ДИСКРЕТНЫЙ АНАЛИЗ И ИССЛЕДОВАНИЕ ОПЕРАЦИЙ
Апрель—июнь 1999. Серия 1. Том 6, № 2, 41–61

УДК 519.714.2

КРИТЕРИЙ ПОРОЖДЕНИЯ МНОЖЕСТВ РАЦИОНАЛЬНЫХ ВЕРОЯТНОСТЕЙ В КЛАССЕ БУЛЕВЫХ ФУНКЦИЙ*)

Р. М. Колпаков

Рассматривается задача порождения посредством булевых функций множеств всех n-ично рациональных вероятностей произвольными конечными подмножествами при любом $n \geqslant 2$. Получен критерий возможности данного порождения в классе всех булевых функций.

1. Формулировка основных результатов

В работе используются следующие обозначения:

$\mathbf{N}$ — множество натуральных чисел;

$(x_1, \ldots, x_n)$ — наибольший общий делитель чисел $x_1, \ldots, x_n$;

$\varphi(n)$ — количество чисел в множестве $\{1, \ldots, n-1\}$, взаимно простых с n (*функция Эйлера*);

$\|\widetilde{\sigma}\|$ — *вес* двоичного набора $\widetilde{\sigma} \in \{0,1\}^k$, т. е. число единичных компонент в наборе $\widetilde{\sigma}$;

B_i^k — *i-й слой* единичного куба $\{0,1\}^k$, т. е. множество всех наборов из $\{0,1\}^k$ веса i;

$|A|$ — число элементов множества A.

Пусть $\widetilde{\sigma} = (\sigma_1 \ldots \sigma_k)$ — произвольный двоичный набор из $\{0,1\}^k$, $\rho_1, \ldots, \rho_k$ — некоторые числа из интервала $(0;1)$. Положим

$$\mathscr{P}_{\widetilde{\sigma}}(\rho_1, \ldots, \rho_k) = (\rho_1)_{\sigma_1} \ldots (\rho_k)_{\sigma_k},$$

где

$$(\rho)_\sigma = \begin{cases} \rho, & \text{если } \sigma = 1; \\ 1-\rho, & \text{если } \sigma = 0. \end{cases}$$

*) Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований (код проекта 96-01-01068) и Федеральной целевой программы «Интеграция» (проект 1997 г. № 473).

Пусть $f(x_1, \ldots, x_k)$ — булева функция. Если $f \not\equiv 0$, то, обозначив через $\mathscr{N}(f)$ множество всех наборов из $\{0,1\}^k$, на которых функция f равна 1, определим $\mathscr{P}\{f(\rho_1, \ldots, \rho_k)\}$ следующим образом:

$$\mathscr{P}\{f(\rho_1, \ldots, \rho_k)\} = \sum_{\tilde{\sigma} \in \mathscr{N}(f)} \mathscr{P}_{\tilde{\sigma}}(\rho_1, \ldots, \rho_k).$$

Величина $\mathscr{P}\{f(\rho_1, \ldots, \rho_k)\}$ является одним из базовых понятий в структурной теории вероятностных автоматов. Она представляет собой вероятность получения значения 1 на выходе функционального элемента, реализующего функцию $f(x_1, \ldots, x_k)$ при условии, что на входы элемента подаются независимые булевы случайные коды такие, что вероятность принятия значения 1 случайным кодом, подающимся на вход переменной x_i, равна ρ_i, $1 \leqslant i \leqslant k$.

Пусть H — множество чисел из интервала $(0,1)$. Число $a \in (0,1)$ *порождается* множеством H, если существует булева функция $f(x_1, \ldots, x_k)$ такая, что $a = \mathscr{P}\{f(\rho_1, \ldots, \rho_k)\}$ для некоторых $\rho_1, \ldots, \rho_k$ из H. Обозначим через $[H]$ множество всех чисел, порождаемых множеством H. Заметим, что если $f(x) = x$, то $\mathscr{P}\{f(\rho)\} = \rho$ для любого $\rho \in (0,1)$. Поэтому $H \subseteq [H]$. Будем также говорить, что множество $A \subseteq (0,1)$ *порождается* множеством H, если $A \subseteq [H]$. Множество H назовем *замкнутым*, если $H = [H]$. Важным направлением исследований в области синтеза преобразователей вероятностных распределений является изучение различных аспектов порождения числовых множеств заданными системами чисел. В частности, в [15, 8] рассмотрены вопросы приближенного порождения чисел одноэлементными множествами и множествами двоично рациональных чисел специального вида. В [2, 9] исследованы сложностные аспекты реализации булевых функций, моделирующих булевы случайные коды.

Поскольку такое порождение чисел представляет собой достаточно сложный объект исследований, то естественным подходом к его изучению является рассмотрение более узких замкнутых классов чисел, всюду плотных в интервале $(0,1)$. Простейшим примером таких классов являются множества рациональных чисел. В частности, при любом натуральном $n \geqslant 2$ мы можем рассмотреть множество всех n-ично рациональных чисел из интервала $(0,1)$, т. е. множество

$$\left\{a = \frac{m}{n^r} \mid 0 < a < 1,\ m, r \in \mathbf{N}\right\},$$

которое будем обозначать через $G[n]$. Нетрудно заметить, что если $\rho_1, \ldots, \rho_k \in G[n]$, то $\mathscr{P}\{f(\rho_1, \ldots, \rho_k)\} \in G[n]$. Следовательно, множество $G[n]$ является замкнутым. Основной недостаток данного определения множества $G[n]$ состоит в том, что, как несложно заметить, при разных

n_1 и n_2 множества $G[n_1]$ и $G[n_2]$ могут совпадать. Однако мы можем охарактеризовать все те числа, для которых данное совпадение имеет место. Для этого обозначим через $\mathscr{I}[n]$ множество всех простых делителей числа n.

Утверждение 1. *Пусть* $n_1, n_2 \in \mathbf{N}$ *и* $n_1, n_2 \geqslant 2$. *Тогда*
a) $G[n_1] \subseteq G[n_2]$ *тогда и только тогда, когда* $\mathscr{I}[n_1] \subseteq \mathscr{I}[n_2]$;
b) $G[n_1] = G[n_1]$ *тогда и только тогда, когда* $\mathscr{I}[n_1] = \mathscr{I}[n_2]$.

Таким образом, множество $G[n]$ однозначно определяется множеством $\mathscr{I}[n]$.

По-видимому, рассматриваемое порождение рациональных чисел впервые изучалось в работе Р. Л. Схиртладзе [14]. В данной работе в качестве преобразователей вероятностных распределений рассматривались вероятностные контактные сети, которые можно представлять как частный случай булевых функций. Было показано, что множества $G[2]$ и $G[3]$ порождаются в классе вероятностных контактных сетей системами чисел $\left\{\frac{1}{2}\right\}$ и $\left\{\frac{1}{3}, \frac{2}{3}\right\}$ соответственно. Таким образом, множества $G[2]$ и $G[3]$ являются *конечно порожденными*, т. е. порождаются некоторыми своими конечными подмножествами. Дальнейшие исследования в данной области были проведены Ф. И. Салимовым в [10, 12, 13]. В частности, в [12] им был доказан следующий важный результат.

Теорема 1. *Пусть* $n \in \mathbf{N}$, $n \geqslant 2$, $\mathscr{I}[n] = \{p_1, \ldots, p_k\}$ *и* $H = \left\{\frac{1}{p_1}, \ldots, \frac{p_1-1}{p_1}, \ldots, \frac{1}{p_k}, \ldots, \frac{p_k-1}{p_k}\right\}$. *Тогда* $G[n] = [H]$.

Из этого результата непосредственно следует, что при любом n множество $G[n]$ является конечно порожденным в классе всех булевых функций. Другое доказательство теоремы 1 можно найти в [4]. Изучение порождения рациональных чисел посредством вероятностных контактных сетей было продолжено нами в [3, 5]. Была установлена конечная порожденность множеств $G[n]$ в классе всех вероятностных контактных сетей для всех составных n, а также для $n = 5$ и $n = 7$. Вопрос о конечной порожденности вероятностными контактными сетями множеств $G[n]$ для простых n, больших 7, остается открытым.

Несмотря на то, что порождающая конечная система чисел для множеств $G[n]$ из теоремы 1 является достаточно простой, остается неизвестным, насколько оптимальной в том или ином смысле является эта система. В связи с этим становится актуальным описание всех порождающих конечных подмножеств для $G[n]$ и, в частности, отыскание критериев полноты для произвольного конечного подмножества из $G[n]$. В настоящей работе устанавливается простой критерий полноты произвольного конечного подмножества из $G[n]$ для любого n. Отметим, что при

исследовании множеств $G[n]$ естественно выделяется случай простых n, когда предлагаемый критерий формулируется и доказывается более просто. Поэтому формулировка критерия для этого случая выделена нами в отдельную теорему.

