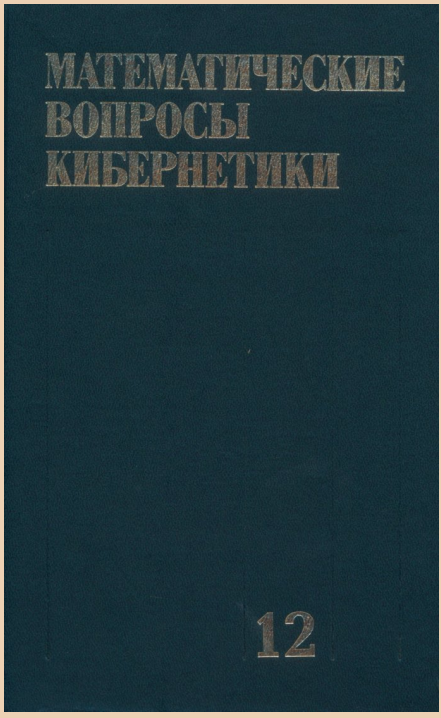
ИПМ им. М.В. Келдыша РАН • Электронная библиотека
Математические вопросы кибернетики • Выпуск 12



Р. М. Колпаков

О дискретных преобразованиях конечных распределений с рациональными вероятностями

Рекомендуемая форма библиографической ссылки: Колпаков Р. М. О дискретных преобразованиях конечных распределений с рациональными вероятностями // Математические вопросы кибернетики. Вып. 12. — М.: ФИЗМАТЛИТ, 2003. — С. 109–146. URL: http://library.keldysh.ru/mvk.asp?id=2003-109

О ДИСКРЕТНЫХ ПРЕОБРАЗОВАНИЯХ КОНЕЧНЫХ РАСПРЕДЕЛЕНИЙ С РАЦИОНАЛЬНЫМИ ВЕРОЯТНОСТЯМИ

Р. М. КОЛПАКОВ

(МОСКВА)

§ 1. Введение

Данная работа посвящена исследованиям дискретных преобразований конечных вероятностных распределений с рациональными значениями вероятностей. Такие преобразования играют важную роль в вопросах реализации случайностей, имеющих большое значение для многих областей математической кибернетики (см. [1, 13]). Под преобразованием вероятностных распределений мы понимаем вероятностное распределение некоторой случайной величины ζ_0, значение которой однозначно определяется значениями конечного числа независимых случайных величин $\zeta_1, \ldots, \zeta_k$ с исходными вероятностными распределениями. Таким образом, данное преобразование задается функцией f: $\Omega_1 \times \ldots \times \Omega_k \longrightarrow \Omega_0$, где Ω_i — множество значений случайной величины ζ_i, $i = 0, 1, \ldots, k$. Нами рассматриваются случайные величины, принимающие конечное число значений. Не ограничивая общности, мы можем считать, что такая случайная величина принимает целые неотрицательные значения, а ее вероятностное распределение задается вектором, j-я компонента которого равна вероятности принятия этой случайной величиной значения $j-1$. Отметим, что этот вектор является *стохастическим*, т. е. все его компоненты неотрицательны и сумма всех его компонент равна 1. Мы будем обозначать j-ю компоненту стохастического вектора $\mathscr{D}$ через $\mathscr{D}[j]$. Пусть $\Omega_i = \{0, 1, \ldots, h_i - 1\}$ и вероятностное распределение случайной величины ζ_i задается стохастическим вектором $\mathscr{D}_i$ размерности h_i, $i = 0, 1, \ldots, k$. Множество $\Omega_1 \times \ldots \times \Omega_k = \{0, 1, \ldots, h_1 - 1\} \times \ldots \times \{0, 1, \ldots, h_k - 1\}$ будем обозначать через $\Omega(\mathscr{D}_1, \ldots, \mathscr{D}_k)$. Для любого подмножества E этого множества обозначим через $\boldsymbol{P}_E(\mathscr{D}_1, \ldots, \mathscr{D}_k)$ вероятность того, что набор $(\sigma_1; \ldots; \sigma_k)$ значений величин $\zeta_1, \ldots, \zeta_k$ содержится в E. Тогда *)

$$\boldsymbol{P}_E(\mathscr{D}_1, \ldots, \mathscr{D}_k) = \sum_{(\sigma_1; \ldots; \sigma_k) \in E} \mathscr{D}_1[\sigma_1 + 1] \cdot \ldots \cdot \mathscr{D}_k[\sigma_k + 1]. \tag{1}$$

