгоритма почти каждое подмножество из M_n удается покрыть не более $1,6\,n/\log n$ прогрессиями, приводится в оставшейся части статьи. В § 4 мы устанавливаем ряд вспомогательных фактов. В § 5, 6 мы доказываем четыре леммы, в которых приведены асимптотики для вероятности того, что на очередном шаге используемого алгоритма случайное число в случайном подмножестве из M_n окажется еще не покрытым отобранными прогрессиями. Пользуясь этими леммами, в § 7 мы доказываем теорему 1.2.

Всюду ниже через I_0 обозначено множество натуральных чисел из интервала $[n(\log n)^{-2},\ n - n(\log n)^{-2}]$.

§ 4. Вспомогательные утверждения

Обозначим через $V_{i,j}(n,k,r)$ множество совокупностей, каждая из которых состоит из r прогрессий длины $l_i = \lfloor l_0 2^{-i}\rfloor$ с различными разностями из $H_{i,j}(n)$, а число $k \in M_n$ принадлежит каждой прогрессии совокупности.

Лемма 4.1. *При любом достаточно большом n, $k \in I_0$ и рассматриваемых i, j справедливо равенство*

$$|V_{i,j}(n,k,r)| = l_i^r \binom{|H_{i,j}(n)|}{r}.$$

Доказательство. Рассматриваемые совокупности прогрессий могут быть получены следующим способом.

1. Указываются r чисел из $H_{i,j}(n)$, которые должны быть разностями отбираемых прогрессий. Имеется $\binom{|H_{i,j}(n)|}{r}$ возможностей.

2. При каждой фиксированной разности указывается место расположения k в прогрессии с этой разностью. Поскольку $k \in I_0$, а $l_i|H_{i,j}(n)| < 2^{l_0} < n(\log n)^{-4}$ согласно (3.1), (3.4), (3.6) и (3.7), имеется точно k прогрессий с заданной разностью, содержащих число k. Следовательно, число возможностей для выбора r прогрессий с заданными разностями равно l_i^r.

Из пп. 1, 2 следует лемма 4.1.

Пусть D — произвольное подмножество из M_n и k — некоторое число из D. Обозначим через $z(D,k,l)$ множество прогрессий из M_n, каждая из которых имеет длину l, содержит число k и пересекается с D не менее чем по двум элементам.

Лемма 4.2. *При любых D, k и l справедливо неравенство*

$$|z(D,k,l)| < |D|l^2.$$

Доказательство. Каждая прогрессия P из $z(D,k,l)$ может быть получена следующим способом. Во-первых, в D отбирается число v, отличное от k и принадлежащее D ($|D|$ возможностей), во-вторых, указывается количество членов, расположенных в P между k и v (менее l возможностей), в-третьих, отмечается место расположения числа k в P (не более l возможностей). Следовательно, $|z(D,k,l)| < |D|l^2$. Лемма 4.2 доказана.

Пусть P — возрастающая прогрессия в M_n с разностью d, первым членом a и последним членом b, где $a \geqslant d$ и $n - b \geqslant d$.

- Совокупность чисел $a-d$ и $b+d$ назовем *границей* прогрессии P и введем обозначение $\widehat{P} = \{P \cup (a-b) \cup (b+d)\}$.
- Совокупность прогрессий $P_1, \ldots, P_r$, содержащих число k, назовем *веером*, если $|\widehat{P}_i \cap \widehat{P}_j| = 1$ при любых i и j, $1 \leqslant i, j \leqslant r$.

Обозначим через $V^1_{i,j}(n,k,r)$ совокупность элементов $U \in V_{i,j}(n,k,r)$, которые не являются веерами.

Лемма 4.3. *При любом n и любых i, j, r справедливо неравенство*

$$|V^1_{i,j}(n,k,r)| < rl_i^r(l_i+1)^2\binom{|H_{i,j}(n)|}{r-1}.$$

Доказательство. Все элементы из $V^1_{i,j}(n,k,r)$ могут быть получены следующим образом. Сначала в M_n отбираются $r-1$ таких прогрессий $P_1, \ldots, P_{r-1}$ длины l_i с разными разностями из $H_{i,j}(n)$, что k входит в каждую прогрессию. Согласно лемме 4.1 имеется $l_i^{r-1}\binom{|H_{i,j}(n)|}{r-1}$ возможностей. Затем к отобранным прогрессиям добавляется такая тупиковая прогрессия P_r длины l_i, что $k \in P_r$ и среди $P_1, \ldots, P_{r-1}$ имеется по крайней мере одна прогрессия, например P_w, такая, что $|\widehat{P}_r \cap \widehat{P}_w| \geqslant 2$. Согласно лемме 4.2 число возможностей для выбора P_r меньше $rl_i(l_i+1)^2$. Лемма 4.2 доказана.

