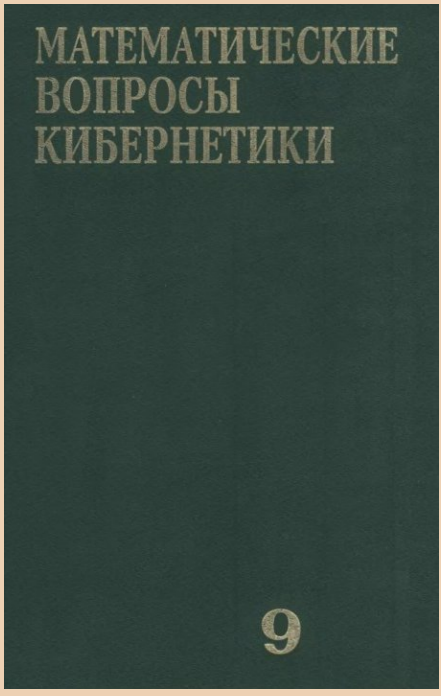
ИПМ им. М.В. Келдыша РАН • Электронная библиотека
Математические вопросы кибернетики • Выпуск 9



Р. М. Колпаков

О преобразованиях булевых случайных величин

Рекомендуемая форма библиографической ссылки: Колпаков Р. М. О преобразованиях булевых случайных величин // Математические вопросы кибернетики. Вып. 9. — М.: ФИЗМАТЛИТ, 2000. — С. 227–252. URL: http://library.keldysh.ru/mvk.asp?id=2000-227

О ПРЕОБРАЗОВАНИЯХ БУЛЕВЫХ СЛУЧАЙНЫХ ВЕЛИЧИН *)

Р. М. КОЛПАКОВ
(МОСКВА)

1. Введение

В структурной теории вероятностных автоматов большое значение имеют вопросы, связанные с преобразованием конечных вероятностных распределений (см. [1]). Одним из наиболее важных как с теоретической, так и с практической точки зрения типов преобразователей вероятностных распределений является преобразователь, который выдает значение моделируемой им случайной величины ζ_0, исходя из значений имеющихся в его распоряжении случайных величин $\zeta_1, \ldots, \zeta_n$ (например, к этому типу относятся активно исследующиеся в последние годы в зарубежной литературе экстракторы [18]). Такой преобразователь естественным образом представляется в виде функции из $\Omega_1 \times \ldots \times \Omega_n$ в Ω_0, где Ω_i — множество значений случайной величины ζ_i, $i = 0, 1, \ldots, n$. В частности, если случайные величины $\zeta_0, \zeta_1, \ldots, \zeta_n$ являются булевыми, т. е. принимают только два различных значения, например, 0 и 1, то данный преобразователь задается некоторой булевой фукцией f: $\{0,1\}^n \to \{0,1\}$. При этом, если случайные величины $\zeta_1, \ldots, \zeta_n$ независимы и вероятность принятия значения 1 случайной величиной ζ_i равна ρ_i, $i = 1, \ldots, n$, то вероятность принятия значения 1 случайной величиной ζ_0 равна

$$\sum_{(\sigma_1 \ldots \sigma_n) \in \{0,1\}^n} (\rho_1)_{\sigma_1} \ldots (\rho_k)_{\sigma_k} f(\sigma_1, \ldots, \sigma_n), \tag{1}$$

где

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

Величину (1) мы будем обозначать через $\mathscr{P}\{f(\rho_1, \ldots, \rho_n)\}$. Через $\mathscr{N}(f)$ мы обозначаем множество всех наборов из $\{0,1\}^n$, на которых функция f обращается в единицу. Используя это обозначение, мы можем переписать $\mathscr{P}\{f(\rho_1, \ldots, \rho_n)\}$ в виде суммы

$$\sum_{(\sigma_1 \ldots \sigma_n) \in \mathscr{N}(f)} (\rho_1)_{\sigma_1} \ldots (\rho_k)_{\sigma_k}.$$

Пусть H — множество чисел из интервала $(0; 1)$. Мы говорим, что 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 $[H]$ замыкание множества H, т. е. множество всех чисел, порождаемых множеством H. Заметим, что, если $f(x) = x$, то

*) Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований (проект 99-01-01175) и Федеральной целевой программы «Интеграция» (проект 473).

$\mathscr{P}\{f(\rho)\} = \rho$ для любого $\rho \in (0; 1)$, тем самым $H \subseteq [H]$. Будем также говорить, что множество $A \subseteq (0; 1)$ *порождается* множеством H, если $A \subseteq [H]$. Мы называем множество H *замкнутым*, если $H = [H]$.

Изучение различных аспектов заданного нами порождения чисел является важным направлением исследований в области синтеза преобразователей вероятностных распределений. Ряд вопросов, связанных с приближенным порождением чисел одноэлементными множествами и некоторыми другими множествами специального вида, был рассмотрен в [10, 16]. Однако вопрос о полном описании замыканий множеств произвольных чисел из интервала (0; 1) остается открытым. Естественным подходом к решению данной проблемы представляется рассмотрение множеств из более узких замкнутых классов чисел, всюду плотных в интервале (0; 1). Таким классом является класс рациональных чисел из интервала (0; 1). Для любого натурального n, большего единицы, мы можем выделить из этого класса подмножество $G[n]$ всех n-ично-рациональных чисел, т. е. множество

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

Нетрудно заметить, что все множества $G[n]$ являются замкнутыми и тем самым представляют собой простейший пример замкнутых подклассов рациональных чисел из интервала (0; 1).

По-видимому, рассматриваемое порождение рациональных чисел впервые изучалось в работе Р. Л. Схиртладзе [15]. В данной работе в качестве преобразователей вероятностных распределений рассматривались вероятностные контактные сети. 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, множеств $G[2]$ и $G[3]$ являются *конечно порожденными*, т. е. порождаются некоторыми своими конечными подмножествами. Дальнейшие исследования в данной области были проведены Ф. И. Салимовым в [11, 14]. Им было доказано, что множество $G[n]$ является конечно порожденным для любого n, и была полностью установлена структура решетки, образуемой множествами $G[n]$. Изучение порождения рациональных чисел в классе вероятностных контактных сетей было продолжено автором в [4, 5]. Была установлена конечная порожденность множеств $G[n]$ в этом классе для всех составных n, а также для $n = 5$ и $n = 7$. В [8] получен критерий порождаемости множеств $G[n]$ произвольными конечными подмножествами при любом n, $n \geqslant 2$. Отметим, что наше исследование фактически является продолжением работы [8] и представленные здесь результаты в значительной степени базируются на результатах этой работы. Мы даем простое описание замыканий произвольных конечных множеств рациональных чисел из интервала (0; 1). Это описание позволяет для любого заданного числа и любого заданного конечного множества рациональных чисел легко определить, порождается ли данное число данным множеством. При исследовании нашей задачи естественно выделяется случай конечных подмножеств множеств $G[p]$, где p — простое число. Наш основной результат для этого случая содержится в разделе 6. В разделе 7 представлен наш основной результат для общего случая.

В работе используются следующие обозначения:

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*);

$|A|$ — число элементов множества A.

2. Вспомогательные результаты

Прежде всего отметим, что существует непосредственная связь между рассматриваемым порождением чисел и бесповторной суперпозицией булевых функций.

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

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

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

$$\mathscr{P}\{h(\rho_1^{(1)}, \ldots, \rho_{k(1)}^{(1)}, \ldots, \rho_1^{(n)}, \ldots, \rho_{k(n)}^{(n)})\} = \\ = \mathscr{P}\left\{\left(\mathscr{P}\{(\rho^0, \ldots, \rho_0^{(0)})\}, \ldots, \mathscr{P}\{(\rho^0, \ldots, \rho_0^{(0)})\}\right)\right\}.$$

Доказательство утверждения 1 по существу сводится к технической проверке приведенного в нем равенства и поэтому нами опущено. Строгое доказательство данного факта можно найти, например, в [6].

Следствие 1. *Для любого множества* H, $H \subseteq (0; 1)$, *множество* $[H]$ *является замкнутым.*

Таким образом, рассматриваемая нами операция замыкания числовых множеств является корректно определенной с точки зрения стандартных свойств операции замыкания.

Рассмотрим функцию $f_{\neg}(x) = \bar{x}$. Очевидно, что $\mathscr{P}\{f_{\neg}(\rho)\} = 1 - \rho$ для любого $\rho \in (0; 1)$. Тем самым справедливо

Утверждение 2. *Если* M — *замкнутое множество, то любое число* ρ *из интервала* $(0; 1)$ *принадлежит* M *тогда и только тогда, когда* $1 - \rho$ *принадлежит* M.

Из этого факта и следствия 1 получаем

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

Рассмотрим булеву функцию $f_*(x, y, z) = x\bar{z} \vee yz$. Нетрудно проверить, что для любых $\rho_x, \rho_y, \rho_z \in (0; 1)$ выполняется равенство

$$\mathscr{P}\{f_*(\rho_x, \rho_y, \rho_z)\} = \rho_x(1 - \rho_z) + \rho_y\rho_z. \tag{2}$$

Следуя терминологии из [2], мы будем называть натуральные числа $a_1, a_2, \ldots, a_k$ *попарно простыми*, если каждое из этих чисел взаимно просто с любым другим из них. Множество натуральных чисел будем называть *разделимым*, если если оно содержит меньше двух чисел, либо все его числа попарно просты. Будем также называть множество натуральных чисел *взаимно простым* с натуральным числом n, если любое число из этого множества взаимно просто с n.

Пусть $A = \{a_1, \ldots, a_k\}$, $B = \{b_1, \ldots, b_t\}$ — конечные множества натуральных чисел. *Наибольшим общим делителем* (A, B) множеств A и B будем называть множество

$$\{(a_i, b_j) \mid i = 1, \ldots, k, j = 1, \ldots, t\},$$

состоящее из наибольших общих делителей всевозможных пар чисел, одно из которых принадлежит множеству A, а другое — множеству B. В случае, если одно из множеств A, B является пустым, для удобства будем считать

$$(A, \varnothing) = (\varnothing, \varnothing) = \varnothing. \tag{3}$$

Заметим, что аналогично операции взятия наибольшего общего делителя чисел введенная нами операция взятия наибольшего общего делителя для множеств чисел обладает свойством ассоциативности и поэтому соответствующим образом обобщается на случай произвольного числа множеств. Именно, если мы имеем s множеств $A_1, \ldots, A_s$ натуральных чисел, где $s \geqslant 2$, то *наибольшим общим делителем* $(A_1, \ldots, A_s)$ этих множеств будем называть множество

$$((\ldots(A_1, A_2), \ldots), A_s) = \{(a_1, a_2, \ldots, a_s) \mid a_1 \in A_1, a_2 \in A_2, \ldots, a_s \in A_s\}.$$

Отметим, что, если множества A и B являются разделимыми, то множество (A, B) также будет разделимым. Обобщив этот факт на случай произвольного числа множеств, получим следующее утверждение.

Утверждение 3. *Наибольший общий делитель разделимых множеств чисел является разделимым множеством.*

Заметим, что, если множество натуральных чисел A взаимно просто с натуральным числом n, то независимо от множества натуральных чисел B множество (A, B) также будет взаимно простым с n. Обобщив это утверждение на случай произвольного числа множеств, можно сформулировать его следующим образом.

Утверждение 4. *Наибольший общий делитель множеств натуральных чисел взаимно прост с любым из чисел, взаимно простых с хотя бы одним из этих множеств.*

Множество натуральных чисел $B = \{b_1, \ldots, b_t\}$ будем называть *мультипликативным разбиением* конечного множества натуральных чисел A, если ему соответствует некоторое разбиение множества A на непересекающиеся (возможно несобственные) подмножества $A_1, \ldots, A_t$ такие, что*) $b_i = \prod\limits_{a \in A_i} a$, $i = 1, \ldots, t$. Отметим, что мультипликативные разбиения обладают следующими очевидными свойствами.

Утверждение 5. *Любое мультипликативное разбиение разделимого множества натуральных чисел является разделимым.*

Утверждение 6. *Если множество натуральных чисел взаимно просто с некоторым натуральным числом n, то любое его мультипликативное разбиение также взаимно просто с n.*

Для любого конечного множества натуральных чисел A будем обозначать через $\|A\|$ произведение всех чисел множества A. Следующий факт является частным случаем утверждения 6.

Следствие 3. *Величина $\|A\|$ взаимно проста с любым натуральным числом, взаимно простым с множеством A.*

Отметим еще одно очевидное свойство наибольшего общего делителя множеств чисел.

Утверждение 7. *Любые конечные разделимые множества A, B удовлетворяют соотношению $\|(A, B)\| = \|A\|\|B\|$.*

В дальнейшем мы воспользуемся следующими известными теоретико-числовыми фактами (см., например, [2]).

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

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

Рассмотрим сравнение первой степени с одним неизвестным

$$ax \equiv b \pmod{m}. \tag{4}$$

*) Здесь и в дальнейшем произведение $\prod\limits_{a \in \varnothing} a$ считается равным единице.

Все решения этого сравнения могут быть легко описаны. Для этого положим $d=(a, m)$.

Лемма 1. *Сравнение* (4) *имеет решения тогда и только тогда, когда* b *делится на* d, *и в этом случае все решения данного сравнения образуют класс вычетов по модулю* m/d.

Согласно лемме 1 в случае, если b делится на d, сравнение (4) имеет решение. Это означает, что существуют целые x и y такие, что $ax+my=b$. Таким образом, мы получаем следующее утверждение.

Следствие 4. *Если* $a, b, c\in N$ *и* c *делится на* (a, b), *то уравнение* $ax+by=c$ *разрешимо в целых числах.*

Пусть $m_1, m_2, \ldots, m_k$ — попарно простые числа. Система сравнений с одним неизвестным

$$\begin{cases} x\equiv b_1 \pmod{m_1}, \\ x\equiv b_2 \pmod{m_2}, \\ \ldots\ldots\ldots\ldots \\ x\equiv b_k \pmod{m_k} \end{cases} \tag{5}$$

всегда имеет решение.

Лемма 2. *Система* (5) *всегда разрешима и все ее решения образуют класс вычетов по модулю* $m_1 m_2 \ldots m_k$.