Теорема 2. *Пусть p — простое число, $H = \left\{\frac{m_1}{p^{r_1}}, \ldots, \frac{m_s}{p^{r_s}}\right\}$ — конечное множество несократимых дробей из $G[p]$, $d = (m_1(p^{r_1} - m_1), \ldots, m_s(p^{r_s} - m_s))$ при $s \geqslant 2$ и $d = m_1(n_1 - m_1)$ при $s = 1$. Тогда равенство $[H] = G[n]$ справедливо тогда и только тогда, когда $d \leqslant 2$.*

В общем случае полученный нами критерий формулируется следующим образом.

Теорема 3. *Пусть n — натуральное число, большее 1, $H = \left\{\frac{m_1}{n_1}, \ldots, \frac{m_s}{n_s}\right\}$ — конечное множество несократимых дробей из $G[n]$, $d = (m_1(n_1 - m_1), \ldots, m_s(n_s - m_s))$ при $s \geqslant 2$ и $d = m_1(n_1 - m_1)$ при $s = 1$. Тогда равенство $[H] = G[n]$ справедливо тогда и только тогда, когда выполнены следующие два условия:*

a) *для любого $p \in \mathscr{P}[n]$ в множестве $\{n_1, \ldots, n_s\}$ найдется число, кратное p;*

b) $d \leqslant 2$.

Доказательства теорем 2 и 3 содержатся в разделах 3 и 4 соответственно.

2. Вспомогательные результаты

В первую очередь отметим, что между рассматриваемым порождением чисел и бесповторной суперпозицией булевых функций известна следующая взаимосвязь.

Утверждение 2. *Пусть $f(x_1, \ldots, x_n)$, $g_1(x_1, \ldots, x_{k(1)}), \ldots, g_n(x_1, \ldots, x_{k(n)})$ — булевы функции и*

$$h(x_1^{(1)}, \ldots, x_{k(1)}^{(1)}, \ldots, x_1^{(n)}, \ldots, x_{k(n)}^{(n)}) = f\left(g_1(x_1^{(1)}, \ldots, x_{k(1)}^{(1)}), \ldots, g_n(x_1^{(n)}, \ldots, x_{k(n)}^{(n)})\right).$$

Тогда для любых $\rho_1^{(1)}, \ldots, \rho_{k(1)}^{(1)}, \ldots, \rho_1^{(n)}, \ldots, \rho_{k(n)}^{(n)} \in (0,1)$ выполняется соотношение

$$\mathscr{P}\{h(\rho_1^{(1)}, \ldots, \rho_{k(1)}^{(1)}, \ldots, \rho_1^{(n)}, \ldots, \rho_{k(n)}^{(n)})\} = \mathscr{P}\left\{f\left(\mathscr{P}\{g_1(\rho_1^{(1)}, \ldots, \rho_{k(1)}^{(1)})\}, \ldots, \mathscr{P}\{g_n(\rho_1^{(n)}, \ldots, \rho_{k(n)}^{(n)})\}\right)\right\}.$$

Доказательство утверждения 2, по существу, сводится к непосредственной проверке приведенного в нем равенства и поэтому нами опущено. Строгое доказательство данного факта можно найти, например, в [6].

Следствие 1. *Для любого множества* $H \subseteq (0,1)$ *выполняется равенство* $[[H]] = [H]$.

Таким образом, введенная нами операция замыкания числовых множеств относительно рассматриваемого порождения чисел является корректно определенной с точки зрения стандартных свойств операции замыкания.

Рассмотрим функцию отрицания $f^{\neg}(x) = \overline{x}$. Ясно, что $\mathscr{P}\{f^{\neg}(\rho)\} = 1 - \rho$ для любого $\rho \in (0,1)$. Поэтому справедливо следующее

Утверждение 3. *Если* M *— замкнутое множество и* $\rho \in (0,1)$, *то* $\rho \in$ M *тогда и только тогда, когда* $1 - \rho \in$ M.

Пользуясь этим фактом и следствием 1, получаем

Следствие 2. *Если* $H \subseteq (0,1)$ *и* $\rho \in (0,1)$, *то* $\rho \in [H]$ *тогда и только тогда, когда* $1 - \rho \in [H]$.

Подобная симметрия между числами ρ и $1 - \rho$ имеет место также для порождающих множеств.

Утверждение 4. *Пусть* $H \subseteq (0,1)$ *и* $\rho \in (0,1)$. *Тогда* $[H \cup \{\rho\}] = [H \cup \{1 - \rho\}]$.

Доказательство. Пусть a — произвольное число из $[H \cup \{\rho\}]$, т. е. $a = \mathscr{P}\{f(\rho_1, \ldots, \rho_k)\}$ для некоторой функции $f(x_1, \ldots, x_k)$ и некоторых $\rho_1, \ldots, \rho_k$ из $H \cup \{\rho\}$. Не ограничивая общности, будем считать, что $\rho_1 = \ldots = \rho_i = \rho$ и $\rho_{i+1}, \ldots, \rho_k \in H$, где $0 \leqslant i \leqslant k$. Тогда, применяя утверждение 2, получаем, что $a = \mathscr{P}\{f'(\rho'_1, \ldots, \rho'_k)\}$, где $f'(x_1, \ldots, x_k) = f(\overline{x}_1, \ldots, \overline{x}_i, x_{i+1}, \ldots, x_k)$, $\rho'_1 = \ldots = \rho'_i = 1 - \rho$ и $\rho'_{i+1} = \rho_{i+1}, \ldots, \rho'_k = \rho_k$. Следовательно, $a \in [H \cup \{1 - \rho\}]$. Таким образом, $[H \cup \{\rho\}] \subseteq [H \cup \{1 - \rho\}]$ и поэтому в силу симметрии между числами ρ и $1 - \rho$ имеем $[H \cup 1 - \rho] = [H \cup \{\rho\}]$.

Аналогично, рассмотрев функцию логического умножения $f^{\&}(x_1, x_2) = x_1 x_2$ и воспользовавшись тем, что $\mathscr{P}\{f^{\&}(\rho_1, \rho_2)\} = \rho_1 \rho_2$ для любых $\rho_1, \rho_2 \in (0,1)$, получаем

Утверждение 5. *Пусть* M *— замкнутое множество чисел и* $\rho_1, \rho_2 \in M$. *Тогда* $\rho_1 \rho_2 \in M$.

В дальнейшем воспользуемся следующими двумя известными теоретико-числовыми фактами (см., например, [1]).

Теорема Эйлера. *Если* $(a, m) = 1$ *и* $m > 1$, *то*

$$a^{\varphi(m)} \equiv 1 \pmod{m}.$$

Утверждение 6. *Если* $(n, m) = 1$ *и* x *пробегает полную систему вычетов по модулю* m, *то* $nx + b$, *где* b *— любое целое, также пробегает полную систему вычетов по модулю* m.

Из утверждения 6 непосредственно следует, что если $(n, m) = 1$, то существует целое x такое, что $nx \equiv 1 \pmod{m}$. Тем самым справедливо следующее

Следствие 3. *Если n и m натуральные взаимно простые числа, то уравнение $nx + my = 1$ разрешимо в целых числах.*

Следствие 3 легко обобщается на случай произвольных пар натуральных чисел.

Следствие 4. *Если n и m натуральные числа и $d = (n, m)$, то существуют такие целые x и y, что $nx + my = d$.*

Доказательство необходимости критерия из теорем 2 и 3 базируется на следующей лемме.

Лемма 1. *Пусть $H = \left\{\frac{m_1}{n_1}, \ldots, \frac{m_s}{n_s}\right\}$ — конечное множество несократимых дробей из интервала $(0; 1)$, $d = (m_1(n_1 - m_1), \ldots, m_s(n_s - m_s))$ при $s \geqslant 2$ и $d = m_1(n_1 - m_1)$ при $s = 1$. Если $d > 2$, то $G[n_1] \not\subseteq [H]$.*

Отметим, что аналогичное утверждение для случая одноэлементных порождающих множеств было доказано в [11]. Мы приводим доказательство данного факта в общем случае.