Пусть $V^2_{i,j}(n,k,r) = V_{i,j}(n,k,r) \setminus V^1_{i,j}(n,k,r)$. Пользуясь леммами 4.1 и 4.3, получаем

Следствие 4.1. *При любом достаточно большом n, $k \in I_0$ и любых рассматриваемых i, j, r справедливо равенство*

$$|V^2_{i,j}(n,k,r)| = l_i^r\binom{|H_{i,j}(n)|}{r}(1 + O(r^2l_i^2/|H_{i,j}(n)|)).$$

§ 5. Количество подмножеств из M_n, содержащих заданные числа, не покрываемые прогрессиями из $S_{0,1}(n)$

Пусть k — произвольное число из M_n. Обозначим через $F(n,k)$ совокупность подмножеств из M_n, содержащих число k. Пусть $F_{i,j}(n,k)$ есть совокупность элементов R из $F(n,k)$ таких, что в R нет ни одной тупиковой прогрессии, которая содержала бы числю k и принадлежала бы множеству $\{S_{0,1}(n) \cup S_{1,1}(n) \cup \ldots \cup S_{i,j}(n)\}$. Положим

$$\mathbf{P}_{i,j}(n,k) = |F_{i,j}(n,k)|/|F(n,k)|. \tag{5.1}$$

Величина $\mathbf{P}_{i,j}(n,k)$ может интерпретироваться как вероятность получения случайного подмножества из $F(n,k)$, в котором нет тупиковых прогрессий, содержащих число k и принадлежащих указанному множеству.

При оценке сложности покрытия, получаемого при помощи описанного алгоритма, необходимо знать асимптотики для вероятностей $\mathbf{P}_{i,j}(n,k)$ при всех рассматриваемых i, j, k. Эти асимптотики устанавливаются индуктивно: по известным асимптотикам для $\mathbf{P}_{0,1}(n,k), \ldots$, $\mathbf{P}_{i,j}(n,k)$ находится асимптотика для $\mathbf{P}_{i+1,1}(n,k)$ при $j = 2^{i-1}$ и для $\mathbf{P}_{i,j+1}(n,k)$ при $j < 2^{i-1}$. Асимптотика для $\mathbf{P}_{0,1}(n,k)$ устанавливается отдельно (лемма 5.1).

При нахождении асимптотики для $\mathbf{P}_{i,j}(n,k)$ используются вспомогательные вероятности, которые определяются так. Пусть $n_1, \ldots, n_r$ — произвольные числа из M_n и $D = \{n_1, \ldots, n_r\}$. Обозначим через $F(n,D)$ совокупность подмножеств R из M_n таких, что каждое число из D принадлежит множеству R. Пусть $F_{i,j}(n,D)$ — совокупность элементов R из $F(n,D)$ таких, что в R нет по крайней мере одной прогрессии из $\{S_{0,1}(n) \cup \ldots \cup S_{i,j}(n)\}$, которая является тупиковой в R и имеет непустое пересечение с D. Пусть

$$\mathbf{P}_{i,j}(n,D) = |F_{i,j}(n,D)|/|F(n,D)|. \tag{5.2}$$

Ясно, что $\mathbf{P}_{i,j}(n,D)$ совпадает с $\mathbf{P}_{i,j}(n,k)$, когда D состоит из одного числа, равного k.

В настоящем параграфе находятся асимптотики для вероятностей $\mathbf{P}_{0,1}(n,k)$ и $\mathbf{P}_{0,1}(n,D)$. Индукционный шаг доказательства описывается в следующем параграфе.

Лемма 5.1. *При любом $k \in I_0$ и $n \to \infty$*

$$\mathbf{P}_{0,1}(n,k) = (1/2)(1 + o(2^{-0{,}25 l_0})).$$

Доказательство. Пусть $P_1, \dots, P_s$ — различные прогрессии длины l_0 с разностями из $H_{0,1}(n)$, содержащие число k. Обозначим через $F_{0,1}^1(n,k,P_1,\dots,P_s)$ совокупность таких элементов R из $F(n,k)$, что прогрессии $P_1,\dots,P_s$ являются тупиковыми в R и в R нет ни одной другой тупиковой прогрессии длины l_0 с разностью из $H_{0,1}(n)$, которая содержит число k. Пусть

$$F_{0,1}^1(n,k,s) = \bigcup F_{0,1}^1(n,k,P_1,\dots,P_s),$$

где объединение берется по всем совокупностям $(P_1,\dots,P_s)$ рассматриваемого вида.

Ясно, что если $\{P_1,\dots,P_s\} \neq \{P_1',\dots,P_s'\}$, то

$$F_{0,1}^1(n,k,P_1,\dots,P_s) \bigcap F_{0,1}^1(n,k,P_1',\dots,P_s') = \varnothing.$$

Следовательно,

$$|F_{0,1}(n,k)| + \sum_{s\geqslant 1} |F_{0,1}^1(n,k,s)| = |F(n,k)| = 2^{n-1}. \tag{5.3}$$

Множество $F_{0,1}^1(n,k,s)$ представим в виде

$$F_{0,1}^1(n,k,s) = F_{0,1}^{1,1}(n,k,s) \bigcup F_{0,1}^{1,2}(n,k,s), \tag{5.4}$$

где

$$F_{0,1}^{1,2}(n,k,s) = F_{0,1}^1(n,k,s) \setminus F_{0,1}^{1,1}(n,k,s), \tag{5.5}$$

$$F_{0,1}^{1,1}(n,k,s) = \bigcup{}^1 F_{0,1}^1(n,k,P_1,\dots,P_s), \tag{5.6}$$

а объединение берется по всем совокупностям $(P_1,\dots,P_s)$, являющимся веерами.