Через $\mathscr{N}_i(f)$ обозначим множество всех наборов из $\Omega(\mathscr{D}_1, \ldots, \mathscr{D}_k)$, на которых функция f принимает значение i. Используя это обозначение, мы определяем компоненты вектора $\mathscr{D}_0$ следующим образом:

$$\mathscr{D}_0[j] = \boldsymbol{P}_{\mathscr{N}_{j-1}(f)}(\mathscr{D}_1, \ldots, \mathscr{D}_k), \quad j = 1, \ldots, h_0. \tag{2}$$

*) В случае $E = \varnothing$ мы естественным образом полагаем сумму (1) равной 0.

В дальнейшем мы обозначаем вектор $\mathscr{D}_0$ через $\boldsymbol{P}\{f(\mathscr{D}_1, \ldots, \mathscr{D}_k)\}$.

Пусть H — множество различных стохастических векторов. Мы говорим, что стохастический вектор $\mathscr{D}$ *порождается* множеством H, если для некоторой функции $f(x_1, \ldots, x_k)$ и некоторых $\mathscr{D}_1, \ldots, \mathscr{D}_k$ из H выполняется равенство $\mathscr{D} = \boldsymbol{P}\{f(\mathscr{D}_1, \ldots, \mathscr{D}_k)\}$. Через $\langle H \rangle$ мы обозначаем *замыкание* множества H, т. е. множество всех стохастических векторов, порождаемых множеством H. Очевидно, что $H \subseteq \langle H \rangle$. Множество H называется *замкнутым*, если $\langle H \rangle = H$. Будем также говорить, что множество A стохастических векторов *порождается* множеством H, если $A \subseteq \langle H \rangle$. Для произвольного множества натуральных чисел T и натурального k мы обозначаем через $T^{>k}$ множество всех чисел из T, больших k. Для любого натурального числа n обозначим через $\mathscr{J}(n)$ множество всех простых делителей этого числа. Кроме того, в работе используются следующие обозначения:

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

$\mathbb{Z}^+$ — множество целых неотрицательных чисел;

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

$|A|$ — число элементов множества A.

Для синтеза генераторов вероятностных распределений большой интерес представляет задача описания замыканий произвольных множеств стохастических векторов. Принципиальная трудность этой задачи заключается, очевидно, в невозможности непосредственного описания таких множеств, поскольку мощность множества всех стохастических векторов равна континууму. Поэтому естественным подходом к ее решению является рассмотрение замыканий подмножеств не более, чем счетных, закнутых классов стохастических векторов, всюду плотных на множестве всех стохастических векторов. Наиболее подходящим примером такого класса представляется множество всех стохастических векторов с рациональными компонентами. Мы обозначаем это множество через $\boldsymbol{SQ}$. Из формул (2) и (1) нетрудно заметить, что любой стохастический вектор, порождаемый векторами из $\boldsymbol{SQ}$, принадлежит $\boldsymbol{SQ}$, тем самым множество $\boldsymbol{SQ}$ является замкнутым. Для любого непустого множества П различных простых чисел мы выделяем из $\boldsymbol{SQ}$ подмножество $G[\Pi]$ всех стохастических векторов, компоненты которых выражаются дробями со знаменателями, являющимися произведениями степеней чисел из П:

$$G[\Pi] = \left\{ (d_1; \ldots; d_h) \;\middle|\; \begin{array}{l} \sum\limits_{i=1}^{h} d_i = 1,\ d_i = \frac{m_i}{n},\ m_i \in \mathbb{Z}^+,\ i = 1, \ldots, h, \\ n \in \mathbb{N},\ \mathscr{J}[n] \subseteq \Pi \end{array} \right\}.$$

Пользуясь формулами (2) и (1), легко получить, что множество $G[\Pi]$, как и множество $\boldsymbol{SQ}$, является замкнутым.