Доказательство леммы 1. Нетрудно заметить, что если $d > 2$, то d либо имеет простой делитель, больший или равный 3, либо является степенью числа 2 и, следовательно, делится на 4. Поэтому среди делителей числа d можно выбрать некоторый делитель $q \geqslant 3$, который либо является простым числом, либо равен 4 и, следовательно, в любом случае является степенью простого числа. Пользуясь этим фактом и тем, что $(m_1, n_1 - m_1) = \ldots = (m_s, n_s - m_s) = 1$ и все числа $m_1(n_1 - m_1), \ldots, m_s(n_s - m_s)$ делятся на q, получаем, что для каждого $i = 1, \ldots, s$ либо число m_i, либо число $n_i - m_i$ делится на q. Поэтому для любого $i = 1, \ldots, s$ либо дробь $\frac{m_i}{n_i}$, либо дробь $1 - \frac{m_i}{n_i} = \frac{n_i - m_i}{n_i}$ имеет числитель, кратный q. Следовательно, в силу утверждения 4 без ограничения общности можно считать, что все числа $m_1, \ldots, m_s$ делятся на q. Пусть $\frac{m}{n}$ — произвольная дробь из $[H]$. Тогда найдется булева функция $f(x_1, \ldots, x_t)$ такая, что $\frac{m}{n} = \mathscr{P}\left\{f\left(\frac{m'_1}{n'_1}, \ldots, \frac{m'_t}{n'_t}\right)\right\}$ для некоторых $\frac{m'_1}{n'_1}, \ldots, \frac{m'_t}{n'_t} \in H$. Обозначив m'_i через $m_i'^{(1)}$ и $n'_i - m'_i$ через $m_i'^{(0)}$, $1 \leqslant i \leqslant t$, получаем, что $\frac{m}{n} = \frac{m'}{n'_1 \ldots n'_t}$, где

$$m' = \sum_{(\sigma_1, \ldots, \sigma_t) \in \mathscr{N}(f)} m_1'^{(\sigma_1)} \ldots m_t'^{(\sigma_t)}. \tag{1}$$

Рассмотрим два возможных случая.

а) Пусть $f(0,\dots,0)=0$. Ясно, что в этом случае в каждом слагаемом $m_1'^{(\sigma_1)}\dots m_t'^{(\sigma_t)}$ из суммы (1) найдется некоторый сомножитель $m_i'^{(1)}=m_i'$, который делится на q. Поэтому любое слагаемое из суммы (1) делится на q. Следовательно, m' делится на q. Так как никакое из чисел $n_1',\dots,n_t'$ не может быть кратным q, то m делится на q.

б) Пусть $f(0,\dots,0)=1$. Тогда согласно утверждению 2 имеем $\mathscr{P}\left\{\bar f\left(\frac{m_1'}{n_1'},\dots,\frac{m_t'}{n_t'}\right)\right\}=1-\mathscr{P}\left\{f\left(\frac{m_1'}{n_1'},\dots,\frac{m_t'}{n_t'}\right)\right\}=1-\frac{m}{n}=\frac{n-m}{n}$ и $\bar f(0,\dots,0)=0$. Следовательно, рассуждая далее аналогично случаю $f(0,\dots,0)=0$, получаем, что $n-m$ делится на q.

Таким образом, для любой дроби m/n из $[H]$ либо $m\equiv 0 \pmod q$, либо $m\equiv n \pmod q$. Выберем натуральное r такое, что $n^r>q$. Так как $q-1\geqslant 2$, то среди чисел $1,\dots,q-1$ найдется некоторое число m'', не принадлежащее классу вычетов числа n^r по модулю q (т. е. множеству чисел, сравнимых с n^r по модулю q). Поскольку m'' также не содержится в классе вычетов числа 0 по модулю q, то $m''/n^r\notin[H]$. Следовательно, $G[n_1]\not\subseteq[H]$.

Основным фактом, используемым для доказательства достаточности условий теорем 2 и 3, является следующая

Лемма 2. *Пусть l/n — произвольная несократимая дробь из интервала $(0;1)$. Тогда для любого $\varepsilon>0$ существует такое $K(\varepsilon)\in\mathbf{N}$, что для каждого целого $k\geqslant K(\varepsilon)$ любая дробь mn^{-k} такая, что $\varepsilon\leqslant mn^{-k}\leqslant 1-\varepsilon$ и m делится на $l(n-l)$, принадлежит множеству $[\{l/n\}]$.*

Доказательство. Если $l/n=1/2$, то утверждение леммы непосредственно следует из теоремы 1. Пусть $l/n\neq 1/2$. Так как согласно утверждению 4 имеем $[mn^{-k}]=[1-mn^{-k}]$, то, не ограничивая общности, будем считать, что $l/n>1/2$, т. е. $l>n-l$. В этом случае

$$\sum_{j=0}^{\infty}\left(\frac{n-l}{l}\right)^j=\frac{1}{1-\frac{n-l}{l}}=\frac{l}{2l-n}\leqslant l. \tag{2}$$

Пусть $\varepsilon>0$. В качестве $K(\varepsilon)$ выберем такое число, чтобы любое k, не меньшее $K(\varepsilon)$, удовлетворяло следующим двум неравенствам:

$$k\geqslant l\cdot\max(2,n-l), \tag{3}$$

$$\left(\frac{l}{n}\right)^k<\frac{\varepsilon}{l(n-l)}. \tag{4}$$

Без ограничения общности будем также считать, что $k\geqslant 3$.

Рассмотрим произвольную дробь mn^{-k}, удовлетворяющую условиям леммы. Обозначим через m' целое число $m/(l(n-l))$. Заметим, что для

любого двоичного набора $\tilde{\sigma} = (\sigma_1 \dots \sigma_k)$ из $\{0,1\}^k$ выполняется соотношение

$$\mathscr{P}_{\tilde{\sigma}}\left(\frac{l}{n},\dots,\frac{l}{n}\right) = \left(\frac{l}{n}\right)_{\sigma_1} \dots \left(\frac{l}{n}\right)_{\sigma_k} = \frac{l^{\|\tilde{\sigma}\|}(n-l)^{k-\|\tilde{\sigma}\|}}{n^k}.$$

Для удобства величину $n^k \mathscr{P}_{\tilde{\sigma}}(l/n,\dots,l/n)$, равную $l^{\|\tilde{\sigma}\|}(n-l)^{k-\|\tilde{\sigma}\|}$, обозначим через $m(\tilde{\sigma})$. Величину $m(\tilde{\sigma})/(l(n-l))$, равную $l^{\|\tilde{\sigma}\|-1}(n-l)^{k-\|\tilde{\sigma}\|-1}$, обозначим через $m'(\tilde{\sigma})$. Ясно, что если $\tilde{\sigma} \neq (0,\dots,0)$ и $\tilde{\sigma} \neq (1,\dots,1)$, то $m'(\tilde{\sigma})$ является целым числом. Аналогично если $f(x_1,\dots,x_k)$ — булева функция, то положим $m(f) = n^k \mathscr{P}\{f(l/n,\dots,l/n)\}$ и $m'(f) = m(f)/(l(n-l))$. Очевидно, что если $f \not\equiv 0$, то

$$m'(f) = \sum_{\tilde{\sigma} \in \mathscr{N}_f} m'(\tilde{\sigma}). \tag{5}$$

Следовательно, если $f(0,\dots,0) = f(1,\dots,1) = 0$, то $m'(f)$ является целым числом. Кроме того, с учетом формулы для вычисления величины $m'(\tilde{\sigma})$ равенство (5) можно переписать в следующем виде:

$$m'(f) = \sum_{i=0}^{k} |\mathscr{N}(f) \cap B_i^k| l^{i-1}(n-l)^{k-i-1}. \tag{6}$$

Формулу (6) можно также обобщить следующим образом. Пусть $f'(x_1,\dots,x_k)$ и $f''(x_1,\dots,x_k)$ — булевы функции и пусть $\delta_i = |\mathscr{N}(f'') \cap B_i^k| - |\mathscr{N}(f') \cap B_i^k|$, $i = 0,1,\dots,k$. Тогда из (6) непосредственно следует, что

$$m'(f'') = m'(f') + \sum_{i=0}^{k} \delta_i l^{i-1}(n-l)^{k-i-1}. \tag{7}$$

Построим последовательность $a_0, a_1, \dots, a_{k-2}$ чисел из множества $\{0,1,\dots,l-1\}$ такую, что для любого $i = 0,1,\dots,k-2$ справедливо сравнение

$$m' \equiv \sum_{j=0}^{i} a_j l^{j-1}(n-l)^{k-j-1} \pmod{l^i}. \tag{8}$$

Числа a_i из этой последовательности будем задавать индукцией по i. Положим $a_0 = 0$. В этом случае для $i = 0$, очевидно, выполняется соотношение (8). Предположим, что для некоторого $r \in \{0,1,\dots,k-3\}$ мы уже нашли числа $a_0, a_1, \dots, a_r$ и тем самым для $i = r$ справедливо соотношение (8). Следовательно, число $m' - \sum_{j=0}^{r} a_j l^{j-1}(n-l)^{k-j-1}$ делится на l^r. Обозначим через b_r целое число $\left(m' - \sum_{j=0}^{r} a_j l^{j-1}(n-l)^{k-j-1}\right) \Big/ l^r$.

Так как $(l, n-l) = 1$ и тем самым $(l, (n-l)^{k-r-2}) = 1$, то согласно утверждению 6 в полной системе вычетов $\{0, 1, \ldots, l-1\}$ по модулю l найдется такое число a_{r+1}, что будет справедливо сравнение

$$a_{r+1}(n-l)^{k-r-2} \equiv b_r \pmod{l}.$$

Домножив обе части и модуль данного сравнения на l^r, получим соотношение, эквивалентное соотношению (8) для $i = r+1$. Таким образом, мы можем найти все числа $a_1, \ldots, a_{k-2}$ искомой последовательности.