В любом R из $\bigcup_{s\geqslant 2} F_{0,1}^{1,2}(n,k,s)$ имеется по крайней мере две тупиковые прогрессии P_1, P_2 длины l_0 с разностями из $H_{0,1}(n)$ такие, что $k \in P_1 \cap P_2$, $|\widehat{P}_1 \cap \widehat{P}_2| \geqslant 2$. Пользуясь (3.4) и леммой 4.2 при $|D| = l_0$, видим, что число таких пар не превосходит $l_0^3 2^{l_0+1}$. Вместе с тем $|\widehat{P}_1 \cup \widehat{P}_2| \geqslant 1,5l_0 + 1$. Поэтому

$$\sum_{s\geqslant 2} |F_{0,1}^{1,2}(n,k,s)| < l_0^3 2^{n-0,5l_0}. \tag{5.7}$$

Далее, пользуясь (3.4), получаем

$$|F_{0,1}^{1,1}(n,k,s)| < l_0^s \binom{h_{0,1}}{s} 2^{n-(l_0+1)s} < \frac{1}{s!}(\ln 2)^s 2^n.$$

Поэтому при $n \to \infty$ имеем

$$\sum_{s\geqslant l_0} |F_{0,1}^{1,1}(n,k,s)| < 2^n \sum_{s\geqslant l_0} \frac{1}{s!}(\ln 2)^s < 2^n n^{-2}. \tag{5.8}$$

Из (5.3)–(5.8) следует, что

$$|F_{0,1}(n,k)| + \sum_{s=1}^{l_0} |F_{0,1}^{1,1}(n,k,s)| = 2^{n-1}(1 + O(l_0^3 2^{-0,5l_0})). \tag{5.9}$$

Нетрудно видеть, что

$$|F_{0,1}^{1,1}(n,k,P_1,\dots,P_s)| = |F_{0,1}(n,k)|2^{-(l_0+1)s}(1 + O(s2^{l_0})).$$

Далее, пользуясь (3.4) и следствием 4.1, убеждаемся, что при любом $s \leqslant l_0$ для выбора рассматриваемых совокупностей $(P_1,\dots,P_s)$ имеется $\frac{1}{s!}(2^{l_0+1}\ln 2)^s(1 + o(2^{-0,5l_0}))$ возможностей.

Из последних двух фактов и (5.6) следует, что

$$|F_{0,1}^{1,1}(n,k,s)| = \frac{1}{s!}|F_{0,1}(n,k)|(\ln 2)^s(1 + o(2^{-0,5l_0})).$$

Поэтому

$$|F_{0,1}(n,k)| + \sum_{s=1}^{l_0} |F_{0,1}^{1,1}(n,k,s)| = |F_{0,1}(n,k)|(1 + o(2^{-0,5l_0}))\sum_{s=0}^{l_0}\frac{1}{s!}(\ln 2)^s$$
$$= 2|F_{0,1}(n,k)|(1 + o(2^{-0,5l_0})). \tag{5.10}$$

Подставляя (5.10) в (5.9) и пользуясь (5.1) при $i = 0$, $j = 1$, а также равенством $|F(n,k)| = 2^{n-1}$, получаем утверждение леммы 5.1.

Лемма 5.2. *Пусть k — любое число из интервала I_0 и D — произвольное подмножество из I_0, $|D| < l_0^2$. Тогда при $n \to \infty$*

$$\mathbf{P}_{0,1}(n,D) = 2^{-|D|}(1 + o(2^{0,25l_0})).$$

Доказательство. Пусть D — произвольное подмножество из I_0, $|D| \leqslant l_0^2$ и $P_1,\dots,P_s$ — различные прогрессии длины l_0 с разностями из $H_{0,1}(n)$ такие, что $|P_i \cap D| = 1$, $1 \leqslant i \leqslant s$. Обозначим через $F_{0,1}^1(n,D,P_1,\dots,P_s)$ совокупность элементов R из $F(n,D)$ таких, что прогрессии $P_1,\dots,P_s$ являются тупиковыми в R и в R нет ни одной

другой тупиковой прогрессии P длины l_0 с разностью из $H_{0,1}(n)$ такой, что $|P \cap D| = 1$. Пусть

$$F^1_{0,1}(n, D, s) = \bigcup F^1_{0,1}(n, D, P_1, \dots, P_s), \tag{5.11}$$

где объединение берется по всем совокупностям $(P_1, \dots, P_s)$ рассматриваемого вида. Ясно, что если $\{P_1, \dots, P_s\} \neq \{P'_1, \dots, P'_s\}$, то

$$F^1_{0,1}(n, D, P_1, \dots, P_s) \cap F^1_{0,1}(n, D, P'_1, \dots, P'_s) = \varnothing.$$

Следовательно,

$$|F_{0,1}(n, D)| + \sum_{s \geqslant 1} |F^1_{0,1}(n, D, s)| = F(n, D) = 2^{-|D|}. \tag{5.12}$$

Множество $F^1_{0,1}(n, D, s)$ представим в виде

$$F^1_{0,1}(n, D, s) = F^{1,1}_{0,1}(n, D, s) \cup F^{1,2}_{0,1}(n, D, s), \tag{5.13}$$