Насколько нам известно, исследования в данной области начались с рассмотрения случая двумерных векторов (поскольку двумерный стохастический вектор однозначно определяется какой-либо одной из его компонент, в работах, посвященных порождению двумерных векторов, как правило, вместо векторов рассматриваются числа, являющиеся вторыми компонентами этих векторов). В [11, 12] показано, что множества всех двумерных стохастических векторов из $G[\{2\}]$ и $G[\{3\}]$ порождаются векторами $\left(\frac{1}{2}; \frac{1}{2}\right)$ и $\left(\frac{1}{3}; \frac{2}{3}\right)$ соответственно. В [7, 10] данные результаты были обобщены на случай множества всех двумерных стохастических векторов из $G[\Pi]$ для произвольного П. При этом была полностью установлена структура решетки, образуемой этими множествами. Аналогичные результаты для случая стохастических векторов произвольной размерности получены в [8, 9]. Некоторые аспекты приближенного порождения двумерных стохастических векторов рассматривались в [6, 12]. В [3] дано явное описание замыканий

всех множеств в классе всех двумерных стохастических векторов из $\boldsymbol{SQ}$. В [5] явно описаны замыкания всех конечных множеств двумерных векторов в классе $\boldsymbol{SQ}$. В настоящей работе мы обобщаем этот результат на случай замыканий всех конечных множеств векторов из $\boldsymbol{SQ}$. Полученное нами описание этих замыканий позволяет для любого заданного стохастического вектора и любого заданного конечного множества векторов из $\boldsymbol{SQ}$ эффективно определить, порождается ли данный вектор данным множеством.

§ 2. Вспомогательные определения и результаты

Базовым свойством замыканий множеств стохастических векторов является

Утверждение 1. *Замыкание любого множества стохастических векторов является замкнутым множеством.*

Доказательство. Пусть M — произвольное множество стохастических векторов, $\mathscr{D}$ — стохастический вектор, порождаемый множеством $\langle M\rangle$. Тогда $\mathscr{D}=\boldsymbol{P}\{f(\mathscr{D}_1,\ldots,\mathscr{D}_n)\}$ для некоторой функции $f(x_1,\ldots,x_n)$ и некоторых стохастических векторов $\mathscr{D}_1,\ldots,\mathscr{D}_n$ из $\langle M\rangle$. Для каждого i, $i=1,\ldots,n$, существуют функция $f_i(x_1,\ldots,x_{k(i)})$ и стохастические векторы $\mathscr{D}_1^{(i)},\ldots,\mathscr{D}_{k(i)}^{(i)}$ из M такие, что $\mathscr{D}_i=\boldsymbol{P}\{f(\mathscr{D}_1^{(i)},\ldots,\mathscr{D}_{k(i)}^{(i)})\}$. Тогда непосредственным образом можно проверить, что

$$\boldsymbol{P}\{\widehat{f}(\mathscr{D}_1^{(1)},\ldots,\mathscr{D}_{k(1)}^{(1)},\ldots,\mathscr{D}_1^{(n)},\ldots,\mathscr{D}_{k(n)}^{(n)})\},$$

где

$$\widehat{f}(x_1^{(1)},\ldots,x_{k(1)}^{(1)},\ldots,x_1^{(n)},\ldots,x_{k(n)}^{(n)})=$$
$$=f\left(f_1(x_1^{(1)},\ldots,x_{k(1)}^{(1)}),\ldots,f_n(x_1^{(n)},\ldots,x_{k(n)}^{(n)})\right).$$

Следовательно, $\mathscr{D}\in\langle M\rangle$. Таким образом, $\langle\langle M\rangle\rangle=\langle M\rangle$.

Заметим, что любой стохастический вектор порождает все векторы, получающиеся из этого вектора перестановкой его компонент. Поэтому из утверждения 1 следует

Утверждение 2. *Для любых стохастических векторов $\mathscr{D}'$ и $\mathscr{D}''$, получающихся друг из друга перестановкой компонент, выполняется* $\langle\{\mathscr{D}'\}\rangle=\langle\{\mathscr{D}''\}\rangle$.