Поскольку в силу неравенства (3) для любого $i = 1, \ldots, k-2$ имеем $a_i \leqslant l \leqslant k \leqslant \binom{k}{i} = |B_i^n|$, то можно построить булеву функцию $f_0(x_1, \ldots, x_k)$ такую, что $|\mathscr{N}(f_0) \cap B_0^k| = |\mathscr{N}(f_0) \cap B_{k-1}^k| = |\mathscr{N}(f_0) \cap B_k^k| = 0$ и $|\mathscr{N}(f_i) \cap B_i^k| = a_i$, $1 \leqslant i \leqslant k-2$. В силу равенства (6) имеем

$$m'(f) = \sum_{i=1}^{k-2} a_i l^{i-1}(n-l)^{k-i-1}. \tag{9}$$

Тем самым, используя соотношение (8) для $i = k-2$, с учетом равенства $a_0 = 0$ получаем, что $m'(f_0) \equiv m' \pmod{l^{k-2}}$. Исходя из соотношений (9), (2) и (4) и используя неравенство $(n-l)/l < 1$, получаем следующую верхнюю оценку для величины $\mathscr{P}\{f_0(l/n, \ldots, l/n)\}$:

$$\begin{aligned}
\mathscr{P}\Big\{f_0\Big(\frac{l}{n}, \ldots, \frac{l}{n}\Big)\Big\} &= \frac{l(n-l)}{n^k} m'(f_0) = \frac{l(n-l)}{n^k} \sum_{i=1}^{k-2} a_i l^{i-1}(n-l)^{n-i-1} \\
&\leqslant \frac{l(n-l)}{n^k} \sum_{i=1}^{k-2} l^i (n-l)^{n-i-1} = \frac{l^{k-1}(n-l)^2}{n^k} \sum_{i=1}^{k-2} \Big(\frac{n-l}{l}\Big)^{k-i-2} \\
&= \frac{l^{k-1}(n-l)^2}{n^k} \sum_{j=0}^{k-3} \Big(\frac{n-l}{l}\Big)^j \leqslant \frac{l^{k-1}(n-l)^2}{n^k} \sum_{j=0}^{\infty} \Big(\frac{n-l}{l}\Big)^j \\
&\leqslant \Big(\frac{l}{n}\Big)^k (n-l)^2 < \frac{\varepsilon}{l(n-l)}(n-l)^2 = \frac{n-l}{l}\varepsilon < \varepsilon \leqslant \frac{m}{n^k}.
\end{aligned}$$

Тем самым

$$m'(f_0) = \frac{n^k}{l(n-l)} \mathscr{P}\Big\{f_0\Big(\frac{l}{n}, \ldots, \frac{l}{n}\Big)\Big\} < \frac{n^k}{l(n-l)} \cdot \frac{m}{n^k} = m'. \tag{10}$$

Отправляясь от функции f_0, построим конечную последовательность k-местных булевых функций $f_0, f_1, \ldots, f_t$, которые принимают единичные значения только на наборах из слоев $B_1^k, \ldots, B_{k-2}^k$, а при каждом i, $1 \leqslant i \leqslant t$, выполняются соотношения

$$m'(f_i) \equiv m' \pmod{l^{k-2}}, \tag{11}$$

$$m'(f_i) \leqslant m'(f_{i-1}) + kl^{k-2}. \tag{12}$$

Построение функций f_i будем проводить индукцией по $i = 0, 1, \ldots, t+1$. Для $i = 0$ искомая функция f_0 уже построена. Предположим, что мы построили функцию f_{i-1}, удовлетворяющую требуемым условиям. Если в каждом слое $B_1^k, \ldots, B_{k-2}^k$ имеется менее l наборов, на которых f_{i-1} принимает значение 0, то положим $f_t = f_{i-1}$ и, таким образом, завершим построение искомой последовательности. Предположим, что в некоторых слоях из $\{B_1^k, \ldots, B_{k-2}^k\}$ содержится не менее l наборов, на которых функция f_{i-1} принимает значение 0. Среди этих слоев выберем слой, в котором наборы имеют наименьший вес. Пусть таким слоем является слой $B_{v(i)}^k$. Будем последовательно строить такие функции $f_i^{v(i)}, \ldots, f_i^{k-2}$ от k переменных, которые принимают значение 1 только на наборах из слоев $B_1^k, \ldots, B_k^k$, а при любом $j = v(i), \ldots, k-2$ выполняются соотношения

$$m'(f_i^j) \equiv m' \pmod{l^j}, \tag{13}$$

$$m'(f_i^j) \leqslant m'(f_i^{j-1}) + l^j(n-l)^{k-j-1}, \tag{14}$$

где $f_i^{v(i)-1} = f_{i-1}$. Функцию $f_i^{v(i)}$ можем построить, выбрав в множестве $B_{v(i)}^i \cap \mathscr{N}(\bar{f}_{i-1})$ произвольное подмножество C, состоящее из l наборов, и положив $\mathscr{N}(f_i^{v(i)}) = \mathscr{N}(f_{i-1}) \cup C$. Тогда, используя равенство (7), получим

$$\begin{aligned} m'(f_i^{v(i)}) &= m'(f_{i-1}) + |C| \cdot l^{v(i)-1}(n-l)^{k-v(i)-1} \\ &= m'(f_{i-1}) + l^{v(i)}(n-l)^{k-v(i)-1}. \end{aligned}$$

Таким образом, функция $f_i^{v(i)}$ удовлетворяет как неравенству (14), так и (в силу справедливости соотношения (11) для функции f_{i-1}) соотношению (13). Пусть для некоторого $j \in \{v(i+1), \ldots, k-2\}$ функции $f_i^{v(i)}, \ldots, f_i^{j-1}$, удовлетворяющие соотношениям (13) и (14), уже построены. Обозначим через b целое число $(m' - m'(f_i^{j-1}))/l^{j-1}$. Поскольку в силу неравенства (3) имеем $\left|\mathscr{N}\left(f_i^{j-1}\right) \cap B_j^k\right| + \left|\mathscr{N}\left(\bar{f}_i^{j-1}\right) \cap B_j^k\right| = \left|B_j^k\right| = \binom{k}{j} \geqslant k \geqslant 2l$, то либо $\left|\mathscr{N}\left(\bar{f}_i^{j-1}\right) \cap B_j^k\right| \geqslant l$, либо $\left|\mathscr{N}\left(f_i^{j-1}\right) \cap B_j^k\right| \geqslant l$. Пусть $\left|\mathscr{N}\left(\bar{f}_i^{j-1}\right) \cap B_j^k\right| \geqslant l$. Так как $(l, (n-l)^{n-j-1}) = 1$, то согласно утверждению 6 в полной системе вычетов $\{0, 1, \ldots, l-1\}$ по модулю l найдется число a' такое, что справедливо сравнение

$$a'(n-l)^{n-j-1} \equiv b \pmod{l}.$$

Домножив обе части и модуль данного сравнения на l^{j-1}, получаем

$$m'(f_i^{j-1}) + a'l^{j-1}(n-l)^{n-j-1} \equiv m' \pmod{l^j}. \tag{15}$$

Выбрав в множестве $\mathscr{N}\left(f_i^{j-1}\right) \cap B_j^k$ произвольное подмножество C', состоящее из a' наборов, положим $\mathscr{N}(f_i^j) = \mathscr{N}(f_i^{j-1}) \cup C'$. Тогда, используя равенство (7), получим

$$m'(f_i^j) = m'(f_i^{j-1}) + a' l^{j-1}(n-l)^{n-j-1}.$$

Таким образом, учитывая соотношение (15) и неравенство $a' \leqslant l$, получаем, что построенная функция f_i^j удовлетворяет соотношениям (13) и (14).

Пусть $|\mathscr{N}(f_i^{j-1}) \cap B_j^k| \geqslant l$. В силу утверждения 6 в полной системе вычетов $\{-(l-1), -(l-2), \ldots, 1, 0\}$ по модулю l найдется число a'' такое, что справедливо сравнение

$$a''(n-l)^{n-j-1} \equiv b \pmod{l},$$

из которого, как и в предыдущем случае, вытекает сравнение

$$m'(f_i^{j-1}) + a'' l^{j-1}(n-l)^{n-j-1} \equiv m' \pmod{l^j}. \tag{16}$$

В множестве $\mathscr{N}(f_i^{j-1}) \cap B_j^k$ выберем произвольное подмножество C'', состоящее из $|a''|$ наборов, и положим $\mathscr{N}(f_i^j) = \mathscr{N}(f_i^{j-1}) \setminus C''$. Тогда, используя соотношения (7) и (16), получаем

$$\begin{aligned} m'(f_i^j) &= m'(f_i^{j-1}) - |a''| l^{j-1}(n-l)^{n-j-1} \\ &= m'(f_i^{j-1}) + a'' l^{j-1}(n-l)^{n-j-1} \equiv m' \pmod{l^j}. \end{aligned}$$

Кроме того, ясно, что $m'(f_i^j) \leqslant m'(f_i^{j-1})$. Таким образом, в этом случае функция f_i^j также удовлетворяет соотношениям (13) и (14).