где

$$F^{1,2}_{0,1}(n, D, s) = F^1_{0,1}(n, D, s) \setminus F^{1,1}_{0,1}(n, D, s), \tag{5.14}$$

$$F^{1,1}_{0,1}(n, D, s) = \bigcup{}^1 F^{1,1}_{0,1}(n, D, P_1, \dots, P_s), \tag{5.15}$$

а объединение берется по всем совокупностям $(P_1, \dots, P_s)$ таким, что $|P_i \cap D| = 1$ при любом i, $1 \leqslant i \leqslant s$, и $(\widehat{P}_i \cap \widehat{P}_j) \setminus D = \varnothing$. Пользуясь (3.4), имеем

$$|F^{1,1}_{0,1}(n, D, s)| < l_0 \binom{|D| h_{0,1}}{s} 2^{n-|D|-(l_0+1)s} < \frac{1}{s!} |D|^s 2^{n-|D|}.$$

Поэтому при $n \to \infty$ получаем

$$\sum_{s \geqslant 6l_0^2} |F^{1,1}_{0,1}(n, D, s)| < 2^{n-|D|} \sum_{s \geqslant 6l_0^2} \frac{1}{s!} |D|^s$$

$$< (\text{ ибо } |D| < l_0^2) < 2^{n-2|D|} n^{-2}. \tag{5.16}$$

Оценим сверху мощность множества $\bigcup_{s \geqslant 2} F^{1,2}_{0,1}(n, D, s)$. Пусть R — произвольный элемент из $F^{1,2}_{0,1}(n, D, P_1, \dots, P_r)$ и $V = \{P_1, \dots, P_r\}$. Обозначим через V' произвольную совокупность прогрессий из V, обладающую следующими свойствами:

◇ если P' и P'' — прогрессии из V', то $(\widehat{P}' \cup \widehat{P}'') \setminus D = \varnothing$;

◇ для любой прогрессии P из $V \setminus V'$ имеется по крайней мере одна прогрессия P' из V' такая, что $(\widehat{P}' \cup \widehat{P}) \setminus D \neq \varnothing$.

Как и при доказательстве (5.14), убеждаемся, что при $n \to \infty$ число элементов из $\bigcup_{s\geqslant 2} F_{0,1}^{1,2}(n, D, s)$, в каждом из которых множество V' состоит не менее чем из $6l_0^2$ прогрессий, меньше величины $2^{n-2|D|}n^{-2}$.

Рассмотрим случай, когда $|V'| < 6l_0^2$. Пусть для определенности $V' = \{P_1, \ldots, P_s\}$. Положим $\widehat{V}' = \{\widehat{P}_1, \ldots, \widehat{P}_s\}$. Обозначим через V'' множество всех прогрессий P длины l_0 с разностями из $H_{0,1}(n)$ таких, что P принадлежит V'' тогда и только тогда, когда $P \cap D \neq \varnothing$ и $(\widehat{P} \cap \widehat{V}') \setminus D \neq \varnothing$. Очевидно, что $V \setminus V' \subseteq V''$. Оценим сверху мощность множества V''. Все прогрессии P из V'' могут быть получены следующим способом. Сначала в D и $\widehat{V}' \setminus D$ отбирается по одному элементу (не более $|D|s(l_0+1)$ возможностей). Затем указывается число членов, расположенных в P между отобранными элементами (менее l_0 возможностей). Наконец, указывается место расположения в P отобранного элемента из D (не более l_0 возможностей). Следовательно,

$$|V''| < |D|s(l_0+1)^3. \tag{5.17}$$

Будем различать два случая.

Случай 1: в $V \setminus V'$ имеется по крайней мере одна прогрессия P такая, что только для одной прогрессии из V', например прогрессии P_i, имеет место соотношение $(\widehat{P} \cap \widehat{P}_i) \setminus D \neq \varnothing$.

Пусть прогрессия P из $V \setminus V'$ такова, что $(\widehat{P} \cap \widehat{P}_i) \setminus D \neq \varnothing$ только при одном i, $1 \leqslant i \leqslant s$. Тогда $|\widehat{P} \cap \widehat{P}_i| > 1,5l_0$ и $|\widehat{P} \cup \widehat{P}_1 \cup \ldots \cup \widehat{P}_s) \setminus D| \geqslant (l_0+1)s + 0,5l_0$. Обозначим через $F_{0,1}^{1,3}(n, D, P_1, \ldots, P_s, P)$ совокупность элементов R из $F_{0,1}^{1,2}(n, D)$ таких, что в R множество V' состоит из прогрессий $P_1, \ldots, P_s$, а P — прогрессия, о которой только что говорилось. Поэтому

$$\begin{aligned}
&|F_{0,1}^{1,3}(n, D, P_1, \ldots, P_s, P)| \\
&\qquad \leqslant |F_{0,1}(n, D)| 2^{n-|D|-(l_0+1)s-0,5l_0}(1 + O(|D|sl_0^3 2^{-l_0})) \\
&\qquad\qquad < |F_{0,1}(n, D)| 2^{n-|D|-(l_0+1)s-0,5l_0-1}.
\end{aligned}$$

Поскольку при фиксированных $P_1, \ldots, P_s$ прогрессия P может быть вы-

брана не более чем $|D|sl_0^3$ способами, воспользовавшись (3.4), получаем

$$\sum_{s=1}^{6l_0^2}\sum_{(P_1,\dots,P_s)}|F_{0,1}^{1,3}(n,D,P_1,\dots,P_s,P)|$$
$$<|F_{0,1}(n,D)|2^{-0{,}25l_0-1}\sum_{s\geqslant 1}\frac{1}{s!}(\ln 2)^s<|F_{0,1}(n,D)|2^{-0{,}25l_0}. \quad (5.18)$$

Случай 2: для любой прогрессии P из $V\setminus V'$ найдутся по крайней мере две прогрессии из V', например прогрессии P_i и P_j, такие, что $(\widehat{P}\cap\widehat{P}_i)\setminus D\neq\varnothing$ и $(\widehat{P}\cap\widehat{P}_j)\setminus D\neq\varnothing$.