Стохастический вектор будем называть *вырожденным*, если он содержит компоненту, равную 1. Мы естественным образом можем считать, что все вырожденные стохастические векторы порождаются пустым множеством и поэтому содержатся в замыкании любого множества чисел. Для любого невырожденного стохастического вектора $\mathscr{D}$ будем обозначать через $\mathscr{D}^+$ стохастический вектор, получающийся из $\mathscr{D}$ удалением всех нулевых компонент. Через M^+, где M — произвольное множество стохастических векторов, мы обозначаем множество всех векторов $\mathscr{D}^+$ таких, что $\mathscr{D}\in M$. Отметим следующий очевидный факт.

Утверждение 3. *Для любого множества M стохастических векторов выполняется* $\langle M\rangle=\langle M^+\rangle$.

Невырожденные стохастические векторы с ненулевыми компонентами будем называть *позитивными* векторами. Множество M стохастических векторов назовем *позитивно замкнутым*, если для любого невырожденного вектора $\mathscr{D}$ из M вектор $\mathscr{D}^+$ также содержится в M. Заметим, что невырожденный вектор $\mathscr{D}$ порождается множеством стохастических векторов тогда и только тогда, когда это множество порождает вектор $\mathscr{D}^+$. Поэтому мы имеем

Утверждение 4. *Позитивно замкнутое множество M порождается множеством H стохастических векторов тогда и только тогда, когда H порождает любой позитивный вектор из M.*

В стохастическом векторе $\mathscr{D} = (d_1; \ldots; d_h)$ компонента d_h однозначно определяется компонентами $d_1, \ldots, d_{h-1}$. Поэтому имеет место

Утверждение 5. *Для любого стохастического вектора $\mathscr{D}_0$ размерности h и любой h-значной функции $f(x_1, \ldots, x_k)$ соотношение $\mathscr{D}_0 = \boldsymbol{P}\{f(\mathscr{D}_1, \ldots, \mathscr{D}_k)\}$ выполняется тогда и только тогда, когда равенства (2) справедливы для $j = 1, \ldots, h-1$.*

Отметим еще один очевидный факт.

Утверждение 6. *Пусть $\mathscr{D}_1, \ldots, \mathscr{D}_k$ — стохастические векторы, $A_1, \ldots, A_s$ — непересекающиеся подмножества множества $\Omega(\mathscr{D}_1, \ldots, \mathscr{D}_k)$. Тогда*

$$\boldsymbol{P}_{\bigcup_{i=1}^{s} E_i}(\mathscr{D}_1, \ldots, \mathscr{D}_k) = \sum_{i=1}^{s} \boldsymbol{P}_{A_i}(\mathscr{D}_1, \ldots, \mathscr{D}_k).$$

Обозначим через E_t^k множество всех упорядоченных наборов, состоящих из k символов $0, 1, \ldots, t-1$. Набор из E_t^k, состоящий из одинаковых символов, называется *однородным*. Мы обозначаем множество всех однородных наборов из E_t^k через C_t^k. Множество $E_t^k \setminus C_t^k$ разбивается на непересекающиеся подмножества, состоящие из всех наборов, имеющих одинаковый состав символов. По аналогии с единичным кубом E_2^k мы называем такие подмножества *слоями*. Совокупность всех слоев в $E_t^k \setminus C_t^k$ обозначается нами через $\mathscr{B}_t^k$. Очевидно, что каждый слой B из $\mathscr{B}_t^k$ определяется набором целых чисел $k_0, k_1, \ldots, k_{t-1}$ таких, что $0 \leqslant k_i < k$ и $\sum_{i=0}^{t-1} k_i = k$, где k_i, $i = 0, 1, \ldots, t-1$, равно количеству символов i в каждом из наборов слоя B. В дальнейшем мы будем обозначать число k_i через $B|i|$. Отметим, что слой B содержит $\frac{k!}{k_0! k_1! \ldots k_{t-1}!}$ различных наборов. Индукцией по убыванию величины $\max_i k_i$ нетрудно проверить, что $\frac{k!}{k_0! k_1! \ldots k_{t-1}!} \geqslant k$. Таким образом, получаем