Замкнутые множества рациональных чисел

Пусть $n, t_1, t_2\in N$, $n\geqslant 2$, $(t_1, t_2)=(t_1, n)=(t_2, n)=1$. Обозначим через $G[n](t_1: t_2)$ следующее подмножество множества $G[n]$:

$$\left\{\frac{m}{n^k} \mid \frac{m}{n^k}\in G[n], m\equiv 0 \pmod{t_1}, m\equiv n^k \pmod{t_2}\right\}.$$

Поскольку $(t_1, t_2)=1$, то, согласно лемме 2, решением системы сравнений

$$\begin{cases} x\equiv 0 \pmod{t_1}, \\ x\equiv n^k \pmod{t_2} \end{cases} \tag{6}$$

является вычет по модулю $t_1 t_2$. Следовательно, в $G[n](t_1: t_2)$ при $n^k > t_1 t_2$ найдется хотя бы одно число со знаменателем, равным n^k, и все такие числа образуют арифметическую прогрессию с разностью $t_1 t_2/n^k$. Отметим также, что, если m удовлетворяет системе (6) и $c\in N$, то, очевидно, $cm\equiv 0 \pmod{t_1}$ и $cm\equiv cn^k \pmod{t_2}$. С другой стороны, если d — общий делитель чисел m и n^k и $(t_1, n)=(t_2, n)=1$, то $(t_1, d)=(t_2, d)=1$, и, следовательно, $m/d\equiv 0 \pmod{t_1}$ и $m/d\equiv n^k/d \pmod{t_2}$. Таким образом, при $(t_1, t_2)=(t_1, n)=(t_2, n)=1$ множество $G[n](t_1: t_2)$ непусто и корректно определено относительно операций сокращения и умножения числителя и знаменателя дроби на одно и то же число. Отметим, что для множеств $G[n](t_1: t_2)$ имеет место следующая очевидная симметрия.

Утверждение 8. *Множество* $G[n](t_1: t_2)$ *содержит число* a *тогда и только тогда, когда* $1-a\in G[n](t_2: t_1)$.

Пусть n — натуральное число, большее единицы, и T — конечное разделимое множество натуральных чисел, взаимно простое с числом n. Обозначим через $\langle G[n]; T\rangle$ следующее подмножество множества $G[n]$:

$$\bigcup_{T'\subseteq T} G[n]\left(\prod_{t\in T'} t: \prod_{t\in T\setminus T'} t\right),$$

где объединение берется по всем, в том числе и несобственным, подмножествам T' множества T. В случае, если $T=\varnothing$, для удобства будем полагать

$$\langle G[n];\varnothing\rangle = G[n]. \tag{7}$$

Покажем, что любое множество $\langle G[n];T\rangle$ является замкнутым.

Лемма 3. *Для любого натурального n, большего единицы, и любого конечного разделимого множества натуральных чисел T, взаимно простого с n, множество $\langle G[n];T\rangle$ является замкнутым.*

Доказательство. Для доказательства леммы необходимо проверить, что для любых чисел $\rho_1,\ldots,\rho_s$ из $\langle G[n];T\rangle$ и любой булевой функции $f(x_1,\ldots,x_s)$, отличной от константы, $\mathscr{P}\{f(\rho_1,\ldots,\rho_s)\}\in\langle G[n];T\rangle$. Докажем это индукцией по s. Для $s=1$ существуют только две отличные от константы булевы функции от одной переменной: тождественная функция $f_{id}(x)=x$, для которой $\mathscr{P}\{f_{id}(\rho_1)\}=\rho_1$, $\rho_1\in\langle G[n];T\rangle$, и функция отрицания $f_\neg(x)=\bar{x}$, для которой $\mathscr{P}\{f_\neg(\rho_1)\}=1-\rho_1$. Так как $\rho_1\in\langle G[n];T\rangle$, то $\rho_1\in G[n]\left(\prod\limits_{t\in T'}t:\ \prod\limits_{t\in T\setminus T'}t\right)$ для некоторого подмножества T' множества T. Тогда согласно утверждению 8 число $1-\rho_1$ принадлежит $G[n]\left(\prod\limits_{t\in T\setminus T'}t:\ \prod\limits_{t\in T'}t\right)\subseteq\langle G[n];T\rangle$. Таким образом, утверждение индукции справедливо для $s=1$. Предположим, что $\mathscr{P}\{g(\rho_1,\ldots,\rho_{s-1})\}\in\langle G[n];T\rangle$ для любых чисел $\rho_1,\ldots,\rho_{s-1}$ из $\langle G[n];T\rangle$ и отличной от константы булевой функции $g(x_1,\ldots,x_{s-1})$. Положим $\mu=\mathscr{P}\{f(\rho_1,\ldots,\rho_s)$. Обозначим через $g_0(x_1,\ldots,x_{s-1})$ и $g_1(x_1,\ldots,x_{s-1})$ функции $f(x_1,\ldots,x_{s-1},0)$ и $f(x_1,\ldots,x_{s-1},1)$, и через μ_0 и μ_1 числа $\mathscr{P}\{g_0(\rho_1,\ldots,\rho_{s-1})\}$ и $\mathscr{P}\{g_1(\rho_1,\ldots,\rho_{s-1})\}$ соответственно. Тогда

$$\mu=\sum_{\tilde{\sigma}\in\mathscr{N}(g_0)}(\rho_1)_{\sigma_1}\ldots(\rho_{s-1})_{\sigma_{s-1}}(\rho_s)_0+\sum_{\tilde{\sigma}\in\mathscr{N}(g_1)}(\rho_1)_{\sigma_1}\ldots(\rho_{s-1})_{\sigma_{s-1}}(\rho_s)_1=$$
$$=(1-\rho_s)\mu_0+\rho_s\mu_1. \tag{8}$$

Для $i=0,1$ согласно индуктивному предположению либо g_i — константа и, соответственно, $\mu_i\in\{0,1\}$, либо $\mu_i\in\langle G[n];T\rangle$. Следовательно, существует некоторое подмножество T_i множества T такое, что μ_i может быть представлено в виде некоторой дроби m_i/n^{k_i}, где $m_i\equiv 0\pmod{\prod\limits_{t\in T_i}t}$ и $m_i\equiv n^{k_i}\pmod{\prod\limits_{t\in T\setminus T_i}t}$ (в случае $\mu_i=0$ можно считать $T_i=T$, в случае $\mu_i=1$, соответственно, $T_i=\varnothing$). Домножив при необходимости числитель и знаменатель одной из дробей m_0/n^{k_0}, m_1/n^{k_1} на подходящий коэффициент, можно считать, что $k_0=k_1$. Аналогичным образом представим число ρ_s из $\langle G[n];T\rangle$ в виде некоторой дроби $m'/n^{k'}$, где $m'\equiv 0\pmod{\prod\limits_{t\in T'}t}$, $m'\equiv n^{k'}\pmod{\prod\limits_{t\in T\setminus T'}t}$, T' — некоторое подмножество множества T. Подставляя в (8) вместо μ_0, μ_1 и ρ_s сопоставленные им дроби, получим

$$\mu=\left(1-\frac{m'}{n^{k'}}\right)\frac{m_0}{n^{k_0}}+\frac{m'}{n^{k'}}\cdot\frac{m_1}{n^{k_0}}=\frac{(n^{k'}-m')m_0+m'm_1}{n^{k_0+k'}}. \tag{9}$$

Обозначим через T_{11}, T_{10}, T_{01}, T_{00} множества $T_0\cap T_1$, $T_0\cap(T\setminus T_1)$, $(T\setminus T_0)\cap T_1$ и $(T\setminus T_0)\cap(T\setminus T_1)$ соответственно. Для каждого $i=0,1$ и каждого $j=0,1$

положим $T'_{ij} = T_{ij} \cap T'$, $T''_{ij} = T_{ij} \cap (T \setminus T')$, $t'_{ij} = \prod\limits_{t \in T'_{ij}} t$, $t''_{ij} = \prod\limits_{t \in T''_{ij}} t$. Заметим, что множество чисел t'_{ij}, t''_{ij}, где $i, j = 0, 1$, является мультипликативным разбиением разделимого множества T, поэтому согласно утверждению 5 все эти числа попарно просты.

Положим $\widehat{T} = T_{11} \cup T'_{10} \cup T''_{01}$. Очевидно, что, $T \setminus \widehat{T} = T_{00} \cup T''_{10} \cup T'_{01}$. Так как $T_0 = T'_{11} \cup T''_{11} \cup T'_{10} \cup T''_{10}$, то $\prod\limits_{t \in T_0} t = t'_{11} t''_{11} t'_{10} t''_{10}$, тем самым выполняется сравнение $m_0 \equiv 0 \pmod{t'_{11} t''_{11} t'_{10} t''_{10}}$. Следовательно, m_0 делится на $t'_{11} t'_{10}$. Так как $T \setminus T' = T''_{11} \cup T''_{10} \cup T''_{01} \cup T''_{00}$, то $\prod\limits_{t \in T \setminus T'} t = t''_{11} t''_{10} t''_{01} t''_{00}$, тем самым верно сравнение $m' \equiv n^{k'} \pmod{t''_{11} t''_{10} t''_{01} t''_{00}}$. Следовательно, $n^{k'} - m'$ делится на $t''_{11} t''_{01}$. Таким образом, учитывая взаимную простоту чисел $t'_{11} t'_{10}$ и $t''_{11} t''_{01}$, получаем, что $(n^{k'} - m')m_0$ делится на $t'_{11} t''_{11} t'_{10} t''_{01}$. Аналогично можно доказать, что $m'm_1$ также делится на $t'_{11} t''_{11} t'_{10} t''_{01}$. Следовательно, заметив, что $t'_{11} t''_{11} t'_{10} t''_{01} = \prod\limits_{t \in \widehat{T}} t$, получаем, что

$$(n^{k'} - m')m_0 + m'm_1 \equiv 0 \pmod{\prod_{t \in \widehat{T}} t}. \tag{10}$$

Рассмотрим также число

$$\begin{aligned} n^{k_0 + k'} - \left((n^{k'} - m')m_0 + m'm_1\right) &= n^{k_0 + k'} - n^{k'}m_0 + m'm_0 - m'm_1 = \\ &= n^{k'}(n^{k_0} - m_0) + m'm_0 - m'n^{k_0} + m'n^{k_0} - m'm_1 = \\ &= n^{k'}(n^{k_0} - m_0) - m'(n^{k_0} - m_0) + m'(n^{k_0} - m_1) = \\ &= (n^{k'} - m')(n^{k_0} - m_0) + m'(n^{k_0} - m_1). \end{aligned}$$

Так как $T \setminus T_0 = T'_{00} \cup T''_{00} \cup T'_{01} \cup T''_{01}$, то $\prod\limits_{t \in T \setminus T_0} t = t'_{00} t''_{00} t'_{01} t''_{01}$, тем самым $m_0 \equiv n^{k_0} \pmod{t'_{00} t''_{00} t'_{01} t''_{01}}$. Следовательно, $n^{k_0} - m_0$ делится на $t'_{00} t'_{01}$. Аналогично можно показать, что $n^{k'} - m'$ делится на $t''_{00} t''_{10}$. Поэтому в силу взаимной простоты чисел $t'_{00} t'_{01}$ и $t''_{00} t''_{10}$ получаем, что $(n^{k'} - m')(n^{k_0} - m_0)$ делится на $t'_{00} t''_{00} t''_{10} t'_{01}$. Аналогичным образом доказывается, что $m'(n^{k_0} - m_1)$, и, следовательно, $n^{k_0 + k'} - \left((n^{k'} - m')m_0 + m'm_1\right)$ также делятся на $t'_{00} t''_{00} t''_{10} t'_{01}$. Таким образом, заметив, что $t'_{00} t''_{00} t''_{10} t'_{01} = \prod\limits_{t \in T \setminus \widehat{T}} t$, имеем

$$(n^{k'} - m')m_0 + m'm_1 \equiv n^{k_0 + k'} \pmod{\prod_{t \in T \setminus \widehat{T}} t}. \tag{11}$$

Учитывая, что $0 < \mu < 1$, из (9), (10) и (11) непосредственно получаем, что $\mu \in G[n]\left(\prod\limits_{t \in \widehat{T}} t : \prod\limits_{t \in T \setminus \widehat{T}} t\right)$, но $G[n]\left(\prod\limits_{t \in \widehat{T}} t : \prod\limits_{t \in T \setminus \widehat{T}} t\right) \subseteq \langle G[n]; T\rangle$, следовательно, $\mu \in \langle G[n]; T\rangle$.

Недостатком нашего определения множеств $\langle G[n]; T\rangle$ является то, что для различных чисел n_1, n_2 и множеств T_1, T_2 множества $\langle G[n_1]; T_1\rangle$, $\langle G[n_2]; T_2\rangle$ могут совпадать. Однако мы можем легко описать, в каких случаях такое совпадение имеет место. Обозначим через $\mathcal{P}[n]$ множество всех простых делителей числа n. Тогда очевидно следующее утверждение.

Утверждение 9. *Пусть $n_1, n_2 \in N$, $n_1, n_2 > 1$ и T — конечное разделимое множество натуральных чисел, взаимно простое с n_1 и n_2. Тогда:*

а) $\langle G[n_1]; T\rangle \subseteq \langle G[n_2]; T\rangle$ *тогда и только тогда, когда* $\mathcal{P}[n_1] \subseteq \mathcal{P}[n_2]$;

б) $\langle G[n_1]; T\rangle = \langle G[n_2]; T\rangle$ *тогда и только тогда, когда* $\mathcal{P}[n_1] = \mathcal{P}[n_2]$.

Для множества натуральных чисел T и натурального k обозначим через T^{-k} множество всех чисел из T, больших k. Заметим, что множество $\langle G[n]; T\rangle$ инвариантно относительно удаления из множества T элементов, равных единице. Поэтому, учитывая соотношение (7), получаем

Утверждение 10. *Для любого натурального n, большего единицы, и любого конечного разделимого множества натуральных чисел T, взаимно простого с n, выполняется*

$$\langle G[n]; T\rangle = \langle G[n]; T^{-1}\rangle.$$

Утверждение 10 может быть усилено следующим образом.