Обозначим через $F_{0,1}^{1,3}(n,D,P_1,\dots,P_s)$ совокупность элементов R из $F_{0,1}^{1,2}(n,D)$ таких, что в R множество V' состоит из прогрессий $P_1,\dots,P_s$. Пользуясь (5.17), нетрудно видеть, что

$$|F_{0,1}^{1,3}(n,D,P_1,\dots,P_s,P)|\leqslant|F_{0,1}(n,D)|2^{n-|D|-(l_0+1)s}(1+O(|D|sl_0^3 2^{-l_0}))$$
$$<|F_{0,1}(n,D)|2^{n-|D|-(l_0+1)s+1}. \quad (5.19)$$

Если $P_1,\dots,P_{s-1}$ уже отобраны, то для выбора P_s имеется не более $|D|sl_0^3$ возможностей. Пользуясь этим фактом и (3.4), получаем, что при $n\to\infty$ число рассматриваемых совокупностей $(P_1,\dots,P_s)$ не превосходит величины

$$\frac{1}{s!}(2^{l_0+1}\ln 2)^{s-1}|D|sl_0^3<\frac{1}{s!}2^{(l_0+1)s-0{,}25l_0}. \quad (5.20)$$

Из (5.19) и (5.20) следует, что при $n\to\infty$

$$\sum_{s=1}^{6l_0^2}\sum_{(P_1,\dots,P_s)}|F_{0,1}^{1,3}(n,D,P_1,\dots,P_s)|<|F_{0,1}(n,D)|2^{n-|D|-0{,}25l_0-2}$$
$$\times\sum_{s\geqslant 1}\frac{1}{s!}(\ln 2)^s<|F_{0,1}(n,D)|2^{n-|D|-0{,}25l_0}. \quad (5.21)$$

Пользуясь (5.11)–(5.16) и (5.21), получаем

$$|F_{0,1}(n,D)|+\sum_{s=1}^{6l_0^2}|F_{0,1}(n,D,s)|=2^{n-|D|}(1+o(2^{-0{,}25l_0})). \quad (5.22)$$

В свою очередь, при любом $s \leqslant 6l_0^2$ справедливо соотношение

$$|F_{0,1}^{1,1}(n, D, P_1, \dots, P_s)| = |F_{0,1}(n, D)| 2^{-(l_0+1)s}(1 + O(s2^{-l_0})).$$

Вместе с тем, пользуясь (3.4) и следствием 4.1, убеждаемся, что для выбора рассматриваемых прогрессий $P_1, \dots, P_s$ имеется $\frac{1}{s!}(|D|2^{l_0+1}\ln 2)^s$ $(1 + o(2^{-0,5l_0}))$ возможностей.

Из последних двух фактов и (5.15) следует, что

$$|F_{0,1}^{1,1}(n, D, s)| = \frac{1}{s!}(|D|\ln 2)^s 2^{n-|D|}(1 + o(2^{-0,25l_0})).$$

Поэтому

$$\begin{aligned} |F_{0,1}(n, D)| &+ \sum_{s=1}^{6l_0^2} |F_{0,1}^{1,1}(n, D, s)| \\ &= |F_{0,1}(n, D)|(1 + o(2^{-0,25l_0})) \sum_{s=0}^{6l_0^2} \frac{1}{s!}(|D|\ln 2)^s \\ &= |F_{0,1}(n, D)| 2^{|D|}(1 + o(2^{-0,25l_0})). \qquad (5.23) \end{aligned}$$

Подставляя (5.23) в (5.22), получаем

$$|F_{0,1}(n, D)| = 2^{n-2|D|}(1 + o(2^{-0,25l_0})).$$

Отсюда и из (5.2) при $i = 0$, $j = 1$ следует утверждение леммы 5.2.

§ 6. Количество подмножеств из M_n, содержащих заданные числа, не покрываемые прогрессиями из $S_{0,1}(n), \dots, S_{i,j}(n)$

В настоящем параграфе устанавливаются асимптотики для вероятностей $\mathbf{P}_{i,j}(n, k)$ и $\mathbf{P}_{i,j}(n, D)$ при любых рассматриваемых i и j, за исключением случая $i = 0$ и $j = 1$, который уже изучен. Асимптотики для $\mathbf{P}_{i,j}(n, k)$ содержатся в лемме 6.1, а для $\mathbf{P}_{i,j}(n, D)$ — в лемме 6.2.