Утверждение 7. *Каждый слой из $\mathscr{B}_t^k$ содержит по крайней мере k различных наборов.*

Следуя стандартной терминологии, мы называем натуральные числа $a_1, a_2, \ldots, a_k$ *попарно простыми*, если каждое из этих чисел взаимно просто с любым другим из них. Множество чисел из $\mathbb{N}^{>1}$ будем называть *разделимым*, если оно содержит меньше двух чисел либо если 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. Пустое множество считается взаимно простым с любым натуральным числом.

Пусть A, B — непустые разделимые множества. Множество B называется *делителем* множества A, если для любого числа b из B множество A содержит число, кратное b. Пустое множество считается делителем любого разделимого множества.

Пусть $A_1, \ldots, A_s$ — конечные разделимые множества. *Наибольшим общим делителем* $(A_1, \ldots, A_s)$ этих множеств мы называем множество

$$\{a \mid a = (a_1, a_2, \ldots, a_s) > 1, \quad a_i \in A_i, \quad i = 1, 2, \ldots, s\},$$

состоящее из больших, чем 1, наибольших общих делителей всевозможных выборок из s чисел по одному числу от каждого из множеств $A_1, \ldots, A_s$.

Если хотя бы одно из множеств $A_1, \ldots, A_s$ является пустым, будем полагать $(A_1, \ldots, A_s) = \varnothing$. Отметим следующие очевидные свойства наибольшего общего делителя разделимых множеств.

Утверждение 8. *Наибольший общий делитель разделимых множеств является разделимым множеством, взаимно простым с любым из чисел, взаимно простых с хотя бы одним из этих множеств.*

Более того, нетрудно убедиться, что $(A_1, \ldots, A_s)$ является делителем каждого из множеств $A_1, \ldots, A_s$, и любой другой делитель каждого из этих множеств является делителем для $(A_1, \ldots, A_s)$. Таким образом, введенное нами понятие наибольшего общего делителя разделимых множеств является естественным обобщением понятия наибольшего общего делителя натуральных чисел. Отметим также ассоциативность операции взятия наибольшего общего делителя разделимых множеств: для любых разделимых множеств A, B, C выполняются равенства

$$((A, B), C) = (A, (B, C)) = (A, B, C).$$

Если множество натуральных чисел A конечно, мы обозначаем через $\|A\|$ произведение всех чисел множества A. Для пустого множества полагаем $\|\varnothing\| = 1$.

Пусть Π — произвольное непустое множество различных простых чисел, T — конечное разделимое множество натуральных чисел, взаимно простых со множеством Π, и a, b — натуральные числа, взаимно простые со множеством Π. Обозначим через $G[\Pi; T]$ следующее подмножество*) множества $G[\Pi]$:

$$\left\{ (d_1; \ldots; d_h) \;\middle|\; \begin{array}{l} d_i = \frac{m_i}{n},\ m_i \in \mathbb{Z}^+,\ i = 1, \ldots, h,\ \sum\limits_{i=1}^{h} d_i = 1,\ n \in \mathbb{N}, \\ \mathscr{J}[n] \subseteq \Pi,\ \exists T_1, \ldots, T_{h-1},\ T \supseteq T_1 \supseteq T_2 \supseteq \ldots \supseteq T_{h-1}, \\ \sum\limits_{j=1}^{i} m_j \equiv 0 \pmod{\|T_i\|},\ i = 1, \ldots, h-1, \\ \sum\limits_{j=1}^{i} m_j \equiv n \pmod{\|T \setminus T_i\|},\ i = 1, \ldots, h-1 \end{array} \right\}.$$