Утверждение 11. *Для любого натурального n, большего единицы, и любого конечного разделимого множества натуральных чисел T, взаимно простого с n, выполняется*

$$\langle G[n]; T\rangle = \langle G[n]; T^{-2}\rangle.$$

Доказательство. В силу утверждения 10 достаточно показать, что, если T содержит число 2, то $\langle G[n]; T\rangle = \langle G[n]; T\setminus\{2\}\rangle$. Пусть m/n^k — произвольная дробь из $\langle G[n]; T\setminus\{2\}\rangle$. Тогда m/n^k принадлежит множеству $G[n]\left(\prod\limits_{t\in E} t:\ \prod\limits_{t\in(T\setminus\{2\})\setminus E} t\right)$, где E — некоторое подмножество множества T. Это означает, что $m\equiv 0 \pmod{\prod\limits_{t\in E} t}$ и $n^k - m \equiv 0 \pmod{\prod\limits_{t\in(T\setminus\{2\})\setminus E} t}$. Если T содержит число 2 и взаимно просто с n, то n нечетно. Поэтому какое-то из чисел m, $n^k - m$ является четным. Пусть m четно. Поскольку T является разделимым, то $T\setminus\{2\}$ взаимно просто с числом 2. Поэтому согласно утверждению 6 число 2 взаимно просто с $\prod\limits_{t\in E} t$. Следовательно, $m\equiv 0 \pmod{\prod\limits_{t\in E\cup\{2\}} t}$. Тем самым

$$m/n^k \in G[n]\left(\prod_{t\in E\cup\{2\}} t:\ \prod_{t\in(T\setminus\{2\})\setminus E} t\right) \subseteq \langle G[n]; T\rangle.$$

В случае, если четным является $n^k - m$, аналогично можно показать, что

$$m/n^k \in G[n]\left(\prod_{t\in E} t:\ \prod_{t\in T\setminus E} t\right) \subseteq \langle G[n]; T\rangle.$$

Таким образом, $\langle G[n]; T\setminus\{2\}\rangle \subseteq \langle G[n]; T\rangle$. С другой стороны, из определения множества $\langle G[n]; T\rangle$ с учетом соотношения (7), очевидно, следует, что для любого подмножества T' множества T выполняется $\langle G[n]; T\rangle \subseteq \langle G[n]; T'\rangle$, поэтому $\langle G[n]; T\rangle \subseteq \langle G[n]; T\setminus\{2\}\rangle$.

Отметим, что в действительности множества $\langle G[n_1]; T_1\rangle$, $\langle G[n_2]; T_2\rangle$ совпадают тогда и только тогда, когда $\mathcal{J}[n_1] = \mathcal{J}[n_2]$ и $T_1^{-2} = T_2^{-2}$. Однако мы опускаем доказательство этого факта, поскольку он нами не используется в дальнейшем.

Замыкания одноэлементных множеств

Для получения нашего основного результата мы предварительно даем полное описание замыканий всех одноэлементных множеств рациональных чисел.

Лемма 4. *Пусть* $\frac{l}{n}$ — *произвольная несократимая дробь из интервала* $(0;1)$. *Тогда для любого* $\varepsilon>0$ *существует такое* $K(\varepsilon)$, $K(\varepsilon)\in N$, *что для любой дроби* $\frac{m}{n^k}$ *из* $G[n](l(n-l):1)$ *такой, что* $k\geqslant K(\varepsilon)$ *и* $\varepsilon\leqslant\frac{m}{n^k}\leqslant 1-\varepsilon$, *существует булева функция* $f(x_1,\ldots,x_k)$ *такая, что* $f(0,\ldots,0)=f(1,\ldots,1)=0$ *и* $\frac{m}{n^k}=\mathscr{P}\left\{f\left(\frac{l}{n},\ldots,\frac{l}{n}\right)\right\}$.

Доказательство. Рассмотрим три случая: $\frac{l}{n}>\frac{1}{2}$, $\frac{l}{n}<\frac{1}{2}$ и $\frac{l}{n}=\frac{1}{2}$.

а) В случае $\frac{l}{n}>\frac{1}{2}$ мы можем непосредственно использовать доказательство леммы 2 из [8], поскольку это доказательство заключается в построении булевой функции, удовлетворяющей условиям нашей леммы.

б) Пусть $\frac{l}{n}<\frac{1}{2}$. Тогда $1-\frac{l}{n}=\frac{n-l}{n}>\frac{1}{2}$, тем самым дробь $\frac{n-l}{n}$ удовлетворяет уже доказанному нами случаю а). Следовательно, для любой дроби $\frac{m}{n^k}$ такой, что $k\geqslant K(\varepsilon)$, $\varepsilon\leqslant\frac{m}{n^k}\leqslant 1-\varepsilon$ и m делится на $(n-l)(n-(n-l))=l(n-l)$, существует булева функция $f(x_1,\ldots,x_k)$ такая, что $f(0,\ldots,0)=f(1,\ldots,1)=0$ и $\frac{m}{n^k}=\mathscr{P}\left\{f\left(\frac{n-l}{n},\ldots,\frac{n-l}{n}\right)\right\}$. Рассмотрев функцию $g(x_1,\ldots,x_k)=f(\overline{x_1},\ldots,\overline{x_k})$, получим, что $g(0,\ldots,0)=g(1,\ldots,1)=0$ и в силу утверждения 1 выполняется равенство

$$\mathscr{P}\left\{g\left(\frac{l}{n},\ldots,\frac{l}{n}\right)\right\}=\mathscr{P}\left\{f\left(\mathscr{P}\left\{f^{\neg}\left(\frac{l}{n}\right)\right\},\ldots,\mathscr{P}\left\{f^{\neg}\left(\frac{l}{n}\right)\right\}\right)\right\}=$$
$$=\mathscr{P}\left\{f\left(\frac{n-l}{n},\ldots,\frac{n-l}{n}\right)\right\}=\frac{m}{n^k}.$$

Таким образом, утверждение леммы справедливо и в этом случае.

в) В случае $\frac{l}{n}=\frac{1}{2}$ для любой булевой функции $f(x_1,\ldots,x_k)$ имеем

$$\mathscr{P}\left\{f\left(\frac{l}{n},\ldots,\frac{l}{n}\right)\right\}=\mathscr{P}\left\{f\left(\frac{1}{2},\ldots,\frac{1}{2}\right)\right\}=\frac{|\mathscr{N}(f)|}{2^k}.$$

Поэтому для доказательства леммы в этом случае нам достаточно предполагать, что $2^{-K(\varepsilon)}<\varepsilon$, и рассмотреть произвольную функцию $f(x_1,\ldots,x_k)$ такую, что $f(0,\ldots,0)=f(1,\ldots,1)=0$ и $|\mathscr{N}(f)|=m$.

Следствие 5. *Для любой несократимой дроби* $\frac{l}{n}$ *из интервала* $(0;1)$ *множество* $G[n](l(n-l):1)$ *содержится в* $\left[\left\{\frac{l}{n}\right\}\right]$.

Доказательство. Заметим, что любая дробь $\frac{m}{n^k}$ из $G[n](l(n-l):1)$ может быть представлена в виде удовлетворяющей условиям леммы 4 дроби $\frac{mn^{K-k}}{n^K}$, где $K=\max(K(\varepsilon),k)$ для $\varepsilon=\min\left(\frac{m}{n^k},1-\frac{m}{n^k}\right)$. Поэтому согласно лемме 4 найдется булева функция $f(x_1,\ldots,x_K)$ такая, что $\frac{m}{n^k}=$ $=\mathscr{P}\left\{f\left(\frac{l}{n},\ldots,\frac{l}{n}\right)\right\}$.

Из утверждения 8 и следствий 5 и 2 непосредственно вытекает

Следствие 6. *Для любой несократимой дроби* $\frac{l}{n}$ *из интервала* $(0; 1)$ *множество* $G[n](1: l(n-l))$ *содержится в* $\left[\left\{\frac{l}{n}\right\}\right]$.

Лемма 5. *Пусть* $\frac{l}{n}$ *— произвольная несократимая дробь из интервала* $(0; 1)$. *Тогда для любого* $\varepsilon > 0$ *существует такое* $K(\varepsilon)$, $K(\varepsilon) \in N$, *что для любой дроби* $\frac{m}{n^k}$ *из* $G[n](l: n-l)$ *такой, что* $k \geqslant K(\varepsilon)$ *и* $\varepsilon \leqslant \frac{m}{n^k} \leqslant 1-\varepsilon$, *существует булева функция* $f(x_1, \ldots, x_k)$ *такая, что* $\frac{m}{n^k} = \mathscr{P}\left\{f\left(\frac{l}{n}, \ldots, \frac{l}{n}\right)\right\}$.

Доказательство. Согласно лемме 4 для любого $\varepsilon > 0$ мы можем подобрать такое K', что для любой дроби m/n^k из $G[n](l(n-l): 1)$ такой, что $k \geqslant K'$ и $\varepsilon/2 \leqslant m/n^k \leqslant 1-\varepsilon/2$, найдется булева функция $f(x_1, \ldots, x_k)$ такая, что $f(0, \ldots, 0) = f(1, \ldots, 1) = 0$ и $m/n^k = \mathscr{P}\{f(l/n, \ldots, l/n)\}$. Выберем $K(\varepsilon)$ таким, чтобы $K(\varepsilon) \geqslant K'$ и $(l/n)^{K(\varepsilon)} < \varepsilon/2$. Пусть m/n^k — произвольная дробь из $G[n](l: n-l)$, удовлетворяющая условиям леммы. Рассмотрим дробь $m'/n^k = m/n^k - l^k/n^k = (m-l^k)/n^k$. С другой стороны, поскольку $m \equiv n^k \pmod{n-l}$ и $l^k \equiv n^k \pmod{n-l}$, то $m' = m - l^k \equiv 0 \pmod{n-l}$. В силу несократимости дроби l/n выполняется равенство $(l, n-l) = 1$, поэтому $m' \equiv 0 \pmod{l(n-l)}$. Так как $0 < (l/n)^k \leqslant (l/n)^{K(\varepsilon)} < \varepsilon/2$ и $\varepsilon \leqslant m/n^k \leqslant 1-\varepsilon$, то $\varepsilon/2 \leqslant m'/n^k \leqslant 1-\varepsilon$. Таким образом, получаем, что $m'/n^k \in G[n](l(n-l): 1)$, $\varepsilon/2 \leqslant m'/n^k \leqslant 1-\varepsilon/2$ и $k \geqslant K(\varepsilon) \geqslant K'$. Следовательно, найдется булева функция $f(x_1, \ldots, x_k)$ такая, что $f(0, \ldots, 0) = f(1, \ldots, 1) = 0$ и $m'/n^k = \mathscr{P}\{f(l/n, \ldots, l/n)\}$. Возьмем функцию $g(x_1, \ldots, x_k) = f(x_1, \ldots, x_k) \vee x_1 \& \ldots \& x_k$. Поскольку $f(1, \ldots, 1) = 0$, то

$$\mathscr{P}\left\{g\left(\frac{l}{n}, \ldots, \frac{l}{n}\right)\right\} = \mathscr{P}\left\{f\left(\frac{l}{n}, \ldots, \frac{l}{n}\right)\right\} + \left(\frac{l}{n}\right)_1 \cdots \left(\frac{l}{n}\right)_1 = \frac{m'}{n^k} + \left(\frac{l}{n}\right)^k = \frac{m}{n^k}.$$

Следствие 7. *Для любой несократимой дроби* $\frac{l}{n}$ *из интервала* $(0; 1)$ *множество* $G[n](l: n-l)$ *содержится в* $\left[\left\{\frac{l}{n}\right\}\right]$.

Доказательство аналогично доказательству следствия 5 из леммы 2.

Из утверждения 8 и следствий 7 и 2 непосредственно вытекает

Следствие 8. *Для любой несократимой дроби* $\frac{l}{n}$ *из интервала* $(0; 1)$ *множество* $G[n](n-l: l)$ *содержится в* $\left[\left\{\frac{l}{n}\right\}\right]$.

Лемма 6. *Для любой несократимой дроби* $\frac{l}{n}$ *из интервала* $(0; 1)$ *выполняется соотношение*

$$\left[\left\{\frac{l}{n}\right\}\right] = \langle G[n]; \{l, n-l\}\rangle.$$

Доказательство. Отметим, что, поскольку дробь l/n несократима, то $(l, n-l) = (l, n) = (n-l, n) = 1$ и, следовательно, множество $\langle G[n]; \{l, n-l\}\rangle$ корректно определено. Так как $\langle G[n]; \{l, n-l\}\rangle = G[n](l(n-l): 1) \cup G[n](1: l(n-l)) \cup G[n](l: n-l) \cup G[n](n-l: l)$, то соотношение $\langle G[n]; \{l, n-l\}\rangle \subseteq [\{l/n\}]$ получается непосредственным суммированием следствий 5, 6, 7 и 8. С другой стороны, множество $\langle G[n]; \{l, n-l\}\rangle$ содержит дробь l/n и согласно лемме 3 является замкнутым, поэтому $[\{l/n\}] \subseteq [\langle G[n]; \{l, n-l\}\rangle] = \langle G[n]; \{l, n-l\}\rangle$.

Основная лемма

Главным вспомогательным утверждением для доказательства наших результатов является

Лемма 7. *Пусть n_1, n_2 — натуральные числа, большие единицы, A — конечное разделимое множество натуральных чисел, взаимно простое с n_1, B — двухэлементное разделимое множество натуральных чисел, взаимно простое с n_2, M — замкнутое множество чисел, содержащее множества $\langle G[n_1]; (A, \{\|B\|\})\rangle$ и $\langle G[n_2]; (\{\|A\|\}, B)\rangle$. Тогда $\langle G[n_1]; (A, B)\rangle \subseteq M$.*

Доказательство. Согласно утверждениям 3 и 4 множества $(A, \{\|B\|\})$, $(\{\|A\|\}, B)$, (A, B) являются разделимыми и взаимно простыми с n_1 и n_2, поэтому множества $\langle G[n_1]; (A, \{\|B\|\})\rangle$, $\langle G[n_2]; (\{\|A\|\}, B)\rangle$ и $\langle G[n_1]; (A, B)\rangle$ являются корректно определенными. Пусть $B = \{b_1, b_2\}$. Рассмотрим произвольную дробь m/n из $\langle G[n_1]; (A, B)\rangle$. Обозначим через E подмножество множества (A, B) такое, что $m/n \in$ $\in G[n_1]\left(\prod\limits_{t\in E} t: \prod\limits_{t\in (A,B)\setminus E} t\right)$. Положим $l' = \prod\limits_{t\in E} t$, $l'' = \prod\limits_{t\in (A,B)\setminus E} t$. Разобьем множество A на подмножества

$$A_{00} = \{\, a \mid a\in A,\ (a, b_1)\notin E,\ (a, b_2)\notin E \,\},$$
$$A_{01} = \{\, a \mid a\in A,\ (a, b_1)\notin E,\ (a, b_2)\in E \,\},$$
$$A_{10} = \{\, a \mid a\in A,\ (a, b_1)\in E,\ (a, b_2)\notin E \,\},$$
$$A_{11} = \{\, a \mid a\in A,\ (a, b_1)\in E,\ (a, b_2)\in E \,\}.$$