Лемма 6.1. *Пусть k — произвольное число из интервала I_0 и для произвольного подмножества D из I_0, $|D| < l_0^2$, справедливо соотношение*

$$\mathbf{P}_{i,j}(n, D) = 2^{-(2^{i-1}+j)|D|}(1 + o(2^{-0,25l_0}))^{2^{i-1}+j}. \qquad (6.1)$$

Тогда если $j \in [1, 2^{i-1} - 1]$, то

$$\mathbf{P}_{i,j+1}(n, k) = 2^{-2^{i-1}-j-1}(1 + o(2^{-0,25l_0}))^{2^{i-1}+j+1}, \qquad (6.2)$$

а если $j = 2^{i-1}$, то

$$\mathbf{P}_{i+1,1}(n,k) = 2^{-2^i-1}(1+o(2^{-0{,}25l_0}))^{2^i+1}. \tag{6.3}$$

Доказательство. Поскольку соотношения (6.2) и (6.3) устанавливаются одинаково, мы ограничимся доказательством соотношения (6.2). Пусть $P_1,\dots,P_s$ — различные прогрессии длины l_i с разностями из $H_{i,j}(n)$, содержащие число k. Обозначим через $F^1_{i,j}(n,k,P_1,\dots,P_s)$ совокупность элементов R из $F(n,k)$ таких, что прогрессии $P_1,\dots,P_s$ включаются в покрытие множества R и в R нет других тупиковых прогрессий длины l_i с разностями из $H_{i,j}(n)$, которые содержат число k и включаются в покрытие множества R.

Пусть

$$F^1_{i,j+1}(n,k,s) = \bigcup F^1_{i,j+1}(n,k,P_1,\dots,P_s), \tag{6.4}$$

где объединение берется по всем совокупностям $(P_1,\dots,P_s)$ рассматриваемого вида. Следовательно,

$$|F_{i,j+1}(n,k)| + \sum_{s\geqslant 1} |F^1_{i,j+1}(n,k,s)| = |F_{i,j}(n,k)|. \tag{6.5}$$

Множество $F^1_{i,j+1}(n,k,s)$ представим в виде

$$F^1_{i,j+1}(n,k,s) = F^{1,1}_{i,j+1}(n,k,s) \cup F^{1,2}_{i,j+1}(n,k,s), \tag{6.6}$$

где $F^{1,1}_{i,j+1}(n,k,s)$ и $F^{1,2}_{i,j+1}(n,k,s)$ не пересекаются,

$$F^{1,1}_{i,j+1}(n,k,s) = \bigcup{}^1 F^1_{i,j+1}(n,k,P_1,\dots,P_s), \tag{6.7}$$

а объединение берется по всем совокупностям $(P_1,\dots,P_s)$, каждая из которых является веером.

В любом R из $\bigcup_{s\geqslant 2} F^{1,2}_{i,j+1}(n,k,s)$ имеются по крайней мере две тупиковые прогрессии P_1, P_2 длины l_i с разностями из $H_{i,j+1}(n)$ такие, что P_1 и P_2 отбираются в покрытие множества R, $k\in P_1$, $k\in P_2$, $|\widehat{P}_1\cap\widehat{P}_2|\geqslant 2$. Согласно (3.7) для выбора P_1 имеется менее $2^{(l_i-1)(2^{i-1}+j+1)+2}$ возможностей, а при заданной P_1 для выбора P_2 — менее $l_i^3 < l_0^3$ возможностей. Значит для выбора P_1 и P_2 имеется менее $l_0^3 2^{(l_i-1)(2^{i-1}+j+1)+2}$ возможностей. Вместе с тем если P_1 и P_2 фиксированы, то согласно (6.1) эти прогрессии включаются в покрытие менее чем в

$$2^{n-(2^{i-1}+j+1)|P_1\cup P_2|+1} < 2^{n-1{,}5l_i(2^{i-1}+j+1)+1}$$

множеств. Поэтому при $n \to \infty$

$$\sum_{s\geqslant 2} |F^{1,2}_{i,j+1}(n,k,s)| < l_0^3 2^{n-2^{i-1}-j+1-0{,}5l_i(2^{i-1}+j+1)}$$

$$= (\text{используем (6.1) при } |D|=1) = o(|F_{i,j}(n,k)|2^{-0{,}25l_0}). \quad (6.8)$$

Далее, при $n \to \infty$

$$\sum_{s\geqslant l_0} |F^{1,1}_{i,j+1}(n,k,s)| < l_i^{l_0}\binom{|H_{i,j+1}(n)|}{l_0} 2^{n-((2^{i-1}+j+1)(l_i-1)+2)l_0}$$

$$< (\text{ см. (3.7)}) < \frac{1}{l_0!}2^n < 2^n n^{-2}. \quad (6.9)$$

Из (6.4)–(6.9) следует, что

$$|F_{i,j+1}(n,k)| + \sum_{s=1}^{l_0} |F^{1,1}_{i,j+1}(n,k,s)| = |F_{i,j}(n,k)|(1+o(2^{0{,}25l_0})). \quad (6.10)$$

Полагая $D = \{P_1 \cup \ldots \cup P_s\} \setminus \{k\}$ и пользуясь (6.1), нетрудно видеть, что

$$|F^{1,1}_{i,j+1}(n,k,P_1,\ldots,P_s)|$$

$$= |F_{i,j+1}(n,k)|2^{-((2^{i-1}+j+1)(l_i-1)+2)s}(1+o(2^{-0{,}25l_0}))^{2^{i-1}+j+1}. \quad (6.11)$$