В случае $T = \varnothing$ мы полагаем $G[\Pi; \varnothing] = G[\Pi]$. Заметим, что принадлежность стохастического вектора $(d_1; \ldots; d_h)$ множеству $G[\Pi; T]$ зависит формально от выбора общего знаменателя n его компонент. Однако в [4] показано, что эта зависимость является фиктивной, т. е. для любых двух общих знаменателей n и n' дробей $\frac{m_1}{n} = \frac{m_1'}{n'}, \ldots, \frac{m_h}{n} = \frac{m_h'}{n'}$ таких, что $\mathscr{J}[n], \mathscr{J}[n'] \subseteq \Pi$, соотношение $\left(\frac{m_1'}{n'}, \ldots, \frac{m_h'}{n'}\right) \in G[\Pi; T]$ выполняется тогда и только тогда, когда выполняется соотношение $\left(\frac{m_1}{n}, \ldots, \frac{m_h}{n}\right) \in G[\Pi; T]$. Таким образом, определение множества $G[\Pi; T]$ является корректным по отношению к операции умножения или сокращения числителей и знаменателей дробей на одно и то же число. Отметим также, что любое множество $G[\Pi; T]$ является позитивно замкнутым и содержит все вырожденные стохастические векторы. Кроме того, для множеств $G[\Pi; T]$ справедливо

Утверждение 9. *Множество $G[\Pi'; T']$ содержит множество $G[\Pi''; T'']$, если $\Pi'' \subseteq \Pi'$ и T' является делителем для T''.*

*) Рассматриваемые в данном определении подмножества $T_1 \ldots, T_{h-1}$ множества T могут быть несобственными.

Доказательство. Рассмотрим произвольный вектор $\mathscr{D} = (m_1/n, \ldots, m_h/n)$ из $G[\Pi''; T'']$, где $\mathscr{J}[n] \subseteq \Pi''$ и, следовательно, $\mathscr{J}[n] \subseteq \Pi'$. Тогда существуют подмножества $T_1, \ldots, T_{h-1}$ множества T'' такие, что

$$T_1 \supseteq T_2 \supseteq \ldots \supseteq T_{h-1} \tag{3}$$

и для любого i, $i = 1, \ldots, h-1$, справедливы соотношения

$$\sum_{j=1}^{i} m_j \equiv 0 \pmod{\|T_i\|}, \quad \sum_{j=1}^{i} m_j \equiv n \pmod{\|T'' \setminus T_i\|}. \tag{4}$$

Для каждого множества T_i обозначим через T_i' подмножество множества T', состоящее из всех тех чисел, которые являются делителями чисел из T_i. Таким образом, все числа из T_i' являются делителями числа $\|T_i\|$. Так как все числа из разделимого множества T' являются попарно простыми, получаем, что $\|T_i\|$ делится на $\|T_i'\|$. Поскольку все числа из $T' \setminus T_i'$ являются делителями чисел из $T'' \setminus T_i$, аналогичным образом можно показать, что $\|T'' \setminus T_i\|$ делится на $\|T' \setminus T_i'\|$. Таким образом, из соотношений (4) вытекают соотношения

$$\sum_{j=1}^{i} m_j \equiv 0 \pmod{\|T_i'\|}, \quad \sum_{j=1}^{i} m_j \equiv n \pmod{\|T' \setminus T_i'\|},$$

и из (3) следует, что $T_1' \supseteq T_2' \supseteq \ldots \supseteq T_{h-1}'$. Поэтому $\mathscr{D} \in G[\Pi'; T']$.

§ 3. Вспомогательные теоретико-числовые утверждения

Утверждение 10. *Если $(n, m) = 1$ и x пробегает полную систему вычетов по модулю m, то $nx + n'$, где n' — любое целое, тоже пробегает полную систему вычетов по модулю m.*

Доказательство утверждения 10 приведено в [2].

Рассмотрим сравнение первой степени с одним неизвестным

$$nx \equiv b \pmod{m}. \tag{5}$$

Из утверждения 10 вытекает разрешимость этого сравнения в случае $(n, m) = 1$.

Лемма 1. *Сравнение* (5) *является разрешимым в случае* $(n, m) = 1$.

Отметим, что сравнение (5) эквивалентно уравнению $nx + my = b$ для двух целочисленных неизвестных x и y. Таким образом, из леммы 1 следует, что в случае $(n, m) = 1$ данное уравнение всегда разрешимо в целых числах. Следующее утверждение является обобщением этого факта на случай произвольных положительных n и m.