Положим $f_i = f_i^{k-2}$. Тогда в силу соотношения (13) при $j = k-2$ функция f_i удовлетворяет соотношению (11). Кроме того, из соотношений (14) с использованием неравенств (2) и (3) получаем

$$\begin{aligned} m'(f_i) &\leqslant m'(f_{i-1}) + \sum_{j=v(i)}^{k-2} l^j (n-l)^{k-j-1} \\ &= m'(f_{i-1}) + l^{k-2}(n-l) \sum_{j=v(i)}^{k-2} \left(\frac{n-l}{l}\right)^{k-j-2} \\ &= m'(f_{i-1}) + l^{k-2}(n-l) \sum_{j=0}^{k-v(i)-2} \left(\frac{n-l}{l}\right)^{j} \\ &\leqslant m'(f_{i-1}) + l^{k-2}(n-l) \sum_{j=0}^{\infty} \left(\frac{n-l}{l}\right)^{j} \\ &\leqslant m'(f_{i-1}) + l^{k-2}(n-l)l \leqslant m'(f_{i-1}) + kl^{k-2}. \end{aligned}$$

Таким образом, для функции f_i справедливо неравенство (12). Заметим также, что $v(i-1) \leqslant v(i)$, и если $v(i-1) = v(i)$, то $|\mathscr{N}(\bar{f}_i) \cap B^k_{v(i)}| < |\mathscr{N}(\bar{f}_{i-1}) \cap B^k_{v(i-1)}|$. Тем самым построение искомой последовательности $f_0, f_1, \ldots, f_t$ обязательно завершится.

Покажем, что

$$m' \leqslant m'(f_t) + kl^{k-2}. \tag{17}$$

Для этого рассмотрим булеву функцию $f'_t(x_1, \ldots, x_k)$ такую, что $\mathscr{N}(f'_t) = \mathscr{N}(f_t) \cup B^k_{k-1}$. Из соотношения (7) вытекает, что

$$m'(f^*_t) = m'(f_t) + |B^k_{k-1}|l^{k-2} = m'(f_t) + kl^{k-2},$$

а из способа построения функции f'_t следует, что $|\mathscr{N}(\bar{f}'_t) \cap B^k_{k-1}| = 0$ и $|\mathscr{N}(\bar{f}'_t) \cap B^k_i| < l$ при $i = 1, \ldots, k-2$. Отсюда и из соотношений (6), (2) и (4) получаем

$$\begin{aligned}
m'(\bar{f}'_t) &= |\mathscr{N}(\bar{f}'_t) \cap B^k_0| \frac{l^{k-1}}{n-l} + \sum_{i=1}^{k-1} |\mathscr{N}(\bar{f}'_t) \cap B^k_i| l^{i-1}(n-l)^{k-i-1} \\
&\quad + |\mathscr{N}(\bar{f}'_t) \cap B^k_k| (n-l)^{k-1}/l \\
&< \frac{l^{k-1}}{n-l} + \sum_{i=1}^{k-2} l^i (n-l)^{k-i-1} + \frac{(n-l)^{k-1}}{l} \\
&\leqslant l^{k-1} + \sum_{i=1}^{k-2} l^i (n-l)^{k-i-1} + (n-l)^{k-1} = \sum_{i=0}^{k-1} l^i (n-l)^{k-i-1} \\
&= l^{k-1} \sum_{i=0}^{k-1} \left(\frac{n-l}{l}\right)^{k-i-1} < l^{k-1} \sum_{i=0}^{\infty} \left(\frac{n-l}{l}\right)^i \leqslant l^k \\
&= n^k \left(\frac{l}{n}\right)^k < n^k \frac{\varepsilon}{l(n-l)}.
\end{aligned}$$

Тем самым

$$\mathscr{P}\left\{\bar{f}'_t\left(\frac{l}{n}, \ldots, \frac{l}{n}\right)\right\} = \frac{l(n-l)}{n^k} m'(\bar{f}'_t) < \varepsilon.$$

Следовательно, в силу утверждения 2 имеем

$$\mathscr{P}\left\{f'_t\left(\frac{l}{n}, \ldots, \frac{l}{n}\right)\right\} = 1 - \mathscr{P}\left\{\bar{f}'_t\left(\frac{l}{n}, \ldots, \frac{l}{n}\right)\right\} > 1 - \varepsilon \geqslant \frac{m}{n^k}.$$

Поэтому

$$m'(f_t) + kl^{k-2} = m'(\bar{f}'_t) = \frac{n^k}{l(n-l)} \mathscr{P}\left\{f'_t\left(\frac{l}{n}, \ldots, \frac{l}{n}\right)\right\} \geqslant \frac{m}{l(n-l)} = m'.$$

Пусть S — подмножество всех таких функций f_i из последовательности $\{f_0, f_1, \ldots, f_t\}$, что $m' \leqslant m'(f_i) + kl^{k-2}$. Из неравенства (17) следует, что $f_t \in S$ и поэтому множество S непусто. Следовательно, в S

можно выбрать функцию, имеющую минимальный порядковый номер. Этот номер обозначим через i^*. Покажем, что

$$m'(f_{i^*}) < m'. \tag{18}$$

Если $i^* = 0$, то неравенство (18) непосредственно следует из (10). Пусть $i^* > 0$. Так как i^* — наименьший порядковый номер функции из S, то $f_{i^*-1} \notin S$. Тем самым справедливо неравенство $m'(f_{i^*-1}) + kl^{k-2} < m'$, из которого с учетом соотношения (12) при $i = i^*$ вытекает неравенство (18). Таким образом,

$$m'(f_{i^*}) < m' \leqslant m'(f_{i^*}) + kl^{k-2},$$

т. е.

$$0 < m' - m'(f_{i^*}) \leqslant kl^{k-2}, \tag{19}$$

и в силу неравенства (11) имеем $m' - m'(f_{i^*}) \equiv 0 \pmod{l^{k-2}}$. Обозначим через d целое число, равное $(m' - m'(f_{i^*}))/l^{k-2}$. Из соотношения (19) вытекает, что $0 < d \leqslant k$. Поэтому в B^k_{k-1} можно выделить некоторое подмножество D, состоящее из d наборов.

Обозначим через $\hat{f}$ булеву функцию от k переменных такую, что $\mathscr{N}(\hat{f}) = \mathscr{N}(f_{i^*}) \cup D$. Используя равенство (6), получаем

$$m'(\hat{f}) = m'(f_{i^*}) + dl^{k-2} = m'(f_{i^*}) + \frac{m' - m'(f_{i^*})}{l^{k-2}} l^{k-2} = m'.$$

Следовательно,

$$\mathscr{P}\Big\{\hat{f}\Big(\frac{l}{n}, \ldots, \frac{l}{n}\Big)\Big\} = \frac{l(n-l)}{n^k} m' = \frac{m}{n^k}.$$

Таким образом, $mn^{-k} \in [\{l/n\}]$. Лемма 2 доказана.

Следствие 5. *Пусть l/n — произвольная несократимая дробь из интервала $(0;1)$. Тогда любая дробь mn^{-k} из $G[n]$, где m делится на $l(n-l)$, принадлежит множеству $[\{l/n\}]$.*

Доказательство. Справедливость данного утверждения вытекает из леммы 2 с учетом того, что любая дробь mn^{-k} может быть представлена, если это необходимо, в виде $\frac{mn^{K(\varepsilon)-k}}{n^{K(\varepsilon)}}$, где $\varepsilon = \min\left(\frac{m}{n^k}, 1 - \frac{m}{n^k}\right)$.