В свою очередь, из (3.7) и леммы 4.2 следует, что число возможностей для выбора рассматриваемых совокупностей $(P_1,\ldots,P_s)$ равно

$$\frac{1}{s!}2^{((l_i-1)(2^{i-1}+j+1)+2)s}(\ln 2)^s(1+o(2^{-0{,}25l_0})). \quad (6.12)$$

Пользуясь (6.4), (6.11) и (6.12), имеем

$$|F^{1,1}_{i,j+1}(n,k,s)|$$

$$= \frac{1}{s!}|F_{i,j+1}(n,k)|(\ln 2)^s(1+o(2^{-0{,}25l_0}))^{2^{i-1}+j}. \quad (6.13)$$

Подставляя (6.13) в (6.11) и пользуясь (6.10), получаем

$$|F_{i,j+1}(n,k)|\sum_{s=0}^{l_0}\frac{1}{s!}(\ln 2)^s(1+o(2^{-0{,}25l_0}))^{2^{i-1}+j}$$

$$= 2|F_{i,j+1}(n,k)|(1+o(2^{-0{,}25l_0}))^{2^{i-1}+j} = |F_{i,j}(n,k)|(1+o(2^{-0{,}25l_0})),$$

т. е.

$$|F_{i,j+1}(n,k)| = \frac{1}{2}|F_{i,j}(n,k)|(1+o(2^{-0{,}25l_0})). \quad (6.14)$$

Воспользовавшись (6.14), (5.1) и (6.1) при $|D|=1$, получаем соотношение (6.2).

Лемма 6.2. *Пусть для произвольного k из интервала I_0 и любых рассматриваемых i, j справедливо соотношение*

$$\mathbf{P}_{i,j}(n,k) = 2^{-2^{i-1}-j}(1+o(2^{-0{,}25l_0}))^{2^{i-1}+j}.$$

Тогда для произвольного подмножества D из I_0, $|D| < l_0^2$, справедливо соотношение

$$\mathbf{P}_{i,j}(n,D) = 2^{-(2^{i-1}+j)|D|}(1+o(2^{0{,}25l_0}))^{2^{i-1}+j}.$$

Доказательство аналогично доказательству леммы 6.1 и поэтому опускается. Отличие состоит лишь в том, что число k всюду надо заменить множеством D.

§ 7. Доказательство теоремы 1.2

Согласно лемме 6.1 вероятность того, что некоторое число из случайного подмножества $R \subseteq M_n$ остается непокрытым прогрессиями из $S_{0,1}(n), \dots, S_{z,2^z-1}(n)$, равна

$$2^{-2^z}(1+o(2^{-0{,}25l_0}))^{2^z} < (\text{ см. (3.2)}) < 2^{-2\log\log n}(1+o(1)) \sim \log^{-2} n.$$

Поэтому математическое ожидание числа элементов в R, которые не покрыты прогрессиями из указанных множеств, по порядку не превосходит величины $n(\log n)^{-2}$. Пользуясь этим фактом и известным неравенством $\mathbf{P}\{X > \varepsilon\} \leqslant \mathbf{E}X/\varepsilon$ при $\varepsilon = n(\log n)^{-1{,}5}$, видим, что почти в каждом подмножестве из M_n двухчленными прогрессиями покрывается $o(n\log^{-1} n)$ чисел. Это означает, что для доказательства теоремы 1.2 достаточно оценить сверху число прогрессий из $S_{0,1}(n), \dots, S_{z,2^z-1}(n)$, которые включаются в покрытие случайного подмножества из M_n согласно алгоритму из § 3, и убедиться, что эта оценка меньше $1{,}6n/\log n$.

Пусть $X_{i,j} = X_{i,j}(R)$ — случайная величина, равная числу прогрессий из $S_{i,j}(n)$, включаемых в покрытие множества R, и пусть $\mathbf{E}X_{i,j}$ — математическое ожидание величины $X_{i,j}$.

Лемма 7.1. *Число прогрессий из множеств $S_{0,1}(n), \dots, S_{z,2^z-1}(n)$, включаемых в покрытие почти каждого подмножества из M_n, при $n \to \infty$ асимптотически равно $\sum \mathbf{E}X_{i,j}$, где суммирование осуществляется по всем рассматриваемым i и j.*

Доказательство. Пусть P — произвольная прогрессия из $S_{i,j}(n)$ такая, что граница P состоит из двух чисел. Если $i = 0$ и $j = 1$, то

имеется 2^{n-l_0-2} подмножеств из M_n, в покрытиях которых содержится P из $S_{0,1}(n)$. Суммируя по всем прогрессиям из $S_{0,1}(n)$ и используя (3.4), убеждаемся, что

$$\begin{aligned}\mathbf{E}X_{0,1} &= n2^{-l_0-2}l_0^{-1}2^{l_0+1}\ln 2(1+O(\ln^{-2} n))\\ &= (1/2)nl_0^{-1}\ln 2(1+O(\ln^{-2} n)). \quad (7.1)\end{aligned}$$