Утверждение 11. *Если $n, m \in \boldsymbol{N}$ и b делится на (n, m), то уравнение $nx + my = b$ разрешимо в целых числах.*

Утверждение 11 может быть обобщено на случай уравнения с произвольным числом переменных

$$n_1 x_1 + \ldots + n_t x_t = b, \tag{6}$$

где $n_1, \ldots, n_t \in \boldsymbol{N}$ и $b \in \boldsymbol{Z}$.

Утверждение 12. *Если b делится на $(n_1, \ldots, n_t)$, то уравнение* (6) *разрешимо в целых числах.*

Доказательство. Докажем данное утверждение индукцией по t. Базисом индукции для $t=2$ служит утверждение 11. Предположим, что утверждение 12 справедливо для некоторого $t \geqslant 2$. Пусть $n_1, \ldots, n_{t+1} \in \boldsymbol{N}$ и b делится на $(n_1, \ldots, n_{t+1})$. Поскольку $(n_1, \ldots, n_{t+1}) = ((n_1, \ldots, n_t), n_{t+1})$, согласно утверждению 11 существуют целые x', x'' такие, что $b = (n_1, \ldots, n_t)x' + n_{t+1}x''$. По индуктивному предположению существуют целые $x_1, \ldots, x_t$ такие, что $(n_1, \ldots, n_t)x' = n_1x_1 + \ldots + n_tx_t$. Таким образом, $b = n_1x_1 + \ldots + n_tx_t + n_{t+1}x''$.

В дальнейшем для удобства любое решение $x_1 = \alpha_1, \ldots, x_t = \alpha_t$ уравнения (6) будем обозначать вектором $(\alpha_1; \ldots; \alpha_t)$ и будем предполагать, что n_1 является максимальным среди натуральных чисел $n_1, \ldots, n_t$. В этом случае утверждение 12 может быть усилено следующим образом.

Утверждение 13. *Если b делится на $(n_1, \ldots, n_t)$, то уравнение* (6) *имеет целочисленное решение $(\alpha_1; \ldots; \alpha_t)$ такое, что*

$$\max_i \alpha_i - \min_i \alpha_i \leqslant n_1. \tag{7}$$

Доказательство. Отметим, что, если b кратно $(n_1, \ldots, n_t)$, то согласно утверждению 12 уравнение (6) имеет хотя бы одно целочисленное решение, и для любого целочисленного решения $(\beta_1; \ldots; \beta_t)$ этого уравнения имеется лишь конечное число других целочисленных решений $(\beta_1'; \ldots; \beta_t')$ таких, что $\max_i \beta_i' - \min_i \beta_i' < \max_i \beta_i - \min_i \beta_i$. Поэтому найдется целочисленное решение $(\alpha_1; \ldots; \alpha_t)$ с минимальной разностью $\max_i \alpha_i - \min_i \alpha_i$. Предположим, что

$$\max_i \alpha_i - \min_i \alpha_i > n_1 = \max_i n_i. \tag{8}$$

Пусть среди чисел $\alpha_1, \ldots, \alpha_t$ максимальным являются числа $\alpha_{i'(1)}, \ldots, \alpha_{i'(\mu)}$, а минимальными — числа $\alpha_{i''(1)}, \ldots, \alpha_{i''(\nu)}$. Рассмотрим случай $\mu \geqslant \nu$. Для $i = 1, \ldots, t$ положим

$$\alpha_i' = \begin{cases} \alpha_i - n_{i''(j)}, & \text{если } i = i'(j), \quad j = 1, \ldots, \nu, \\ \alpha_i + n_{i'(j)}, & \text{если } i = i''(j), \quad j = 1, \ldots, \nu, \\ \alpha_i & \text{в остальных случаях.} \end{cases}$$

Заметим, что $(\alpha_1'; \ldots; \alpha_t')$ также является целочисленным решением уравнения (6). Учитывая неравенство (8), нетрудно проверить, что любое число α_i' удовлетворяет неравенствам $\min_i \alpha_i < \alpha_i' \leqslant \max_i \alpha_i$. Таким образом, имеем неравенство $\max_i \alpha_i' - \min_i \alpha_i' < \max_i \alpha_i - \min_i \alpha_i$, противоречащее минимальности разности $\max_i \alpha_i - \min_i \alpha_i$. Аналогичным образом получаем противоречие в случае $\mu < \nu$. Поэтому $(\alpha_1; \ldots; \alpha_t)$ удовлетворяет соотношению (7).