Для $i, j = 0, 1$, $\sigma = 1, 2$ положим $l_{ij}^{(\sigma)} = \prod\limits_{a\in A_{ij}} (a, b_\sigma)$, $l_{ij} = l_{ij}^{(1)} l_{ij}^{(2)}$ и $l^{(\sigma)} =$ $= \prod\limits_{i=0}^{1}\prod\limits_{j=0}^{1} l_{ij}^{(\sigma)}$. Очевидно, что $l' = l_{11}^{(1)} l_{11}^{(2)} l_{10}^{(1)} l_{01}^{(2)} = l_{11} l_{10}^{(1)} l_{01}^{(2)}$ и $l'' = l_{00}^{(1)} l_{00}^{(2)} l_{01}^{(1)} l_{10}^{(2)} =$ $= l_{00} l_{01}^{(1)} l_{10}^{(2)}$. Так как множество чисел $l_{ij}^{(\sigma)}$ является мультипликативным разбиением разделимого и взаимно простого с числами n_1 и n_2 множества (A, B), то согласно утверждениям 5 и 6 все эти числа попарно просты и взаимо просты с n_1 и n_2. Аналогично имеем, что все числа l_{ij} являются попарно простыми и взаимо простыми с n_1 и n_2. Поскольку $(b_1, b_2) = 1$, то

$$l_{ij} = \prod_{a\in A_{ij}} (a, b_1) \prod_{a\in A_{ij}} (a, b_2) = \prod_{a\in A_{ij}} (a, b_1)(a, b_2) =$$
$$= \prod_{a\in A_{ij}} (a, b_1 b_2) = \prod_{a\in A_{ij}} (a, \|B\|) = \prod_{t\in (A_{ij}, \{\|B\|\})} t, \quad i, j = 0, 1. \quad (12)$$

Так как $A = A_{00}\cup A_{01}\cup A_{10}\cup A_{11}$ и все числа из A попарно просты, то

$$l^{(\sigma)} = \prod_{a\in A_{00}} (a, b_\sigma) \prod_{a\in A_{01}} (a, b_\sigma) \prod_{a\in A_{10}} (a, b_\sigma) \prod_{a\in A_{11}} (a, b_\sigma) =$$
$$= \prod_{a\in A} (a, b_\sigma) = (\|A\|, b_\sigma), \quad \sigma = 1, 2. \quad (13)$$

Отметим, что $\|(A, B)\| = l^{(1)} l^{(2)} = l_{00} l_{01} l_{10} l_{11}$. Обозначим через E_1 множество $(A_{11}\cup A_{10}, \{\|B\|\})$ и через E_2 множество $(A_{11}\cup A_{01}, \{\|B\|\})$.

Если $l_{01} l_{10} = 1$, т. е. $l_{01}^{(1)} = l_{01}^{(2)} = l_{10}^{(1)} = l_{10}^{(2)} = 1$, то $l' = l_{11}$ и $l'' = l_{01} l_{10} l_{00}$, поэтому согласно соотношениям (12) имеем

$$l' = \prod_{t\in (A_{11}, \{\|B\|\})} t,$$
$$l'' = \prod_{t\in (A_{01}, \{\|B\|\})\cup (A_{10}, \{\|B\|\})\cup (A_{00}, \{\|B\|\})} t = \prod_{t\in (A, \{\|B\|\})\setminus (A_{11}, \{\|B\|\})} t.$$

Таким образом, мы в этом случае получаем, что $G[n_1](l'\colon l'') \subseteq \subseteq \langle G[n_1]; (A, \{\|B\|\})\rangle$ и, следовательно, согласно условиям леммы, $m/n \in \in M$. Пусть $l_{01}l_{10} > 1$. Положим $\widehat{n}_2 = n_2^{\varphi(l_{01}l_{10})}$. Так как $(n_2, l_{01}) = (n_2, l_{10}) = 1$, то $(n_2, l_{01}l_{10}) = 1$, поэтому согласно теореме Эйлера $\widehat{n}_2 \equiv 1 \pmod{l_{01}l_{10}}$. Выберем натуральное k_2 такое, что $\widehat{n}_2^{k_2} > 3\|(A, B)\|$. Домножив числитель и знаменатель дроби m/n на подходящий коэффициент, представим ее в виде $\widehat{m}/n_1^{k_1}$, где $\widehat{m}, k_1 \in N$ и $\min(\widehat{m}, n_1^{k_1} - \widehat{m}) > \|(A, B)\|\widehat{n}_2^{k_2}$.

Рассмотрим систему сравнений

$$\begin{cases} x \equiv n_1^{k_1} \pmod{l_{10}}, \\ x \equiv -n_1^{k_1} \pmod{l_{01}}. \end{cases} \tag{14}$$

Так как $(l_{10}, l_{01}) = 1$, то согласно лемме 2 данная система имеет решение, являющееся классом вычетов по модулю $l_{01}l_{10}$:

$$x \equiv \alpha \pmod{l_{01}l_{10}}.$$

Рассмотрим сравнение

$$l_{00}l_{11}x \equiv \alpha \pmod{l_{01}l_{10}}. \tag{15}$$

Поскольку числа $l_{00}, l_{11}, l_{01}, l_{10}$ попарно просты, то $(l_{00}l_{11}, l_{01}l_{10}) = 1$. Поэтому согласно лемме 1 данное сравнение имеет решением некоторый класс вычетов по модулю $l_{01}l_{10}$. Пусть β — наименьший положительный вычет из этого класса. Положим $\gamma = \beta l_{00}l_{11}$. Так как $\alpha \equiv n_1^{k_1} \pmod{l_{10}}$, $\alpha \equiv -n_1^{k_1} \pmod{l_{01}}$ и $(n_1, l_{10}) = (n_1, l_{01}) = 1$, то $(\alpha, l_{10}) = (\alpha, l_{01}) = 1$, тем самым $(\alpha, l_{10}l_{01}) = 1$. Тогда, поскольку $\gamma \equiv \alpha \pmod{l_{10}l_{01}}$, то $(\gamma, l_{10}l_{01}) = 1$. Следовательно, $(\beta, l_{10}l_{01}) = 1$.

Рассмотрим сравнения

$$(\gamma l^{(1)})x \equiv \widehat{m} \pmod{l_{11}l_{10}}, \tag{16}$$

$$(\gamma l^{(1)})x \equiv \widehat{m} - n_1^{k_1} \pmod{l_{00}l_{01}}. \tag{17}$$

Так как числа $l_{00}^{(1)}, l_{01}^{(1)}, l_{11}^{(1)}, l_{00}^{(2)}$ взаимно просты с числом $l_{10}^{(2)}$, то произведение этих чисел $l_{00}l_{00}^{(1)}l_{01}^{(1)}l_{11}^{(1)}$ также взаимно просто с $l_{10}^{(2)}$. Кроме того, поскольку число $l_{10}^{(2)}$ является делителем числа $l_{10}l_{01}$, взаимно простого с числом β, то $l_{10}^{(2)}$ также взаимно просто с β. Таким образом, получаем, что число $l_{10}^{(2)}$ взаимно просто с произведением чисел β и $l_{00}l_{00}^{(1)}l_{01}^{(1)}l_{11}^{(1)}$:

$$(\beta l_{00}l_{00}^{(1)}l_{01}^{(1)}l_{11}^{(1)}, l_{10}^{(2)}) = 1. \tag{18}$$

Следовательно,

$$(\gamma l^{(1)}, l_{11}l_{10}) = (\beta l_{00}l_{11}l_{00}^{(1)}l_{01}^{(1)}l_{10}^{(1)}l_{11}^{(1)}, l_{11}l_{10}^{(1)}l_{10}^{(2)}) = l_{11}l_{10}^{(1)}(\beta l_{00}l_{00}^{(1)}l_{01}^{(1)}l_{11}^{(1)}, l_{10}^{(2)}) = l_{11}l_{10}^{(1)}.$$

Аналогично (18) можно доказать, что $(\beta l_{11}l_{00}^{(1)}l_{10}^{(1)}l_{11}^{(1)}, l_{01}^{(2)}) = 1$. Поэтому

$$(\gamma l^{(1)}, l_{00}l_{01}) = (\beta l_{00}l_{11}l_{00}^{(1)}l_{01}^{(1)}l_{10}^{(1)}l_{11}^{(1)}, l_{00}l_{01}^{(1)}l_{01}^{(2)}) = l_{00}l_{01}^{(1)}(\beta l_{11}l_{00}^{(1)}l_{10}^{(1)}l_{11}^{(1)}, l_{01}^{(2)}) = l_{00}l_{01}^{(1)}.$$

Так как $\widehat{m}/n_1^{k_1} \in G[n_1](l'\colon l'')$, то $\widehat{m}$ делится на $l' = l_{11}l_{10}^{(1)}l_{01}^{(2)}$. Следовательно, $\widehat{m}$ делится на $l_{11}l_{10}^{(1)} = (\gamma l^{(1)}, l_{11}l_{10})$. Поэтому согласно лемме 1 сравнение (16) имеет решение, являющееся классом вычетов по модулю $l_{11}l_{10}/l_{11}l_{10}^{(1)} = l_{10}^{(2)}$:

$$x \equiv \alpha_1 \pmod{l_{10}^{(2)}}. \tag{19}$$

Из $\widehat{m}/n_1^{k_1} \in G[n_1](l'\colon l'')$ также следует, что $\widehat{m} - n_1^{k_1}$ делится на $l'' = l_{00}l_{01}^{(1)}l_{10}^{(2)}$. Следовательно, $\widehat{m} - n_1^{k_1}$ делится на $l_{00}l_{01}^{(1)} = (\gamma l^{(1)}, l_{00}l_{01})$. Поэтому согласно лемме 1 сравнение (17) имеет решение, являющееся классом вычетов по модулю $l_{11}l_{01}/l_{11}l_{10}^{(1)} = l_{01}^{(2)}$:

$$x \equiv \beta_1 \pmod{l_{01}^{(2)}}. \tag{20}$$

Таким образом, система сравнений (16) и (17) сводится к системе сравнений (19) и (20). Так как $(l_{10}^{(2)}, l_{01}^{(2)}) = 1$, то согласно лемме 2 система сравнений (19) и (20) имеет решение, являющееся классом вычетов по модулю $l_{10}^{(2)}l_{01}^{(2)}$. Обозначим через γ_1 наименьший положительный вычет из данного класса.

Рассмотрим также сравнения

$$(\gamma l^{(2)})x \equiv -\widehat{m} \pmod{l_{11}l_{01}}, \tag{21}$$

$$(\gamma l^{(2)})x \equiv n_1^{k_1} - \widehat{m} \pmod{l_{00}l_{10}}. \tag{22}$$

Аналогично соотношению (18) можно показать, что $(\beta l_{00}l_{00}^{(2)}l_{10}^{(2)}l_{11}^{(2)}, l_{01}^{(1)}) = 1$ и $(\beta l_{11}l_{00}^{(2)}l_{01}^{(2)}l_{11}^{(2)}, l_{10}^{(1)}) = 1$. Поэтому

$$(\gamma l^{(2)}, l_{11}l_{01}) = (\beta l_{00}l_{11}l_{00}^{(2)}l_{01}^{(2)}l_{10}^{(2)}l_{11}^{(2)}, l_{11}l_{01}^{(1)}l_{01}^{(2)}) = l_{11}l_{01}^{(2)}(\beta l_{00}l_{00}^{(2)}l_{10}^{(2)}l_{11}^{(2)}, l_{01}^{(1)}) = l_{11}l_{01}^{(2)},$$
$$(\gamma l^{(2)}, l_{00}l_{10}) = (\beta l_{00}l_{11}l_{00}^{(2)}l_{01}^{(2)}l_{10}^{(2)}l_{11}^{(2)}, l_{00}l_{10}^{(1)}l_{10}^{(2)}) = l_{00}l_{10}^{(2)}(\beta l_{11}l_{00}^{(2)}l_{01}^{(2)}l_{11}^{(2)}, l_{10}^{(1)}) = l_{00}l_{10}^{(2)}.$$

Так как $\widehat{m}$ делится на $l' = l_{11}l_{10}^{(1)}l_{01}^{(2)}$, то $\widehat{m}$ делится на $l_{11}l_{01}^{(2)} = (\gamma l^{(2)}, l_{11}l_{01})$. Поэтому согласно лемме 1 сравнение (21) имеет решение, являющееся классом вычетов по модулю $l_{11}l_{01}/l_{11}l_{01}^{(2)} = l_{01}^{(1)}$:

$$x \equiv \alpha_2 \pmod{l_{01}^{(1)}}. \tag{23}$$

Мы также имеем, что $n_1^{k_1} - \widehat{m}$ делится на $l'' = l_{00}l_{01}^{(1)}l_{10}^{(2)}$, тем самым $n_1^{k_1} - \widehat{m}$ делится на $l_{00}l_{10}^{(2)} = (\gamma l^{(2)}, l_{00}l_{10})$. Поэтому согласно лемме 1 получаем, что сравнение (22) имеет решение, являющееся классом вычетов по модулю $l_{00}l_{10}/l_{00}l_{10}^{(2)} = l_{10}^{(1)}$:

$$x \equiv \beta_2 \pmod{l_{10}^{(1)}}. \tag{24}$$

Таким образом, система сравнений (21) и (22) сводится к системе сравнений (23) и (24). Поскольку $(l_{01}^{(1)}, l_{10}^{(1)}) = 1$, то согласно лемме 2 система сравнений (23) и (24) имеет решение, являющееся классом вычетов по модулю $l_{01}^{(1)}l_{10}^{(1)}$. Обозначим через γ_2 наименьший положительный вычет из данного класса.