Пусть $i \geqslant 1$ и $1 \leqslant j \leqslant 2^{i-1}$. Тогда из леммы 6.2 следует, что имеется

$$2^{n-(2^{i-1}+j)l_i-2}(1+o(2^{-0,25l_0}))^{2^{i-1}+j} = 2^{n-(2^{i-1}+j)l_i-2}(1+O(\ln^{-2}))$$

подмножеств из M_n, в покрытиях которых содержится P из $P_{i,j}(n)$. Суммируя по всем прогрессиям из $S_{i,j}(n)$, с учетом (3.6) и (3.7) убеждаемся, что

$$\begin{aligned}\mathbf{E}X_{i,j} &= n2^{-(2^{i-1}+j)l_i-2}l_i^{-1}2^{(l_i-1)(2^{i-1}+j)+2}\ln 2(1+O(\ln^{-2} n))\\ &= nl_i^{-1}2^{-2^{i-1}-j}\ln 2(1+O(\ln^{-2} n)) \sim nl_i^{-1}2^{i-2^{i-1}-j}\ln 2. \quad (7.2)\end{aligned}$$

Нетрудно видеть, что при любых рассматриваемых i и j

$$\mathbf{E}X_{i,j}^2 = ((\mathbf{E}X_{i,j})^2 + \mathbf{E}X_{i,j})(1+O(\ln^{-2} n)). \quad (7.3)$$

Теперь воспользуемся следующим неравенством Чебышева (см. [7]):

$$\mathbf{E}\{|X-\mathbf{E}X| \geqslant u\} \leqslant (\mathbf{E}X^2 - \mathbf{E}^2X)u^{-2}.$$

Полагая $X = X_{i,j}$, $u = (\ln n)^{-1/2}\mathbf{E}X_{i,j}$ и пользуясь (7.1), (7.2), получаем

$$\begin{aligned}&\mathbf{P}\{|X_{i,j}-\mathbf{E}X_{i,j}| \geqslant (\ln n)^{-1/2}\mathbf{E}X_{i,j}\}\\ &\qquad < O((\ln n)^{-1}) + O((\mathbf{E}X_{i,j})^{-1}\ln n) = O((\ln n)^{-1}).\end{aligned}$$

Поэтому

$$\begin{aligned}&\sum_{i,j}\mathbf{P}\{|X_{i,j}-\mathbf{E}X_{i,j}| \geqslant (\ln n)^{-1/2}\mathbf{E}X_{i,j}\}\\ &\qquad < O(2^z(\ln n)^{-1}) = (\text{см. (3.2)}) = o(1).\end{aligned}$$

Отсюда следует утверждение леммы 7.1.

Наконец, оценим сверху величину $\sum_{i,j}\mathbf{E}X_{i,j}$. Пользуясь (7.1) и (7.2), получаем

$$\begin{aligned}\sum_{i,j}\mathbf{E}X_{i,j} &\sim nl_0^{-1}\ln 2\Big(2^{-1}+\sum_{i=1}^{z}\sum_{j=1}^{2^{i-1}}2^{i-2^{i-1}-j}\Big) = nl_0^{-1}\ln 2\Big(1+(3/4)+(15/32)\\ &\quad + 2^{-4}(1-2^{-8}) + 2^{-11}(1-2^{-16}) + \sum_{i=6}^{z}2^{i-2^{i-1}}\sum_{j=1}^{2^{i-1}}2^{-j}\Big)\\ &\quad < 2,2815nl_0^{-1}\ln 2 < 1,582nl_0^{-1}.\end{aligned}$$

Теорема 1.2 доказана.

ЛИТЕРАТУРА

1. **Сапоженко А. А., Асратян А. С., Кузюрин Н. Н.** Обзор некоторых результатов по задачам о покрытии // Методы дискретного анализа в решении комбинаторных задач. Новосибирск, 1977. Вып. 30. С. 46–75.
2. **Коршунов А. Д.** О сложности кратчайших дизъюнктивных нормальных форм булевых функций // Методы дискретного анализа в изучении булевых функций и графов. Новосибирск, 1981. Вып. 37. С. 9–41.
3. **Коршунов А. Д.** О сложности кратчайших дизъюнктивных нормальных форм случайных булевых функций // Методы дискретного анализа в оптимизации управляющих систем. Новосибирск, 1983. Вып. 40. С. 25–53.
4. **Кислицын С. С., Сапоженко А. А.** О представлении множества чисел теоретико-множественной суммой арифметических прогрессий // Вопросы кибернетики. М.: Научный совет АН СССР по комплексной проблеме "Кибернетика", 1975. Вып. 16. С. 53–62.
5. **Новиков С. В., Олексин С. В.** О покрытии множества арифметическими прогрессиями // Изв. АН БССР. Сер. физ.-мат. наук. 1979. № 6. С. 25–27.
6. **Глаголев В. В.** О покрытии арифметическими прогрессиями // Методы дискретного анализа в синтезе управляющих систем. Новосибирск, 1978. Вып. 32. С. 34–39.
7. **Феллер В.** Введение в теорию вероятностей и ее применения. М.: Мир, 1967. Т. 1.

Адрес автора:

РОССИЯ,
630090, Новосибирск,
Университетский пр., 4,
Институт математики СО РАН

Статья поступила

29 марта 1994 г.