3. Доказательство теоремы 2

Лемма 3. *Пусть p — простое число, M — замкнутое множество чисел, $m_1, m_2 \in \mathbf{N}$ и $(m_1, p) = (m_2, p) = 1$. Далее, пусть любая дробь mp^{-r} из $G[p]$, где m делится на m_1 или на m_2, принадлежит множеству M. Тогда любая дробь mp^{-r} из $G[p]$, где m делится на (m_1, m_2), принадлежит множеству M.*

Доказательство. Пусть mp^{-r} — произвольная дробь из $G[p]$, где m делится на (m_1, m_2). Выберем натуральные числа r_1 и r_2 такие, что $p^{r_1} > m_1 m_2$, $r_2 \geqslant r$ и r_2 кратно числу $\varphi(m_1)$. Так как число $mp^{r_1+r_2-r}$ делится на (m_1, m_2), то в силу следствия 4 найдутся такие целые c_1, c_2, что

$$mp^{r_1+r_2-r} = c_1 m_1 + c_2 m_2; \tag{20}$$

при этом в качестве c_2 мы, очевидно, можем выбрать некоторое число из множества $\{1, \ldots, m_1\}$. Следовательно,

$$0 < c_2 m_2 \leqslant m_1 m_2 < p^{r_1}. \tag{21}$$

Поэтому в силу равенства (20) имеем

$$p^{r_1+r_2} > mp^{r_1+r_2-r} > c_1 m_1 > mp^{r_1+r_2-r} - p^{r_1} \geqslant p^{r_1+r_2-r} - p^{r_1} \geqslant 0.$$

Таким образом, $\frac{c_1 m_1}{p^{r_1+r_2}} \in G[p]$ и согласно условиям доказываемой леммы $\frac{c_1 m_1}{p^{r_1+r_2}} \in M$. Рассмотрим дробь $\frac{c_1 m_1 + p^{r_1}}{p^{r_1+r_2}}$. Так как

$$0 < c_1 m_1 + p^{r_1} < mp^{r_1+r_2-r} + p^{r_1} \leqslant (m+1)p^{r_1+r_2-r} \leqslant p^r p^{r_1+r_2-r} = p^{r_1+r_2},$$

то $\frac{c_1 m_1 + p^{r_1}}{p^{r_1+r_2}} \in G[p]$. Следовательно, $1 - \frac{c_1 m_1 + p^{r_1}}{p^{r_1+r_2}} = \frac{p^{r_1+r_2} - p^{r_1} - c_1 m_1}{p^{r_1+r_2}} \in G[p]$. Поскольку r_2 делится на $\varphi(m_1)$ и $(p, m_1) = 1$, то согласно теореме Эйлера $p^{r_2} - 1$ делится на m_1. Отсюда следует, что $p^{r_1+r_2} - p^{r_2} - c_1 m_1 = p^{r_1}(p^{r_2} - 1) - c_1 m_1$ делится на m_1. Поэтому согласно условиям леммы имеем $1 - \frac{c_1 m_1 + p^{r_1}}{p^{r_1+r_2}} \in M$. Следовательно, в силу утверждения 3 получаем, что $\frac{c_1 m_1 + p^{r_1}}{p^{r_1+r_2}} \in M$. Аналогично из неравенств (21) и условий леммы вытекает, что $\frac{c_2 m_2}{p^{r_1}} \in M$. Рассмотрим булеву функцию $f^+(x, y, z) = x\overline{z} \vee yz$. Нетрудно убедиться, что

$$\mathscr{P}\Big\{f^+(\rho_x, \rho_y, \rho_z)\Big\} = \rho_x(1 - \rho_z) + \rho_y \rho_z.$$

Пользуясь этим соотношением и равенством (20), имеем

$$\begin{aligned}\mathscr{P}\Big\{f^+\Big(\frac{c_1 m_1}{p^{r_1+r_2}}, \frac{c_1 m_1 + p^{r_1}}{p^{r_1+r_2}}, \frac{c_2 m_2}{p^{r_1}}\Big)\Big\} &= \frac{c_1 m_1}{p^{r_1+r_2}}\Big(1 - \frac{c_2 m_2}{p^{r_1}}\Big) + \frac{c_1 m_1 + p^{r_1}}{p^{r_1+r_2}} \cdot \frac{c_2 m_2}{p^{r_1}} \\ &= \frac{c_1 m_1 + c_2 m_2}{p^{r_1+r_2}} = \frac{mp^{r_1+r_2-r}}{p^{r_1+r_2}} = \frac{m}{p^r}.\end{aligned}$$

Так как $\frac{c_1 m_1}{p^{r_1+r_2}}, \frac{c_1 m_1 + p^{r_1}}{p^{r_1+r_2}}, \frac{c_2 m_2}{p^{r_1}} \in M$ и множество M замкнуто, то $\frac{m}{p^r} \in M$.

Следствие 6. *Пусть $s \geqslant 2$, p — простое число, M — замкнутое множество чисел, $m_1, \ldots m_s$ — натуральные числа такие, что $(m_1, p) = \ldots = (m_s, p) = 1$. Пусть для каждого $i = 1, \ldots, s$ любая дробь mp^{-r}*

из $G[p]$, где m делится на m_i, принадлежит множеству M. Тогда любая дробь mp^{-r} из $G[p]$, где m делится на $(m_1, \dots, m_s)$, принадлежит множеству M.

Данное утверждение непосредственно вытекает из леммы 3 применением индукции по s.

Лемма 4. *Пусть p — простое число, $H = \left\{\frac{m_1}{p^{r_1}}, \dots, \frac{m_s}{p^{r_s}}\right\}$ — конечное множество несократимых дробей из $G[p]$, $d = (m_1(p^{r_1} - m_1), \dots, m_s(p^{r_s} - m_s))$ при $s \geqslant 2$ и $d = m_1(p^{r_1} - m_1)$ при $s = 1$. Тогда любая дробь mp^{-r} из $G[p]$, где m делится на d, принадлежит множеству $[H]$.*

Доказательство. Ясно, что для каждого $i = 1, \dots, s$ любая дробь mp^{-r} из $G[p]$ при необходимости может быть представлена в виде дроби $\frac{mp^{r_i k - r}}{p^{r_i k}}$, где $k = \left\lceil r/r_i \right\rceil$. Поэтому в силу следствия 5 имеем, что для каждого $i = 1, \dots, s$ любая дробь mp^{-r} из $G[p]$, где m делится на $m_i(p^{r_i} - m_i)$, принадлежит множеству $[H]$. При этом по следствию 1 множество $[H]$ является замкнутым. Таким образом, утверждение леммы очевидно при $s = 1$ и вытекает из следствия 6 при $s \geqslant 2$.

Следствие 7. *Пусть p — простое число, $H = \left\{\frac{m_1}{p^{r_1}}, \dots, \frac{m_s}{p^{r_s}}\right\}$ — конечное множество несократимых дробей из $G[p]$, $d = (m_1(p^{r_1} - m_1), \dots, m_s(p^{r_s} - m_s))$ при $s \geqslant 2$ и $d = m_1(p^{r_1} - m_1)$ при $s = 1$. Тогда если $d \leqslant 2$, то $G[p] \subseteq [H]$.*

Доказательство. Если $d = 1$, то данное утверждение непосредственно следует из леммы 4. Пусть $d = 2$. Тогда из соотношения $(d, p) = 1$ вытекает, что $p \neq 2$. Следовательно, p — нечетное число. Поэтому любая дробь $\frac{m}{p^r}$ из $G[p]$ либо дробь $1 - \frac{m}{p^r} = \frac{p^r - m}{p^r}$ имеет четный числитель и тем самым согласно лемме 4 принадлежит множеству $[H]$. Следовательно, в силу следствия 2 обе эти дроби принадлежат множеству $[H]$. Таким образом, и в этом случае $G[p] \subseteq [H]$.

Остается заметить, что из следствия 7 непосредственно вытекает достаточность условий теоремы 2. Необходимость этих условий следует из леммы 1.

4. Доказательство теоремы 3

При доказательстве теоремы 3 используется следующая лемма, являющаяся обобщением леммы 3.

Лемма 5. *Пусть n_1, n_2, m_1, m_2 — такие натуральные числа, что $n_1, n_2 > 1$ и $(m_1, n_1) = (m_1, n_2) = (m_2, n_2) = 1$. Далее, пусть $0 \leqslant \varepsilon < 1/2$, M — замкнутое множество чисел, содержащее любую дробь $m/n_1^r < 1 - \varepsilon$ из $G[n_1]$, где m делится на m_1, и любую дробь m/n_2^r из $G[n_2]$, где m*

делится на m_2. *Тогда в* M *содержится любая дробь* m/n_1^r *из* $G[n_1]$, *где* $\varepsilon < m/n_1^r < 1-\varepsilon$ *и* m *делится на* (m_1, m_2).