Положим $\delta = \gamma_1 l^{(1)} + \gamma_2 l^{(2)}$. Так как γ_1 удовлетворяет сравнениям (19) и (20) и γ_2 удовлетворяет сравнениям (23) и (24), то γ_1 удовлетворяет сравнениям (16) и (17) и γ_2 удовлетворяет сравнениям (21) и (22). Следовательно,

$$\gamma l^{(1)}\gamma_1 \equiv \widehat{m} \pmod{l_{10}}, \tag{25}$$

$$\gamma l^{(1)}\gamma_1 \equiv \widehat{m} - n_1^{k_1} \pmod{l_{01}}, \tag{26}$$

$$\gamma l^{(2)}\gamma_2 \equiv -\widehat{m} \pmod{l_{01}}, \tag{27}$$

$$\gamma l^{(2)}\gamma_2 \equiv n_1^{k_1} - \widehat{m} \pmod{l_{10}}. \tag{28}$$

Почленно складывая сравнение (25) со сравнением (28) и сравнение (26) со сравнением (27), получим

$$\gamma l^{(1)}\gamma_1 + \gamma l^{(2)}\gamma_2 = \gamma\delta \equiv n_1^{k_1} \pmod{l_{10}},$$
$$\gamma l^{(1)}\gamma_1 + \gamma l^{(2)}\gamma_2 = \gamma\delta \equiv -n_1^{k_1} \pmod{l_{01}}.$$

Таким образом, $\gamma\delta$ удовлетворяет системе (14). Тогда $\gamma\delta \equiv \alpha \pmod{l_{01}l_{10}}$. Поскольку $\gamma \equiv \alpha \pmod{l_{01}l_{10}}$, то $\gamma\delta \equiv \gamma \pmod{l_{01}l_{10}}$. В силу равенства $(\gamma, l_{01}l_{10}) = 1$, мы можем поделить обе части последнего сравнения на γ, получив, что $\delta \equiv 1 \pmod{l_{01}l_{10}}$. Так как $\widehat{n}_2 \equiv 1 \pmod{l_{01}l_{10}}$, то $\widehat{n}_2^{k_2} \equiv 1 \pmod{l_{01}l_{10}}$. Поэтому из сравнения $\delta \equiv 1 \pmod{l_{01}l_{10}}$ следует, что $\delta \equiv \widehat{n}_2^{k_2} \pmod{l_{01}l_{10}}$. Таким образом, $\widehat{n}_2^{k_2} - \delta$ делится на $l_{01}l_{10}$. Обозначим целое число $(\widehat{n}_2^{k_2} - \delta)/l_{01}l_{10}$ через τ. Так как $\gamma_1 \leqslant l_{10}^{(2)}l_{01}^{(2)} \leqslant l^{(2)}$, то $\gamma_1 l^{(1)} \leqslant l^{(2)}l^{(1)} = \|(A, B)\|$. Аналогично $\gamma_2 l^{(2)} \leqslant \|(A, B)\|$. Таким образом, $\delta \leqslant 2\|(A, B)\|$. Следовательно, поскольку $\widehat{n}_2^{k_2} > 3\|(A, B)\|$, то $\widehat{n}_2^{k_2} - \delta > \|(A, B)\|$. Поэтому $\tau > \|(A, B)\|/l_{01}l_{10} = l_{00}l_{11}$. Так как числа $l_{00}^{(1)}, l_{11}^{(1)}, l_{00}^{(2)}, l_{11}^{(2)}$ попарно просты, то $(l_{00}^{(1)}l_{11}^{(1)}, l_{00}^{(2)}l_{11}^{(2)}) = 1$. Поэтому согласно следствию 4 найдутся целые ξ_1, ξ_2 такие, что $\tau = \xi_1 l_{00}^{(1)}l_{11}^{(1)} + \xi_2 l_{00}^{(2)}l_{11}^{(2)}$, при этом, очевидно, число ξ_1 может быть выбрано из множества $\{1, \ldots, l_{00}^{(2)}l_{11}^{(2)}\}$. В таком случае $\xi_1 l_{00}^{(1)}l_{11}^{(1)} \leqslant l_{00}^{(2)}l_{11}^{(2)}l_{00}^{(1)}l_{11}^{(1)} = l_{00}l_{11} < \tau$, следовательно, $\xi_2 l_{00}^{(2)}l_{11}^{(2)} > 0$, тем самым $\xi_2 > 0$.

Положим $c = \gamma_1 + \xi_1 l_{01}^{(2)}l_{10}^{(2)}$. Рассмотрим дробь $cl^{(1)}/\widehat{n}_2^{k_2}$. Очевидно, что $cl^{(1)} > 0$. Заметим также, что

$$l_{01}^{(2)}l_{10}^{(2)}l^{(1)} = l_{01}^{(2)}l_{10}^{(2)}l_{00}^{(1)}l_{01}^{(1)}l_{10}^{(1)}l_{11}^{(1)} = l_{01}l_{10}l_{00}^{(1)}l_{11}^{(1)}. \tag{29}$$

Аналогично имеем $l_{01}^{(1)}l_{10}^{(1)}l^{(2)} = l_{01}l_{10}l_{00}^{(2)}l_{11}^{(2)}$. Поэтому

$$\begin{aligned}\widehat{n}_2^{k_2} - cl^{(1)} &= \widehat{n}_2^{k_2} - \gamma_1 l^{(1)} - \xi_1 l_{01}^{(2)}l_{10}^{(2)}l^{(1)} = \\ &= \delta + \tau l_{01}l_{10} - \gamma_1 l^{(1)} - \xi_1 l_{01}l_{10}l_{00}^{(1)}l_{11}^{(1)} = \gamma_2 l^{(2)} + (\tau - \xi_1 l_{00}^{(1)}l_{11}^{(1)})l_{01}l_{10} = \\ &= \gamma_2 l^{(2)} + \xi_2 l_{00}^{(2)}l_{11}^{(2)}l_{01}l_{10} = \gamma_2 l^{(2)} + \xi_2 l_{01}^{(1)}l_{10}^{(1)}l^{(2)} = (\gamma_2 + \xi_2 l_{01}^{(1)}l_{10}^{(1)})l^{(2)} > 0.\end{aligned}$$

Таким образом, $cl^{(1)}/\widehat{n}_2^{k_2} \in G[n_2](l^{(1)}: l^{(2)})$. Из (13) получаем, что

$$G[n_2](l^{(1)}: l^{(2)}) = G[n_2]((\|A\|, b_1): (\|A\|, b_2)) \subseteq \langle G[n_2]; (\{\|A\|\}, B)\rangle.$$

Поэтому согласно условиям леммы $cl^{(1)}/\widehat{n}_2^{k_2} \in M$.

Положим $m_1 = \widehat{m} - \gamma cl^{(1)}$. Так как $\beta \leqslant l_{01}l_{10}$, то $\gamma = \beta l_{00}l_{11} \leqslant l_{01}l_{10}l_{00}l_{11} = \|(A, B)\|$. Тогда, поскольку $cl^{(1)} < \widehat{n}_2^{k_2}$, то $\gamma cl^{(1)} < \|(A, B)\|\widehat{n}_2^{k_2} < \widehat{m}$. Следовательно, $\widehat{m} > m_1 > 0$. Таким образом, $m_1/n_1^{k_1} \in G[n_1]$. Обозначим через m_1^* число $\widehat{m} - \gamma\xi_1 l_{01}^{(2)}l_{10}^{(2)}l^{(1)}$. Используя равенство (29), имеем $m_1^* = \widehat{m} - \gamma\xi_1 l_{01}l_{10}l_{00}^{(1)}l_{11}^{(1)} \equiv \widehat{m} \pmod{l_{01}l_{10}}$. Следовательно, $m_1 = m_1^* - \gamma\gamma_1 l^{(1)} \equiv \widehat{m} - \gamma\gamma_1 l^{(1)} \pmod{l_{01}l_{10}}$, т. е.

$$m_1 \equiv \widehat{m} - \gamma\gamma_1 l^{(1)} \pmod{l_{10}}, \tag{30}$$

$$m_1 \equiv \widehat{m} - \gamma\gamma_1 l^{(1)} \pmod{l_{01}}. \tag{31}$$

Сопоставляя соотношение (30) со сравнением (25), получаем, что

$$m_1 \equiv 0 \pmod{l_{10}}. \tag{32}$$

Аналогично сопоставляя сравнения (31) и (26), имеем

$$m_1 \equiv n_1^{k_1} \pmod{l_{01}}. \tag{33}$$

Поскольку $m_1 \equiv \widehat{m} \pmod{\gamma}$ и γ делится на $l_{00}l_{11}$, то $m_1 \equiv \widehat{m} \pmod{l_{00}l_{11}}$. Поэтому из $\widehat{m} \equiv 0 \pmod{l_{11}}$ и $\widehat{m} \equiv n_1^{k_1} \pmod{l_{00}}$ следует, что

$$m_1 \equiv 0 \pmod{l_{11}}, \tag{34}$$

$$m_1 \equiv n_1^{k_1} \pmod{l_{00}}. \tag{35}$$

Так как $(l_{10}, l_{11}) = (l_{01}, l_{00}) = 1$, то из сравнений (32), (34) и сравнений (33), (35) соответственно вытекает, что

$$m_1 \equiv 0 \pmod{l_{10}l_{11}}, \quad m_1 \equiv n_1^{k_1} \pmod{l_{01}l_{00}}.$$

Таким образом, $m_1/n_1^{k_1} \in G[n_1](l_{10}l_{11}: l_{01}l_{00})$. Из соотношений (12) получаем, что

$$l_{10}l_{11} = \prod_{t \in (A_{11}, \{\|B\|\}) \cup (A_{10}, \{\|B\|\})} t = \prod_{t \in E_1} t,$$

$$l_{01}l_{00} = \prod_{t \in (A_{01}, \{\|B\|\}) \cup (A_{00}, \{\|B\|\})} t = \prod_{t \in (A, \{\|B\|\}) \setminus E_1} t.$$

Поэтому $G[n_1](l_{10}l_{11}: l_{01}l_{00}) \subseteq \langle G[n_1]; (A, \{\|B\|\})\rangle$. Следовательно, согласно условиям леммы, $m_1/n_1^{k_1} \in M$.

Положим $m_2 = m_1 + \gamma \widehat{n}_2^{k_2}$. Так как $\gamma \leqslant \|(A, B)\|$ и $\widehat{m} > m_1$, то

$$\gamma \widehat{n}_2^{k_2} \leqslant \|(A, B)\| \widehat{n}_2^{k_2} < n_1^{k_1} - \widehat{m} < n_1^{k_1} - m_1,$$

тем самым $m_1 < m_2 < n_1^{k_1}$. Таким образом, $m_2/n_1^{k_1} \in G[n_1]$. Поскольку верно сравнение $\widehat{n}_2^{k_2} \equiv 1 \pmod{l_{01}l_{10}}$, то $m_2 \equiv m_1 + \gamma \pmod{l_{01}l_{10}}$, т. е.

$$m_2 \equiv m_1 + \gamma \pmod{l_{10}}, \quad m_2 \equiv m_1 + \gamma \pmod{l_{01}}. \tag{36}$$

Так как $\gamma \equiv \alpha \pmod{l_{01}l_{10}}$, то γ удовлетворяет системе (14). Поэтому

$$\gamma \equiv n_1^{k_1} \pmod{l_{10}}, \tag{37}$$

$$\gamma \equiv -n_1^{k_1} \pmod{l_{01}}. \tag{38}$$

Почленно складывая сравнения (32) и (33) со сравнениями (37) и (38) соответственно, получаем, что

$$m_1 + \gamma \equiv n_1^{k_1} \pmod{l_{10}}, \quad m_1 + \gamma \equiv 0 \pmod{l_{01}}.$$

Сопоставляя эти соотношения со сравнениями (36), имеем

$$m_2 \equiv n_1^{k_1} \pmod{l_{10}}, \tag{39}$$

$$m_2 \equiv 0 \pmod{l_{01}}. \tag{40}$$

Так как $m_2 \equiv m_1 \pmod{\gamma}$ и γ делится на $l_{00}l_{11}$, то $m_2 \equiv m_1 \pmod{l_{00}l_{11}}$. Поэтому из соотношений (34) и (35) соответственно следует, что

$$m_2 \equiv 0 \pmod{l_{11}}, \tag{41}$$

$$m_2 \equiv n_1^{k_1} \pmod{l_{00}}. \tag{42}$$

Поскольку $(l_{01}, l_{11}) = (l_{10}, l_{00}) = 1$, то из сравнений (40), (41) и сравнений (39), (42) соответственно вытекает, что

$$m_2 \equiv 0 \pmod{l_{01}l_{11}}, \quad m_2 \equiv n_1^{k_1} \pmod{l_{10}l_{00}}.$$

Таким образом, $m_2/n_1^{k_1} \in G[n_1](l_{01}l_{11}: l_{10}l_{00})$. Из (12) получаем, что

$$l_{01}l_{11} = \prod_{t \in (A_{01}, \{\|B\|\}) \cup (A_{11}, \{\|B\|\})} t = \prod_{t \in E_2} t,$$

$$l_{10}l_{00} = \prod_{t \in (A_{10}, \{\|B\|\}) \cup (A_{00}, \{\|B\|\})} t = \prod_{t \in (A, \{\|B\|\}) \setminus E_2} t.$$

Следовательно, $G[n_1](l_{01}l_{11}\colon l_{10}l_{00}) \subseteq \langle G[n_1]; (A, \{\|B\|\})\rangle$. Поэтому согласно условиям леммы, $m_2/n_1^{k_1} \in M$.

Согласно соотношению (2) для функции $f_*(x, y, z)$ имеем

$$\mathscr{P}\left\{f_*\left(\frac{m_1}{n_1^{k_1}}, \frac{m_2}{n_1^{k_1}}, \frac{cl^{(1)}}{\widehat{n}_2^{k_2}}\right)\right\} = \frac{m_1}{n_1^{k_1}} \cdot \left(1 - \frac{cl^{(1)}}{\widehat{n}_2^{k_2}}\right) + \frac{m_2}{n_1^{k_1}} \cdot \frac{cl^{(1)}}{\widehat{n}_2^{k_2}} =$$

$$= \frac{m_1(\widehat{n}_2^{k_2} - cl^{(1)}) + m_2 cl^{(1)}}{n_1^{k_1}\widehat{n}_2^{k_2}} = \frac{m_1\widehat{n}_2^{k_2} + (m_2 - m_1)cl^{(1)}}{n_1^{k_1}\widehat{n}_2^{k_2}} =$$

$$= \frac{m_1\widehat{n}_2^{k_2} + \gamma\widehat{n}_2^{k_2}cl^{(1)}}{n_1^{k_1}\widehat{n}_2^{k_2}} = \frac{m_1 + \gamma cl^{(1)}}{n_1^{k_1}} = \frac{\widehat{m}}{n_1^{k_1}}.$$

Таким образом, поскольку $m_1/n_1^{k_1}, m_2/n_1^{k_1}, cl^{(1)}/\widehat{n}_2^{k_2} \in M$ и M замкнуто, то $m/n = \widehat{m}/n_1^{k_1} \in M$.

Основной результат для множеств из $G[p]$, где p — простое

Основной целью данного исследования является описание замыканий конечных множеств рациональных чисел из интервала (0; 1). Поскольку любое рациональное число однозначно выражается некоторой несократимой дробью, без ограничения общности мы можем рассматривать только замыкания конечных множеств несократимых дробей из интервала (0; 1).

Пусть $H = \left\{\frac{m_1}{n_1}, \ldots, \frac{m_s}{n_s}\right\}$ — произвольное конечное множество несократимых дробей из интервала (0; 1). Положим

$$T[H] = \begin{cases} (\{m_1, n_1 - m_1\}, \ldots, \{m_s, n_s - m_s\}), & \text{если } s \geqslant 2; \\ \{m_1, n_1 - m_1\}, & \text{если } s = 1. \end{cases}$$

В силу несократимости дробей множества H для любого i, $i = 1, \ldots, s$, имеем $(m_i, n_i) = (n_i - m_i, n_i) = (m_i, n_i - m_i) = 1$. Поэтому для любого i, $i = 1, \ldots, s$, множество $\{m_i, n_i - m_i\}$ является разделимым и взаимно простым с n_i. Следовательно, согласно утверждениям 3 и 4 множество $T[H]$ обладает следующими свойствами.

Утверждение 12. *Для любого множества* $H = \left\{\frac{m_1}{n_1}, \ldots, \frac{m_s}{n_s}\right\}$ *несократимых дробей из интервала* (0; 1) *множество* $T[H]$ *является разделимым и взаимно простым с каждым из чисел* $n_1, \ldots, n_s$.

В данном исследовании мы отдельно выделяем случай замыканий конечных множеств дробей, знаменатели которых являются степенями одного и того же простого числа, т. е. замыканий конечных подмножеств множеств $G[p]$, где p — простое число. В этом случае наш основной результат формулируется и доказывается более просто.

Теорема 2. *Пусть* p *— простое число,* $H = \left\{\frac{m_1}{n_1}, \ldots, \frac{m_s}{n_s}\right\}$ *— конечное множество несократимых дробей из* $G[p]$. *Тогда* $[H] = \langle G[p]; T[H]\rangle$.

Для доказательства теоремы 2 мы используем ряд вспомогательных утверждений. Доказательство следующей леммы дословно совпадает с доказательством леммы 3 в работе [8] и поэтому здесь нами опущено.

Лемма 8. *Пусть* p *— натуральное число, большее единицы,* $a, b \in N$, $(a, p) = (b, p) = 1$, M *— замкнутое множество чисел, содержащее множества* $G[p](a\colon 1)$ *и* $G[p](b\colon 1)$. *Тогда* $G[p]((a, b)\colon 1) \subseteq M$.

Поскольку для любого конечного множества натуральных чисел A, взаимно простого с p, множество $\langle G[p]; A\rangle$ содержит $G[p](\|A\|: 1)$ и согласно следствию 3 число $\|A\|$ взаимно просто с p, то из леммы 8 получаем

Следствие 9. *Пусть p — натуральное число, большее единицы, A — конечное разделимое множество натуральных чисел, взаимно простое с p, b — натуральное число, $(b, p) = 1$, M — замкнутое множество чисел, содержащее множества $\langle G[p]; A\rangle$ и $G[p](b: 1)$. Тогда $G[p]((\|A\|, b): 1) \subseteq M$.*

Лемма 9. *Пусть p — натуральное число, большее единицы, A — конечное разделимое множество натуральных чисел, взаимно простое с p, b — натуральное число, $(b, p) = 1$, M — замкнутое множество чисел, содержащее множества $\langle G[p]; A\rangle$ и $G[p](b: 1)$. Тогда $\langle G[p]; (A, \{b\})\rangle \subseteq M$.*

Доказательство. Согласно утверждениям 3 и 4 множество $(A, \{b\})$ разделимо и взаимно просто с p, поэтому множество $\langle G[p]; (A, \{b\})\rangle$ определено корректно. Рассмотрим произвольную дробь m/n из $\langle G[p]; (A, \{b\})\rangle$. Тогда найдется некоторое подмножество E множества $(A, \{b\})$ такое, что $m/n \in G[p](l': l'')$, где $l' = \prod_{e \in E} e$, $l'' = \prod_{e \in (A, \{b\}) \setminus E} e$. Обозначим через A' подмножество множества A, состоящее из тех чисел a, для которых $(a, b) \in E$. Положим $\widehat{l'} = \prod_{a \in A'} a$, $\widehat{l''} = \prod_{a \in A \setminus A'} a$. Число l', очевидно, является делителем числа $\widehat{l'}$, поэтому $\widehat{l'} = u'l'$, где u' — некоторое целое число. Аналогично существует некоторое целое число u'' такое, что $\widehat{l''} = u''l''$. Положим также $d = \|(A, \{b\})\|$ и $\widehat{d} = \|A\|$. Согласно утверждению 7 и следствию 3 имеем $(\widehat{d}, b) = d$ и $(\widehat{d}, p) = 1$. Заметим, что $\widehat{l'}\widehat{l''} = \widehat{d}$, $l'l'' = d$ и согласно утверждению 5 числа $\widehat{l'}$, $\widehat{l''}$ взаимно просты. Отметим также, что из взаимной простоты всех элементов множества A следует $(\widehat{l'}, b) = (\prod_{a \in A'} a, b) = \prod_{a \in A'} (a, b) = l'$ и аналогично $(\widehat{l''}, b) = l''$.

Если $\widehat{d} = 1$, т. е. все элементы множества A равны единице, то все элементы множества $(A, \{b\})$ также равны единице, тем самым $\langle G[p]; (A, \{b\})\rangle = G[p] = \langle G[p]; A\rangle$. Поэтому в этом случае утверждение леммы очевидно. Пусть $\widehat{d} > 1$. Обозначим через $\widehat{p}$ число $p^{\varphi(\widehat{d})}$. Так как $(\widehat{d}, p) = 1$, то согласно теореме Эйлера $\widehat{p} \equiv 1 \pmod{\widehat{d}}$. Выберем натуральное k_0 таким, чтобы $\widehat{p}^{k_0} > \widehat{d}$. Домножив числитель и знаменатель дроби m/n на подходящий коэффициент, мы можем представить ее в виде $\widehat{m}/\widehat{p}^{k}$, где $\widehat{m}$, $k \in N$ и $\min(\widehat{m}, \widehat{p}^{k} - \widehat{m}) > \widehat{d}\widehat{p}^{k_0}$.

Рассмотрим систему сравнений

$$\begin{cases} x \equiv 0 \pmod{\widehat{l'}}, \\ x \equiv 1 \pmod{\widehat{l''}}. \end{cases} \tag{43}$$

Так как $(\widehat{l'}, \widehat{l''}) = 1$, то согласно лемме 2 данная система имеет решение, являющееся классом вычетов по модулю $\widehat{l'}\widehat{l''} = \widehat{d}$:

$$x \equiv \alpha \pmod{\widehat{d}}.$$

Рассмотрим также систему сравнений

$$\begin{cases} x \equiv 0 \pmod{\widehat{l''}}, \\ x \equiv 1 \pmod{\widehat{l'}}. \end{cases} \tag{44}$$

Аналогично системе (43) решением этой системы является некоторый класс вычетов по модулю $\hat{d}$:

$$x \equiv \beta \pmod{\hat{d}}.$$

Из множества $\left\{1, \ldots, \hat{d}\right\}$ мы, очевидно, можем выбрать γ такое, что

$$\alpha + \gamma \equiv \beta \pmod{\hat{d}}. \tag{45}$$

Покажем, что $(\gamma, \hat{l}') = (\gamma, \hat{l}'') = 1$. Для этого предположим от противного, что $(\gamma, \hat{l}') = \delta > 1$. Так как α есть решение системы (43), то $\alpha \equiv 0 \pmod{\hat{l}'}$. Следовательно, $\alpha \equiv 0 \pmod{\delta}$. Мы также имеем $\gamma \equiv 0 \pmod{\delta}$. Почленно складывая два последних сравнения, получаем

$$\alpha + \gamma \equiv 0 \pmod{\delta}. \tag{46}$$

Так как $\hat{l}'$ является делителем числа $\hat{d}$, то $\hat{d}$ делится на δ. Поэтому из соотношения (45) вытекает, что $\alpha + \gamma \equiv \beta \pmod{\delta}$. Сопоставляя это сравнение со сравнением (46), получаем, что $\beta \equiv 0 \pmod{\delta}$. С другой стороны, поскольку β является решением системы (44), то $\beta \equiv 1 \pmod{\hat{l}'}$, и, следовательно, $\beta \equiv 1 \pmod{\delta}$. Таким образом, учитывая $\beta \equiv 0 \pmod{\delta}$, получаем, что $0 \equiv 1 \pmod{\delta}$, т. е. δ является делителем единицы, что противоречит нашему предположению. Предположим теперь, что $(\gamma, \hat{l}'') = \delta > 1$. Поскольку β является решением системы (44), то $\beta \equiv 0 \pmod{\hat{l}''}$, и, следовательно, $\beta \equiv 0 \pmod{\delta}$. Поэтому, учитывая $\gamma \equiv 0 \pmod{\delta}$, получаем, что

$$\beta - \gamma \equiv 0 \pmod{\delta}. \tag{47}$$

Из соотношения (45) вытекает, что $\alpha \equiv \beta - \gamma \pmod{\hat{d}}$. Так как $\hat{d}$ делится на $\hat{l}''$, то $\hat{d}$ также делится на δ. Поэтому $\alpha \equiv \beta - \gamma \pmod{\delta}$. Сопоставляя это сравнение со сравнением (47), получаем, что $\alpha \equiv 0 \pmod{\delta}$. С другой стороны, поскольку α является решением системы (43), то $\alpha \equiv 1 \pmod{\hat{l}''}$, и, следовательно, $\alpha \equiv 1 \pmod{\delta}$. Поэтому, учитывая $\alpha \equiv 0 \pmod{\delta}$, снова получаем, что $0 \equiv 1 \pmod{\delta}$, т. е. приходим к противоречию и в этом случае. Таким образом, $\hat{l}'$ и $\hat{l}''$ взаимно просты с γ. Следовательно, $(\gamma, \hat{d}) = (\gamma, \hat{l}'\hat{l}'') = 1$.

Рассмотрим сравнения

$$(\gamma d)x \equiv \hat{m} \pmod{\hat{l}'}, \tag{48}$$

$$(\gamma d)x \equiv \hat{m} - \hat{p}^* \pmod{\hat{l}''}. \tag{49}$$

Поскольку d является делителем $\hat{d}$ и $(\gamma, \hat{d}) = 1$, то $(\gamma, d) = 1$. Следовательно,

$$(\gamma d, \hat{l}') = (\gamma, \hat{l}')(d, \hat{l}') = (d, \hat{l}') = ((\hat{d}, b), \hat{l}') =$$
$$= (\hat{d}, (b, \hat{l}')) = (\hat{d}, l') = (u'l'\hat{l}'', l') = l'.$$

Аналогично имеем

$$(\gamma d, \hat{l}'') = l''.$$

Так как $\hat{m}/\hat{p}^* \in G[p](l' : l'')$, то $\hat{m} \equiv 0 \pmod{l'}$ и $\hat{m} \equiv \hat{p}^* \pmod{l''}$. Таким образом, $\hat{m} \equiv 0 \pmod{(\gamma d, \hat{l}')}$ и $\hat{m} - \hat{p}^* \equiv 0 \pmod{(\gamma d, \hat{l}'')}$. Поэтому согласно лемме 1 получаем, что сравнения (48) и (49) имеют решения, при

этом решением сравнения (48) является некоторый класс вычетов по модулю $\widehat{l'}/l' = u'$:

$$x \equiv c' \pmod{u'},$$

а решением сравнения (49) является некоторый класс вычетов по модулю $\widehat{l''}/l'' = u''$:

$$x \equiv c'' \pmod{u''},$$

Таким образом, объединяя сравнения (48) и (49), получим следующую систему:

$$\begin{cases} x \equiv c' \pmod{u'}, \\ x \equiv c'' \pmod{u''}. \end{cases} \tag{50}$$

Поскольку u' и u'' являются соответственно делителями взаимно простых чисел $\widehat{l'}$ и $\widehat{l''}$, то $(u', u'') = 1$. Поэтому согласно лемме 2 данная система имеет решение, являющееся классом вычетов по модулю $u'u''$. Пусть c_0 — наименьший положительный вычет из этого класса.

Положим $m_0 = \widehat{m} - \gamma dc_0$. Так как $0 < c_0 \leqslant u'u''$, то $0 < dc_0 \leqslant du'u'' = u'u''l'l'' = \widehat{l'}\widehat{l''} = \widehat{d} < \widehat{p}^{k_0}$. Тогда, поскольку $0 < \gamma \leqslant \widehat{d}$, то $\widehat{m} > m_0 > \widehat{m} - \gamma\widehat{p}^{k_0} \geqslant \widehat{m} - \widehat{d}\widehat{p}^{k_0} > 0$. Число c_0 является решением системы (50), поэтому оно одновременно является решением сравнений (48) и (49):

$$\gamma dc_0 \equiv \widehat{m} \pmod{\widehat{l'}},$$
$$\gamma dc_0 \equiv \widehat{m} - \widehat{p}^* \pmod{\widehat{l''}}.$$

Тем самым

$$m_0 = \widehat{m} - \gamma dc_0 \equiv 0 \pmod{\widehat{l'}}, \tag{51}$$

$$m_0 = \widehat{m} - \gamma dc_0 \equiv \widehat{p}^* \pmod{\widehat{l''}}. \tag{52}$$

Таким образом, $m_0/\widehat{p}^* \in G[p](\widehat{l'}: \widehat{l''}) = G[p](\prod_{a \in A'} a: \prod_{a \in A \setminus A'} a) \subseteq \langle G[p]; A \rangle$. Следовательно, по условию леммы, $m_0/\widehat{p}^* \in M$.

Положим теперь $m_1 = m_0 + \gamma\widehat{p}^{k_0} = \widehat{m} + \gamma(p^{k_0} - dc_0)$. Так как $0 < dc_0 < \widehat{p}^{k_0}$ и $0 < \gamma \leqslant \widehat{d}$, то $\widehat{m} < m_1 < \widehat{m} + \gamma\widehat{p}^{k_0} \leqslant \widehat{m} + \widehat{d}\widehat{p}^{k_0} < \widehat{m} + (\widehat{p}^* - \widehat{m}) = \widehat{p}^*$. Поскольку $\widehat{p} \equiv 1 \pmod{\widehat{d}}$ и $\widehat{l''}$ является делителем $\widehat{d}$, то $\widehat{p}^* \equiv 1 \pmod{\widehat{l''}}$. Поэтому из соотношений (51) и (52) вытекает, что число c_0 удовлетворяет системе (43). Следовательно,

$$c_0 \equiv \alpha \pmod{\widehat{d}}. \tag{53}$$

Из соотношения $\widehat{p} \equiv 1 \pmod{\widehat{d}}$ мы также имеем $\widehat{p}^{k_0} \equiv 1 \pmod{\widehat{d}}$, поэтому

$$\gamma\widehat{p}^{k_0} \equiv \gamma \pmod{\widehat{d}}. \tag{54}$$

Почленно складывая сравнения (53) и (54), получаем

$$m_1 = m_0 + \gamma\widehat{p}^{k_0} \equiv \alpha + \gamma \pmod{\widehat{d}}.$$

Сопоставив это соотношение со сравнением (45), получаем $m_1 \equiv \beta \pmod{\widehat{d}}$. Следовательно, число m_1 удовлетворяет системе сравнений (44). Поскольку

$\widehat{p} \equiv 1 \pmod{\widehat{d}}$ и $\widehat{l'}$ является делителем $\widehat{d}$, то $\widehat{p}^k \equiv 1 \pmod{\widehat{l'}}$. Поэтому из того, что m_1 удовлетворяет системе (44), следует, что

$$m_1 \equiv 0 \pmod{\widehat{l''}}, \quad m_1 \equiv \widehat{p}^k \pmod{\widehat{l'}}.$$

Таким образом, $m_1/\widehat{p}^k \in G[p](\widehat{l''}: \widehat{l'}) = G[p](\prod\limits_{a \in A \setminus A'} a: \prod\limits_{a \in A'} a) \subseteq \langle G[p]; A\rangle$. Следовательно, по условию леммы $m_1/\widehat{p}^k \in M$.