Доказательство. Пусть m/n_1^r — произвольная дробь из $G[p]$, где m делится на (m_1, m_2), $\varepsilon < m/n_1^r < 1-\varepsilon$. Выберем такие натуральные числа r_1 и r_2, которые кратны числу $\varphi(m_1)$ и удовлетворяют неравенствам $m_1 m_2 < n_2^{r_2} < n_1^{r_1-r}$. Так как число $mn_1^{r_1-r}$ делится на (m_1, m_2), то согласно следствию 4 найдутся такие целые c_1, c_2, что

$$mn_1^{r_1-r} = c_1 m_1 + c_2 m_2; \tag{22}$$

при этом в качестве c_2 мы, очевидно, можем выбрать некоторое число из множества $\{1, \ldots, m_1\}$. Следовательно,

$$0 < c_2 m_2 \leqslant m_1 m_2 < n_2^{r_2} < n_1^{r_1-r}. \tag{23}$$

Поэтому $\frac{c_2 m_2}{n_2^{r_2}} \in G[n_2]$ и в силу условий доказываемой леммы $\frac{c_2 m_2}{n_2^{r_2}} \in M$. Из соотношений (22) и (23) следует, что

$$0 \leqslant (m-1)n_1^{r_1-r} = mn_1^{r_1-r} - n_1^{r_1-r} < c_1 m_1 < mn_1^{r_1-r}.$$

Поэтому

$$0 < \frac{c_1 m_1}{n_1^{r_1}} < \frac{mn_1^{r_1-r}}{n_1^{r_1}} = \frac{m}{n_1^r} < 1-\varepsilon,$$

т. е. $0 < \frac{c_1 m_1}{n_1^{r_1}} < 1-\varepsilon$, и в силу условий леммы $\frac{c_1 m_1}{n_1^{r_1}} \in M$. Из соотношений (22) и (23) также следует, что

$$mn_1^{r_1-r} < c_1 m_1 + n_2^{r_2} < mn_1^{r_1-r} + n_1^{r_1-r} = (m+1)n_1^{r_1-r}.$$

Поэтому

$$\varepsilon < \frac{m}{n_1^r} = \frac{mn_1^{r_1-r}}{n_1^{r_1}} < \frac{c_1 m_1 + n_2^{r_2}}{n_1^{r_1}} < \frac{(m+1)n_1^{r_1-r}}{n_1^{r_1}} = \frac{m+1}{n_1^r} \leqslant 1.$$

Таким образом, $\varepsilon < \frac{c_1 m_1 + n_2^{r_2}}{n_1^{r_1}} < 1$ и, следовательно, $0 < 1 - \frac{c_1 m_1 + n_2^{r_2}}{n_1^{r_1}} < 1-\varepsilon$. Так как r_1 и r_2 делятся на $\varphi(m_1)$ и $(m_1, n_1) = (m_1, n_2) = 1$, то из теоремы Эйлера следует, что $n_1^{r_1} \equiv 1 \pmod{m_1}$, $n_2^{r_2} \equiv 1 \pmod{m_1}$. Поэтому $n_1^{r_1} - n_2^{r_2}$ делится на m_1. Таким образом, $n_1^{r_1} - n_2^{r_2} - c_1 m_1$ делится на m_1 и поэтому в силу условий леммы получаем $1 - \frac{c_1 m_1 + n_2^{r_2}}{n_1^{r_1}} = \frac{n_1^{r_1} - c_1 m_1 - n_2^{r_2}}{n_1^{r_1}} \in M$. Следовательно, согласно утверждению 3 имеем $\frac{c_1 m_1 + n_2^{r_2}}{n_1^{r_1}} \in M$. Рассмотрим булеву функцию f^+, определенную в доказательстве леммы 3. Напомним, что

$$\mathscr{P}\Big\{f^+(\rho_x, \rho_y, \rho_z)\Big\} = \rho_x(1-\rho_z) + \rho_y \rho_z.$$

Используя (22), получаем

$$\mathscr{P}\Big\{f^+\Big(\frac{c_1m_1}{n_1^{r_1}}, \frac{c_1m_1+n_2^{r_2}}{n_1^{r_1}}, \frac{c_2m_2}{n_2^{r_2}}\Big)\Big\}$$
$$= \frac{c_1m_1}{n_1^{r_1}}\Big(1-\frac{c_2m_2}{n_2^{r_2}}\Big) + \frac{c_1m_1+n_2^{r_2}}{n_1^{r_1}}\cdot\frac{c_2m_2}{n_2^{r_2}}$$
$$= \frac{c_1m_1+c_2m_2}{n_1^{r_1}} = \frac{mn_1^{r_1-r}}{n_1^{r_1}} = \frac{m}{n_1^r}.$$

Пользуясь этим фактом и тем, что числа $\frac{c_1m_1}{n_1^{r_1}}, \frac{c_1m_1+n_2^{r_2}}{n_1^{r_1}}, \frac{c_2m_2}{n_2^{r_2}}$ принадлежат множеству M, в силу замкнутости множества M получаем, что $m/n_1^r \in M$.

Лемма 6. *Пусть n_1, n_2, m_1, m_2 — такие натуральные числа, что $n_1, n_2 > 1$ и $(n_1, n_2) = (m_1, n_1) = (m_2, n_2) = 1$, M — замкнутое множество чисел, содержащее любую дробь m/n_1^r из $G[n_1]$, где m делится на m_1, и любую дробь m/n_2^r из $G[n_2]$, где m делится на m_2. Тогда M содержит любую дробь m/n_1^r из $G[n_1]$, где m делится на (m_1, m_2).*

Доказательство. Пусть $m/n_1^r \in G[n_1]$ и m делится на (m_1, m_2). Множество всех простых сомножителей числа m_1 разобьем на две группы: первая группа состоит из всех сомножителей, не являющихся делителями числа n_2, вторая группа — из делителей числа n_2. Обозначим через m_1' и m_1'' произведения всех сомножителей из первой и второй групп соответственно. Заметим, что $m_1 = m_1'm_1''$, $(m_1', n_2) = 1$ и m_1'' является делителем числа n_2^k для некоторого достаточно большого натурального k. Выберем натуральное k_2 такое, что $k_2 \geqslant k$ и $\frac{m_2n_1}{n_2^{k_2}} < \min\Big(\frac{m}{n_1^r}, 1-\frac{m}{n_1^r}\Big)$. В этом случае имеем

$$\frac{m_2n_1}{n_2^{k_2}} < \frac{m}{n_1^r} < 1-\frac{m_2n_1}{n_2^{k_2}} = \frac{n_2^{k_2}-m_2n_1}{n_2^{k_2}}. \tag{24}$$

Покажем, что любая дробь $\frac{m'}{n_1^{r'}}$ из $G[n_1]$ такая, что $\frac{m'}{n_1^{r'}} < \frac{n_2^{k_2}-m_2n_1}{n_2^{k_2}}$ и m' делится на $m_1'(n_2^{k_2}-m_2n_1)$, принадлежит множеству M. Пусть

$$0 < \frac{m'}{n_1^{r'}} < \frac{n_2^{k_2}-m_2n_1}{n_2^{k_2}} \tag{25}$$

и $m' = cm_1'(n_2^{k_2}-m_2n_1)$, где $c \in \mathbf{N}$. Тогда

$$\frac{m'}{n_1^{r'}} = \frac{cm_1'n_2^{k_2}}{n_1^{r'}}\cdot\frac{n_2^{k_2}-m_2n_1}{n_2^{k_2}} = \frac{cm_1d}{n_1^{r'}}\cdot\frac{n_2^{k_2}-m_2n_1}{n_2^{k_2}}, \tag{26}$$

где $d = n_2^{k_2}/m_1'' \in \mathbf{N}$. Так как в силу неравенств (24) дробь $\frac{m_2 n_1}{n_2^{k_2}}$ принадлежит множеству $G[n_2]$, то в силу условий леммы $\frac{m_2 n_1}{n_2^{k_2}} \in M$. Следовательно, согласно утверждению 3 в множестве M содержится дробь $\frac{n_2^{k_2} - m_2 n_1}{n_2^{k_2}}$. Из соотношений (25), (26) следует, что $0 < \frac{cm_1 d}{n_1^{r'}} < 1$. Поэтому в силу условий леммы $\frac{cm_1 d}{n_1^{r'}} \in M$. Таким образом, из равенства (26) согласно утверждению 5 получаем, что $\frac{m'}{n_1^{r'}} \in M$. Поскольку m_1' — делитель числа m, взаимно простого с n_1, и $(n_1, n_2) = 1$, то $(m_1', n_1) = 1$ и $(n_2^{k_2} - m_2 n_1, n_1) = 1$. Следовательно, $(m_1'(n_2^{k_2} - m_2 n_1), n_1) = 1$. Кроме того, поскольку $(m_1', n_2) = (n_1, n_2) = (m_2, n_2) = 1$, то $(m_1'(n_2^{k_2} - m_2 n_1), n_2) = 1$. Таким образом, $(m_1'(n_2^{k_2} - m_2 n_1), n_1) = (m_1'(n_2^{k_2} - m_2 n_1), n_2) = (m_2, n_2) = 1$ и M содержит любую дробь $\frac{m'}{n_1^{r'}} < 1 - \frac{m_2 n_1}{n_2^{k_2}}$ из $G[n_1]$, где $m' \frac{m_2 n_1}{n_2^{k_2}}$ делится на $m_1'(n_2^{k_2} - m_2 n_1)$, и любую дробь $\frac{m'}{n_2^{r'}}$ из $G[n_2]$, где m' делится на m_2. Применяя лемму 5, получаем, что M содержит любую дробь $\frac{m'}{n_1^{r'}}$ из $G[n_1]$ такую, что $\frac{m_2 n_1}{n_2^{k_2}} < \frac{m}{n_1^r} < 1 - \frac{m_2 n_1}{n_2^{k_2}}$ и m' делится на $(m_1'(n_2^{k_2} - m_2 n_1), m_2)$. Так как $(m_2, n_2) = 1$ и m_1'' делит число n_2^k, то $(n_2^{k_2} - m_2 n_1, m_2) = (m_1'', m_2) = 1$. Следовательно, $(m_1'(n_2^{k_2} - m_2 n_1), m_2) = (m_1', m_2) = (m_1' m_1'', m_2) = (m_1, m_2)$. Отсюда и из неравенства (24) следует, что $m/n_1^r \in M$.