Рассмотрим также число $dc_0/\widehat{p}^{k_0}$. Поскольку $0 < dc_0 < \widehat{p}^{k_0}$, то $dc_0/\widehat{p}^{k_0} \in$ $\in G[p](d\colon 1)$. Так как $d = (\widehat{d}, b) = (\|A\|, b)$, то согласно следствию 9 имеем $G[p](d\colon 1) \subseteq M$. Следовательно, $dc_0/\widehat{p}^{k_0} \in M$.

В силу соотношения (2) для функции $f_*(x, y, z)$ имеем

$$\mathscr{P}\left\{f_*\left(\frac{m_0}{\widehat{p}^k}, \frac{m_1}{\widehat{p}^k}, \frac{dc_0}{\widehat{p}^{k_0}}\right)\right\} = \frac{m_0}{\widehat{p}^k} \cdot \left(1 - \frac{dc_0}{\widehat{p}^{k_0}}\right) + \frac{m_1}{\widehat{p}^k} \cdot \frac{dc_0}{\widehat{p}^{k_0}} =$$

$$= \frac{m_0(\widehat{p}^{k_0} - dc_0) + m_1 dc_0}{\widehat{p}^{k+k_0}} = \frac{m_0\widehat{p}^{k_0} + (m_1 - m_0)dc_0}{\widehat{p}^{k+k_0}} =$$

$$= \frac{m_0\widehat{p}^{k_0} + \gamma\widehat{p}^{k_0}dc_0}{\widehat{p}^{k+k_0}} = \frac{m_0 + \gamma dc_0}{\widehat{p}^k} = \frac{\widehat{m}}{\widehat{p}^k} = \frac{m}{n}.$$

Поскольку $m_0/\widehat{p}^k, m_1/\widehat{p}^k, dc_0/\widehat{p}^{k_0} \in M$ и M замкнуто, получаем, что $m/n \in M$.

Следствие 10. *Пусть p — натуральное число, большее единицы, A, B — конечные разделимые множества натуральных чисел, взаимно простые с p, M — замкнутое множество чисел, содержащее множества $\langle G[p]; A\rangle$ и $\langle G[p]; B\rangle$. Тогда $\langle G[p]; (A, \{\|B\|\})\rangle \subseteq M$.*

Это утверждение непосредственно вытекает из леммы 9 и очевидного соотношения $G[p](\|B\|\colon 1) \subseteq \langle G[p]; B\rangle$.

Применяя следствие 10 и лемму 7 для случая $n_1 = n_2 = p$, получим следующее утверждение.

Лемма 10. *Пусть p — натуральное число, большее единицы, A — конечное разделимое множество натуральных чисел, взаимно простое с p, B — двухэлементное разделимое множество натуральных чисел, взаимно простое с p, M — замкнутое множество чисел, содержащее множества $\langle G[p]; A\rangle$ и $\langle G[p]; B\rangle$. Тогда $\langle G[p]; (A, B)\rangle \subseteq M$.*

Следствие 11. *Пусть p, s — натуральные числа, большие единицы, $A_1, \ldots, A_s$ — двухэлементные разделимые множества натуральных чисел, взаимно простые с p, M — замкнутое множество чисел, содержащее множества $\langle G[p]; A_1\rangle, \ldots, \langle G[p]; A_s\rangle$. Тогда $\langle G[p]; (A_1, \ldots, A_s)\rangle \subseteq M$.*

Это утверждение непосредственно получается из леммы 10 применением индукции по s.

Доказательство теоремы 2. Согласно утверждению 12 множество $T[H]$ разделимо и взаимно просто с p, поэтому множество $\langle G[p]; T[H]\rangle$ определено корректно. Отметим также, что согласно следствию 1 множество $[H]$ является замкнутым. Заметим, что для любого i, $i = 1, \ldots, s$, дробь m_i/n_i принадлежит содержащемуся в $\langle G[p]; T[H]\rangle$ множеству $G[p](\prod\limits_{t \in T_i'} t: \prod\limits_{t \in T_i''} t)$, где

$$T_i' = \big(\{m_1, n_1 - m_1\}, \ldots, \{m_{i-1}, n_{i-1} - m_{i-1}\}, \{m_i\},$$
$$\{m_{i+1}, n_{i-1} - m_{i+1}\}, \ldots, \{m_s, n_s - m_s\}\big),$$

$$T_i'' = \big(\{m_1, n_1 - m_1\}, \ldots, \{m_{i-1}, n_{i-1} - m_{i-1}\}, \{n_i - m_i\},$$
$$\{m_{i+1}, n_{i-1} - m_{i+1}\}, \ldots, \{m_s, n_s - m_s\}\big).$$

Поэтому $\langle G[p]; T[H]\rangle$ содержит множество H и согласно лемме 3 является замкнутым множеством. Следовательно, $[H] \subseteq [\langle G[p]; T[H]\rangle] = \langle G[p]; T[H]\rangle$.

Для доказательства обратного соотношения мы используем лемму 6, согласно которой для любого i, $i = 1, \ldots, s$, выполняется $\langle G[n_i]; \{m_i, n_i - m_i\}\rangle = [\{m_i/n_i\}] \subseteq [H]$. Поскольку все числа $n_1, \ldots, n_s$ являются степенями числа p, то согласно утверждению 9 для любого i, $i = 1, \ldots, s$, имеем $\langle G[n_i]; \{m_i, n_i - m_i\}\rangle = \langle G[p]; \{m_i, n_i - m_i\}\rangle$ и, следовательно, $\langle G[p]; \{m_i, n_i - m_i\}\rangle \subseteq [H]$. Поэтому соотношение $\langle G[p]; T[H]\rangle \subseteq [H]$ очевидно при $s = 1$ и вытекает из следствия 11 при $s \geqslant 2$.

Используя утверждение 11, можно модифицировать теорему 2 следующим образом.

Теорема 3. *Пусть p — простое число, $H = \left\{\frac{m_1}{n_1}, \ldots, \frac{m_s}{n_s}\right\}$ — конечное множество несократимых дробей из $G[p]$. Тогда $[H] = \langle G[p]; T[H]^{-2}\rangle$.*

Основной результат для общего случая

Замыкание произвольного конечного множества рациональных чисел описывается следующим образом.

Теорема 4. *Пусть $H = \left\{\frac{m_1}{n_1}, \ldots, \frac{m_s}{n_s}\right\}$ — конечное множество несократимых дробей из интервала $(0; 1)$. Тогда*

$$[H] = \langle G[\widehat{n}]; T[H]\rangle, \quad \text{где } \widehat{n} = \prod_{p \in \bigcup_{i=1}^{s} \mathcal{P}[n_i]} p.$$

Для доказательства теоремы 4 также используется ряд вспомогательных утверждений. Следующая лемма приведена с доказательством в работе [8] в качестве леммы 6. Поэтому в данной работе мы приводим эту лемму без доказательства.

Лемма 11. *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 множества $G[n_1](m_1\colon 1)$ и $G[n_2](m_2\colon 1)$. Тогда $G[n_1]((m_1, m_2)\colon 1) \subseteq M$.*

Следствие 12. *Пусть n_1, n_2 — взаимно простые натуральные числа, большие единицы, A — конечное разделимое множество натуральных чисел, взаимно простое с n_1, b — натуральное число, $(b, n_2) = 1$, M — замкнутое множество чисел, содержащее множества $\langle G[n_1]; A\rangle$ и $G[n_2](b\colon 1)$. Тогда $G[n_1](\|A\|, b)\colon 1) \subseteq M$.*

Множество $\langle G[n_1]; A\rangle$ содержит $G[n_1](\|A\|\colon 1)$ и, согласно следствию 3, число $\|A\|$ взаимно просто с n_1, поэтому данное утверждение вытекает из леммы 11.

Лемма 12. *Пусть n_1, n_2 — взаимно простые натуральные числа, большие единицы, A — конечное разделимое множество натуральных чисел, взаимно простое с n_1, b — натуральное число, $(b, n_2) = 1$, M — замкнутое множество чисел, содержащее множества $\langle G[n_1]; A\rangle$ и $G[n_2](b\colon 1)$. Тогда $\langle G[n_1]; (A, \{b\})\rangle \subseteq M$.*

Доказательство. Согласно следствию 3 имеем $(\|A\|, n_1) = 1$, тем самым $((\|A\|, b), n_1) = 1$. В силу следствия 12 множество M содержит $G[n_1](((\|A\|, b)\colon 1)$. Поэтому согласно лемме 9 множество M содер-

жит $\langle G[n_1]; (A, \{(\|A\|, b)\})\rangle$. Очевидно, что для любого $a \in A$ выполняется $(a, b) = (a, (\|A\|, b))$, поэтому $(A, \{b\}) = (a, \{(\|A\|, b)\|)$. Таким образом, $\langle G[n_1]; (A, \{b\})\rangle = \langle G[n_1]; (A, \{(\|A\|, b)\})\rangle \subseteq M$.

Следствие 13. *Пусть n_1, n_2 — взаимно простые натуральные числа, большие единицы, A, B — конечные разделимые множества натуральных чисел, взаимно простые с числами n_1 и n_2 соответственно, M — замкнутое множество чисел, содержащее множества $\langle G[n_1]; A\rangle$ и $\langle G[n_1]; B\rangle$. Тогда $\langle G[n_1]; (A, \{\|B\|\})\rangle \subseteq M$.*

Это утверждение непосредственно вытекает из леммы 12 и очевидного соотношения $G[n_2](\|B\|: 1) \subseteq \langle G[n_2]; B\rangle$.

Применяя следствие 13 и лемму 7, получим следующее утверждение.

Лемма 13. *Пусть n_1, n_2 — взаимно простые натуральные числа, большие единицы, A — конечное разделимое множество натуральных чисел, взаимно простое с n_1, B — двухэлементное разделимое множество натуральных чисел, взаимно простое с n_2, M — замкнутое множество чисел, содержащее множества $\langle G[n_1]; A\rangle$ и $\langle G[n_2]; B\rangle$. Тогда $\langle G[n_1]; (A, B)\rangle \subseteq M$.*

Следствие 14. *Пусть $n_1, \ldots, n_s$, где $s \geqslant 2$, — натуральные числа, большие единицы, и $(n_1, n_2) = \ldots = (n_1, n_s) = 1$, A_1 — конечное разделимое множество натуральных чисел, взаимно простое с n_1, $A_2, \ldots, A_s$ — двухэлементные разделимые множества натуральных чисел, взаимно простые с числами $n_2, \ldots, n_s$ соответственно, M — замкнутое множество чисел, содержащее множества $\langle G[n_1]; A_1\rangle, \ldots, \langle G[n_s]; A_s\rangle$. Тогда $\langle G[n_1]; (A_1, \ldots, A_s)\rangle \subseteq M$.*

Это утверждение непосредственно получается из леммы 13 с помощью индукции по s.

Лемма 14. *Пусть n_1, n_2 — взаимно простые натуральные числа, большие единицы, A — конечное разделимое множество натуральных чисел, взаимно простое с n_1 и n_2, M — замкнутое множество чисел, содержащее множества $\langle G[n_1]; A\rangle$ и $\langle G[n_2]; A\rangle$. Тогда $\langle G[n_1 n_2]; A\rangle \subseteq M$.*

Доказательство. Пусть $m/(n_1 n_2)^k$ — произвольная дробь из множества $\langle G[n_1 n_2]; A\rangle$. Тогда найдется некоторое подмножество E множества A такое, что $m/(n_1 n_2)^k \in G[n_1 n_2](l': l'')$, где $l' = \prod\limits_{e \in E} e$, $l'' = \prod\limits_{e \in A \setminus E} e$. Положим $d = \|A\|$. Заметим, что $l' l'' = d$. Выберем натуральное k_2 такое, что $n_2^{k_2 - k} > d$. Домножив числитель и знаменатель дроби $m/(n_1 n_2)^k$ на подходящий коэффициент, представим ее в виде $\widehat{m}/(n_1^{k_1} n_2^k)$, где $\widehat{m}, k_1 \in N$ и $\min(\widehat{m}, n_1^{k_1} n_2^k - \widehat{m}) > d n_2^{k_2}$.

Согласно следствию 3 выполняется $(d, n_2) = 1$, тогда $(d^2, n_2^k) = 1$, поэтому согласно следствию 4 найдутся целые c_0, c_1 такие, что $c_0 d^2 + c_1 n_2^k = \widehat{m}$, при этом, очевидно, число c_0 может быть выбрано из множества $\{1, \ldots, n_2^k\}$. Тогда имеем

$$n_1^{k_1} n_2^k > \widehat{m} > c_1 n_2^k \geqslant \widehat{m} - n_2^k d^2 > d n_2^{k_2} - d^2 n_2^k = d n_2^k (n_2^{k_2 - k} - d) > 0.$$

Следовательно, $n_1^{k_1} > c_1 > 0$. Поэтому дробь $c_1/n_1^{k_1}$ принадлежит множеству $G[n_1]$. Отметим также, что $c_1 n_2^k = \widehat{m} - c_0 d^2 \equiv \widehat{m} \pmod d$. Так как $\widehat{m}/(n_1^{k_1} n_2^k) \in G[n_1 n_2](l': l'')$, то $\widehat{m} \equiv 0 \pmod{l'}$ и $\widehat{m} \equiv n_1^{k_1} n_2^k \pmod{l''}$. Поскольку l' — делитель d, то $c_1 n_2^k \equiv \widehat{m} \pmod d$ влечет $c_1 n_2^k \equiv \widehat{m} \pmod{l'}$. Поэтому из $\widehat{m} \equiv 0 \pmod{l'}$ следует

$$c_1 n_2^k \equiv 0 \pmod{l'}. \tag{55}$$

Аналогично из $\widehat{m} \equiv n_1^{k_1} n_2^k \pmod{l''}$ получаем

$$c_1 n_2^k \equiv n_1^{k_1} n_2^k \pmod{l''}. \tag{56}$$

Так как $(d, n_2^k) = (l'l'', n_2^k) = 1$, то $(l', n_2^k) = (l'', n_2^k) = 1$. Поэтому мы можем поделить обе части сравнений (55) и (56) на n_2^k, получив

$$c_1 \equiv 0 \pmod{l'}, \quad c_1 \equiv n_1^{k_1} \pmod{l''}. \tag{57}$$

Таким образом, $c_1/n_1^{k_1} \in G[n_1](l': l'') \subseteq \langle G[n_1]; A\rangle \subseteq M$.