Следствие 8. *Пусть* $s \geqslant 2$, *а натуральные числа* $n_1, \ldots, n_s$, $m_1, \ldots, m_s$ *таковы, что* $n_1, \ldots, n_s > 1$, $(m_1, n_1) = \ldots = (m_s, n_s) = 1$, $(n_1, n_2) = \ldots = (n_1, n_s) = 1$. *Далее, пусть* $M \subseteq (0; 1)$ — *замкнутое множество и для каждого* $i = 1, \ldots, s$ *множество* M *содержит любую дробь* m/n_i^r *из* $G[n_i]$, *где* m *делится на* m_i. *Тогда* M *содержит любую дробь* m/n_1^r *из* $G[n_1]$, *где* m *делится на* $(m_1, \ldots, m_s)$.

Справедливость данного утверждения непосредственно вытекает из леммы 6 применением индукции по s.

Доказательство теоремы 3. *Необходимость.* Предположим, что условие a) не выполнено, т. е. для некоторого p из $\mathscr{I}[n]$ во множестве H нет ни одной дроби со знаменателем, кратным p. Это означает, что все дроби из H принадлежат множеству $G[\hat{n}]$, где $\hat{n} = \prod_{q \in \mathscr{I}[n] \setminus \{p\}} q$. Поэтому в силу замкнутости множества $G[\hat{n}]$ получаем, что $[H] \subseteq G[\hat{n}]$. Однако согласно утверждению 1 имеем $G[\hat{n}] \subset G[n]$ и, следовательно, $[H] \subset G[n]$. Необходимость условия b) непосредственно следует из леммы 1.

Достаточность. Пусть выполнено условие a). Рассмотрим произвольное $p \in \mathscr{I}[n]$. Без ограничения общности будем считать, что числа $n_1, \ldots, n_t$, где $1 \leqslant t \leqslant s$, делятся на p, а числа $n_{t+1} \ldots, n_s$ взаимно просты с p. Положим $d' = (m_1(n_1 - m_1), \ldots, m_t(n_t - m_t))$ при $t \geqslant 2$

и $d' = m_1(n_1 - m_1)$ при $t = 1$. Так как при каждом $i = 1, \ldots, t$ любая дробь mp^{-r} из $G[p]$ при необходимости может быть представлена в виде дроби $\frac{m(n_i/p)^r}{n_i^r}$, то в силу следствия 5 при каждом $i = 1, \ldots, t$ любая дробь mp^{-r} из $G[p]$, где m делится на $m_i(n_i - m_i)$, принадлежит множеству $[H]$, которое в силу следствия 1 является замкнутым. Следовательно, применяя следствие 6 в случае $t \geqslant 2$, получаем, что $[H]$ содержит любую дробь mp^{-r} из $G[p]$, где m делится на d'. Покажем, что тогда $[H]$ содержит любую дробь mp^{-r} из $G[p]$, где m делится на d. Для этого заметим, что если $t = s$, то $d = d'$. Пусть $t < s$. Тогда в силу следствия 5 при каждом $i = t, \ldots, s$ любая дробь m/n_i^r из $G[n_i]$, где m делится на $m_i(n_i - m_i)$, принадлежит множеству $[H]$. При этом $(p, n_{t+1}) = \ldots = (p, n_s) = 1$. Следовательно, мы можем применить следствие 8, и убедиться в том, что и в этом случае $[H]$ содержит любую дробь mp^{-r} из $G[p]$, где m делится на $(d', m_{t+1}(n_{t+1} - m_{t+1}), \ldots, m_s(n_s - m_s)) = d$.

Пусть $d \leqslant 2$. Тогда, используя рассуждения, аналогичные доказательству следствия 8, получаем, что $G[p] \in [H]$. Таким образом, при любом $p \in \mathscr{P}[n]$ множество $[H]$ содержит все дроби $\frac{1}{p}, \ldots, \frac{p-1}{p}$ из $G[p]$. Следовательно, пользуясь теоремой 1 и свойством замкнутости множества $[H]$, получаем, что $G[n] \subseteq [H]$. Поэтому в силу замкнутости множества $G[n]$ имеем $G[n] = [H]$.

Заключение

Отметим, что поскольку любое число порождается конечным множеством чисел из порождающего множества, полученный критерий полноты может быть легко сформулирован также для случая бесконечных порождающих подмножеств.

В последнее время все большее внимание уделяется сложностным аспектам моделирования булевых случайных величин. Одним из содержательных понятий сложности случайной величины является минимальное число исходных случайных кодов, необходимое для ее реализации. На языке порождения чисел это понятие соответствует определению сложности порождения числа как минимально возможного количества переменных функции, порождающей данное число. Ряд результатов, связанных со сложностью порождения рациональных чисел преобразователями вероятностных распределений из различных классов, получен автором в [5, 7, 16]. В связи с представленной в данной работе характеризацией всех конечных порождающих подмножеств множеств $G[n]$ естественным образом возникает проблема получения оценок сложности порождения чисел из этих множеств для произвольных конечных порождающих систем.

Автор признателен О. Б. Лупанову за ряд ценных замечаний, высказанных им при обсуждении работы.

ЛИТЕРАТУРА

1. **Виноградов И. М.** Основы теории чисел. М.: Наука, 1981.
2. **Захаров В. М., Салимов Ф. И.** К теории структурного синтеза детерминированных преобразователей вероятности // Problems of Control and Information Theory. 1977. V. 6, N 2. P. 137–148.
3. **Колпаков Р. М.** О порождении рациональных чисел вероятностными контактными сетями // Вестн. МГУ. Математика, механика. 1992. № 5. С. 46–52.
4. **Колпаков Р. М.** О порождении рациональных чисел монотонными функциями // Теоретические и прикладные аспекты математических исследований: Сб. науч. тр. М.: Изд-во Моск. ун-та, 1994. С. 13–17.
5. **Колпаков Р. М.** О порождении рациональных чисел вероятностными контактными π-сетями // Дискрет. математика. 1994. Т. 6, вып. 3. С. 18–38.
6. **Колпаков Р. М.** Порождение рациональных чисел вероятностными сетями и булевыми функциями: Дис. ... канд. физ.-мат. наук. М., 1994.
7. **Колпаков Р. М.** О верхних оценках сложности порождения рациональных чисел вероятностными π-сетями // Вестн. МГУ. Математика, механика. 1995. № 5. С. 99–102.
8. **Нурмеев Н. Н.** О булевых функциях с аргументами, принимающими случайные значения // Проблемы теоретической кибернетики: Тез. докл. VIII Всесоюз. конф. Ч. 2. Горький: Изд-во Горьк. ун-та, 1988. С. 59–60.
9. **Нурмеев Н. Н.** О сложности реализации преобразователей вероятностей схемами из функциональных элементов // Методы и системы технической диагностики: Межвуз. сб. науч. тр. Саратов: Изд-во Сарат. ун-та, 1993. Вып. 18. С. 131–132.
10. **Салимов Ф. И.** К вопросу моделирования булевых случайных величин функциями алгебры логики // Вероятностные методы и кибернетика. Казань: Изд-во Казан. ун-та, 1979. Вып. 15. С. 68–89.
11. **Салимов Ф. И.** Моделирование преобразований случайных кодов функциями k-значной логики: Дис. ... канд. физ.-мат. наук. Казань, 1983.
12. **Салимов Ф. И.** Об одном семействе алгебр распределений // Изв. вузов. Математика. 1988. № 7. С. 64–72.
13. **Салимов Ф. И.** Конечная порожденность алгебр распределений // Дискрет. анализ и исслед. операций. Сер. 1. 1997. Т. 4, № 2. С. 43–50.

14. Схиртладзе Р. Л. О синтезе p-схемы из контактов со случайными дискретными состояниями // Сообщ. АН ГрузССР. 1961. Т. 26, № 2. С. 181–186.

15. Схиртладзе Р. Л. О методе построения булевой случайной величины с заданным распределением вероятностей // Дискретный анализ: Сб. науч. тр. Новосибирск: Ин-т математики СО АН СССР, 1966. Вып. 7. С. 71–80.

16. Kolpakov R. M. On the complexity of generation of rational numbers by Boolean functions // Fund. Inform. 1995. V. 22, N 3. P. 289–298.

Адрес автора:

Московский
государственный университет,
мех.-мат. факультет,
Воробьевы горы,
119899 Москва,
Россия.

Статья поступила
10 декабря 1998 г.