Положим $c_2 = c_1 + dn_2^{k_2-k}$. Так как

$$0 < c_1 < c_2 n_2^k = c_1 n_2^k + dn_2^{k_2} < \widehat{m} + dn_2^{k_2} < n_1^{k_1} n_2^k,$$

то $0 < c_2 < n_1^{k_1}$. Поэтому дробь $c_2/n_1^{k_1}$ принадлежит множеству $G[n_1]$. Так как c_2 сравнимо с c_1 по модулю $d = l'l''$, то из справедливости соотношений (57) для c_1 вытекает справедливость аналогичных соотношений для c_2:

$$c_2 \equiv 0 \pmod{l'}, \quad c_2 \equiv n_1^{k_1} \pmod{l''}.$$

Таким образом, $c_2/n_1^{k_1}$ также принадлежит множеству $G[n_1](l': l'')$, поэтому $c_2/n_1^{k_1} \in \langle G[n_1]; A\rangle \subseteq M$.

Рассмотрим также дробь $dc_0/n_2^{k_2}$. Заметим, что $0 < dc_0 \leqslant dn_2^k < n_2^{k_2}$, следовательно, $dc_0/n_2^{k_2} \in G[n_2](d: 1) \subseteq \langle G[n_2]; A\rangle \subseteq M$.

Используя соотношение (2) для функции $f_*(x, y, z)$, получаем

$$\mathscr{P}\left\{f_*\left(\frac{c_1}{n_1^{k_1}}, \frac{c_2}{n_1^{k_1}}, \frac{dc_0}{n_2^{k_2}}\right)\right\} = \frac{c_1}{n_1^{k_1}} \cdot \left(1 - \frac{dc_0}{n_2^{k_2}}\right) + \frac{c_2}{n_1^{k_1}} \cdot \frac{dc_0}{n_2^{k_2}} =$$

$$= \frac{c_1(n_2^{k_2} - dc_0) + c_2 dc_0}{n_1^{k_1} n_2^{k_2}} = \frac{c_1 n_2^{k_2} + (c_2 - c_1)dc_0}{n_1^{k_1} n_2^{k_2}} =$$

$$= \frac{c_1 n_2^{k_2} + d^2 c_0 n_2^{k_2-k}}{n_1^{k_1} n_2^{k_2}} = \frac{c_1 n_2^k + d^2 c_0}{n_1^{k_1} n_2^k} = \frac{\widehat{m}}{n_1^{k_1} n_2^k} = \frac{m}{(n_1 n_2)^k}.$$

Следовательно, поскольку $c_1/n_1^{k_1}, c_2/n_1^{k_1}, dc_0/n_2^{k_2} \in M$ и M замкнуто, то $m/(n_1 n_2)^k \in M$.

Следствие 15. *Пусть $n_1, \ldots, n_s$, где $s \geqslant 2$, — попарно простые натуральные числа, большие единицы, A — конечное разделимое множество натуральных чисел, взаимно простое с числами $n_1, \ldots, n_s$, M — замкнутое множество чисел, содержащее множества $\langle G[n_1]; A\rangle, \ldots, \langle G[n_s]; A\rangle$. Тогда $\langle G[n_1 \ldots n_s]; A\rangle \subseteq M$.*

Это утверждение непосредственно получается из леммы 14 применением индукции по s.

Доказательство теоремы 4. Согласно утверждению 12 множество $T[H]$ разделимо и взаимно просто с числами $n_1, \ldots, n_s$, тем самым $T[H]$ взаимно просто с числом $\widehat{n}$, являющимся делителем числа $n_1 \ldots n_s$. Таким образом, множество $\langle G[p]; T[H]\rangle$ определено корректно. Отметим также, что согласно следствию 1 множество $[H]$ является замкнутым. Заметим, что для любого i, $i = 1, \ldots, s$, дробь m_i/n_i принадлежит содержащемуся в $\langle G[n_i]; T[H]\rangle$ множеству $G[n_i](\prod\limits_{t \in T_i'} t: \prod\limits_{t \in T_i''} t)$, где

$$T_i' = (\{m_1, n_1 - m_1\}, \ldots, \{m_{i-1}, n_{i-1} - m_{i-1}\}, \{m_i\},$$
$$\{m_{i+1}, n_{i-1} - m_{i+1}\}, \ldots, \{m_s, n_s - m_s\}),$$

$$T_i'' = (\{m_1, n_1 - m_1\}, \ldots, \{m_{i-1}, n_{i-1} - m_{i-1}\}, \{n_i - m_i\},$$
$$\{m_{i+1}, n_{i-1} - m_{i+1}\}, \ldots, \{m_s, n_s - m_s\}).$$

По утверждению 9 для любого i, $i=1,\ldots,s$, множество $\langle G[n_i]; T[H]\rangle$ содержится в $\langle G[\widehat{n}]; T[H]\rangle$, поэтому получаем, что $\langle G[\widehat{n}]; T[H]\rangle$ содержит H и согласно лемме 3 является замкнутым множеством. Следовательно, $[H]\subseteq[\langle G[\widehat{n}]; T[H]\rangle]=\langle G[\widehat{n}]; T[H]\rangle$.

Докажем теперь, что $\langle G[\widehat{n}]; T[H]\rangle\subseteq[H]$. Для удобства обозначим множество $\bigcup_{i=1}^{s}\mathscr{P}[n_i]$ через П. Рассмотрим произвольное простое p из П. Без ограничения общности мы можем считать, что p является делителем чисел $n_1,\ldots,n_t$, где $1\leqslant t\leqslant s$, и не является делителем чисел $n_{t+1},\ldots,n_s$. Обозначим через H' подмножество $\left\{\frac{m_1}{n_1},\ldots,\frac{m_t}{n_t}\right\}$ множества H. Используя утверждение 9 и лемму 6, для любого i, $i=1,\ldots,t$, имеем

$$\langle G[p]; \{m_i, n_i-m_i\}\rangle\subseteq\langle G[n_i]; \{m_i, n_i-m_i\}\rangle=\left[\left\{\frac{m_i}{n_i}\right\}\right]\subseteq[H].$$

Тогда применяя в случае $t\geqslant 2$ следствие 11, получим, что $[H]$ содержит множество $\langle G[p]; T[H']\rangle$. В случае $t=s$ имеем $H'=H$, поэтому

$$\langle G[p]; T[H]\rangle\subseteq[H]. \tag{58}$$

Пусть $t<s$. Согласно лемме 6 для любого i, $i=t+1,\ldots,s$, выполняется $\langle G[n_i]; \{m_i, n_i-m_i\}\rangle\subseteq\left[\left\{\frac{m_i}{n_i}\right\}\right]$. Таким образом, множество $[H]$ наряду со множеством $\langle G[p]; T[H']\rangle$ содержит множества $\langle G[n_{t+1}]; \{m_{t+1}, n_{t+1}-m_{t+1}\}\rangle,\ldots,\langle G[n_s]; \{m_s, n_s-m_s\}\rangle$, где числа $n_{t+1},\ldots,n_s$ взаимно просты с p. Поэтому мы можем применить следствие 14 и получить, что в этом случае также справедливо соотношение (58). Таким образом, мы показали, что соотношение (58) выполняется для любого p из П. Тогда соотношение $\langle G[\widehat{n}]; T[H]\rangle\subseteq[H]$ очевидно при $|\Pi|=1$ и вытекает из следствия 15 при $|\Pi|\geqslant 2$.

Используя утверждение 11, можно модифицировать теорему 4 следующим образом.

Теорема 5. *Пусть* $H=\left\{\frac{m_1}{n_1},\ldots,\frac{m_s}{n_s}\right\}$ — *конечное множество несократимых дробей из интервала* $(0;1)$, *где* $\widehat{n}=\prod_{p\in\bigcup_{i=1}^{s}\mathscr{P}[n_i]}p$. *Тогда*

$$[H]=\langle G[\widehat{n}]; T[H]^{-2}\rangle.$$

Заключение

Заметим, что используемое нами для описания замыкания $[H]$ множество $T[H]^{-2}$ может быть, очевидно, вычислено по формуле

$$T[H]^{-2}=((\ldots(\{m_1, n_1-m_1\}^{-2}, \{m_2, n_2-m_2\}^{-2})^{-2},\ldots)^{-2}, \{m_s, n_s-m_s\}^{-2})^{-2}$$

и такой способ вычисления является более выгодным в практическом плане (в случае, если для какого-либо i, $i=2,\ldots,s$, множество

$$((\ldots(\{m_1, n_1-m_1\}^{-2}, \{m_2, n_2-m_2\}^{-2})^{-2},\ldots)^{-2}, \{m_i, n_i-m_i\}^{-2})^{-2},$$

оказалось пустым, то из (3) и (7) непосредственно получаем, что $T[H]^{-2}=\varnothing$ и соответственно $\langle G[n]; T[H]^{-2}\rangle=G[n]$).

В данной работе мы рассматриваем только замыкания конечных множеств чисел, однако, как нетрудно убедиться, полученные нами результаты могут быть сформулированы также для случая замыканий бесконечных множеств. Отметим также, что рассмотренная нами задача описания всех возможных преобразований булевых случайных величин представляет собой частный случай задачи описания всех возможных преобразований случайных величин, принимающих произвольное конечное число различных значений. Ряд существенных результатов в решении этой более общей задачи был получен Ф. И. Салимовым в работах [12, 13]. Обобщение наших результатов на случай преобразователей случайных величин, принимающих конечное число различных значений, позволило бы, на наш взгляд, непосредственно приступить к практической реализации преобразователей вероятностных распределений.

С практической точки зрения также являются важными сложностные аспекты построения преобразователей вероятностных распределений. В работах [3, 9] исследовалась сложность схемной реализации преобразователей булевых случайных величин. Другой содержательной мерой сложности преобразователей вероятностных распределений является количество используемых ими исходных случайных величин. Под сложностью порождения числа множеством чисел тогда понимается минимальная возможная сложность преобразователя булевых случайных величин с распределениями, задаваемыми числами из данного множества, в булеву случайную величину с распределением, задаваемым данным числом. В работах автора [7, 17] получены асимптотически точные оценки сложности порождения рациональных чисел конечными множествами рациональных чисел специального вида. Однако вопрос об асимптотике сложности порождения рациональных чисел произвольными конечными множествами рациональных чисел остается пока открытым.

Автор благодарен проф. О. М. Касим-Заде за ценную библиографическую информацию и за поддержку данных исследований.

СПИСОК ЛИТЕРАТУРЫ

1. Бухараев Р. Г. Основы теории вероятностных автоматов. — М.: Наука, 1985.
2. Виноградов И. М. Основы теории чисел. — М.: Наука, 1981.
3. Захаров В. М., Салимов Ф. И. К теории структурного синтеза детерминированных преобразователей вероятности // Problems of Control and Information Theory. — 1977. — V. 6, № 2. — P. 137–148.
4. Колпаков Р. М. О порождении рациональных чисел вероятностными контактными сетями // Вестник МГУ. Сер. 1. Математика. Механика. — 1992. — № 5. — С. 46–52.
5. Колпаков Р. М. О порождении рациональных чисел вероятностными контактными π-сетями // Дискретная математика. — 1994. — № 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 сложности порождения рациональных чисел одноэлементными множествами в классе всех булевых функций // Материалы VII межгосударственной школы-семинара «Синтез и сложность управляющих систем». — М.: Изд-во МГУ, 1996. — С. 13–14.
8. Колпаков Р. М. Критерий порождения множеств рациональных вероятностей в классе булевых функций // Дискретный анализ и исследование операций. Сер. 1. — Новосибирск: ИМ СО РАН, 1999. — Т. 6, № 2. — С. 41–61.
9. Нурмеев Н. Н. О сложности реализации преобразователей вероятностей схемами из функциональных элементов // Методы и системы тех. диагностики: межвуз. сборник научных трудов. Вып. 18. — Саратов, 1993. — С. 131–132.
10. Нурмеев Н. Н. О булевых функциях с аргументами, принимающими случайные значения // VIII Всесоюзная конференция «Проблемы теоретической кибернетики»: Тез. докл. — Горький, 1988. — Ч. 2. — С. 59–60.
11. Салимов Ф. И. К вопросу моделирования булевых случайных величин функциями алгебры логики // Вероятностные методы и кибернетика. Вып. 15. — Казань: Казанский гос. университет, 1979. — С. 68–89.

12. Салимов Ф. И. Конечная порожденность некоторых алгебр над случайными величинами // Вопросы кибернетики. Вып. 86. — М., 1982. — С. 122–130.
13. Салимов Ф. И. Конечная порожденность алгебр распределений // Дискретный анализ и исследование операций. — Новосибирск: ИМ СО РАН, 1997. — Т. 4, № 2. — С. 43–50.
14. Салимов Ф. И. Об одном семействе алгебр распределений // Известия вузов. Сер. Математика. — 1988. — № 7. — С. 64–72.
15. Схиртладзе Р. Л. О синтезе p-схемы из контактов со случайными дискретными состояниями // Сообщ. АН ГрССР. — 1961. — Т. 26, № 2. — С. 181–186.
16. Схиртладзе Р. Л. О методе построения булевой случайной величины с заданным распределением вероятностей // Дискретный анализ. Вып. 7. — Новосибирск: ИМ СО АН СССР, 1966. — С. 71–80.
17. Kolpakov R. M. On the complexity of generation of rational numbers by Boolean functions // Fundamenta Informaticae. — 1995. — V. 22, № 3. — P. 289–298.
18. Nisan N., Ta-Shma A. Extracting randomness: A survey and new constructions // J. of Computer and System Sciences. — 1999. — V. 58, № 1. — P. 148–173.

Поступило в редакцию 25 V 2000