Следствие 1. *Если b делится на $(n_1, \ldots, n_t)$ и $b \geqslant n_1 \sum_{i=1}^{t} n_i$, то уравнение* (6) *имеет целочисленное решение $(\alpha_1; \ldots; \alpha_t)$ такое, что любое число α_i удовлетворяет неравенствам*

$$0 < \alpha_i \leqslant \frac{b}{\sum_{i=1}^{t} n_i} + n_1.$$

Доказательство. Если b кратно $(n_1, \ldots, n_t)$, то согласно утверждению 13 уравнение (6) имеет целочисленное решение $(\alpha_1; \ldots; \alpha_t)$, удовлетворяющее соотношению (7). Предположим, что $\alpha_j \leqslant 0$ для некоторого j. Тогда из соотношения (7) следует, что $\alpha_i \leqslant \alpha_j + n_1 \leqslant n_1$ для любого i,

$i = 1, \ldots, t$. Поэтому

$$\sum_i n_i \alpha_i \leqslant \sum_{i \neq j} n_i n_1 < n_1 \sum_i n_i \leqslant b.$$

Следовательно, в этом случае $(\alpha_1; \ldots; \alpha_t)$ не может быть решением уравнения (6). Предположим теперь, что $\max\limits_i \alpha_i > \frac{b}{\sum\limits_i n_i} + n_1$. Тогда из соотношения (7) вытекаетет, что $\alpha_i > \frac{b}{\sum\limits_i n_i}$ для любого $i = 1, \ldots, t$. Поэтому $\sum\limits_i n_i \alpha_i > b$. Следовательно, в этом случае мы снова получаем противоречие с тем, что $(\alpha_1; \ldots; \alpha_t)$ является решением уравнения (6). Таким образом, все числа α_i удовлетворяют требуемым неравенствам.

Будем теперь дополнительно предполагать, что $t \geqslant 3$ и $(n_1, \ldots, n_t) = 1$. Для $i = 1, 2, \ldots, t$ обозначим через λ_i наибольший общий делитель всех чисел $n_1, \ldots, n_t$, кроме числа n_i, и положим $\lambda = \lambda_1 \lambda_2 \ldots \lambda_t$. Отметим, что для любых чисел λ_i и λ_j, где $i \neq j$, имеем $(\lambda_i, \lambda_j) = (n_1, \ldots, n_t) = 1$, поэтому все числа $\lambda_1, \ldots, \lambda_t$ являются попарно простыми.

Пусть $k \in \boldsymbol{N}^{>1}$. Обозначим через d наибольший общий делитель всех чисел $n_u^k n_v$, где $u = 2, 3, \ldots, t$, $v = 1, 2, \ldots, t$ и $v \neq u$. Обозначив через $d^{(u)}$ наибольший общий делитель чисел $n_u^k n_v$, где $v = 1, 2, \ldots, t$ и $v \neq u$, равный числу $n_u^k \lambda_u$, получим, что $d = (d^{(2)}, d^{(3)}, \ldots, d^{(t)}) = (n_2^k \lambda_2, n_3^k \lambda_3, \ldots, n_t^k \lambda_t)$. Следовательно, d является общим делителем чисел $n_2^k \lambda_2 \ldots \lambda_t$, $n_3^k \lambda_2 \ldots$ $\ldots \lambda_t, \ldots, n_t^k \lambda_2 \ldots \lambda_t$, поэтому d является делителем числа

$$(n_2^k \lambda_2 \ldots \lambda_t, n_3^k \lambda_2 \ldots \lambda_t, \ldots, n_t^k \lambda_2 \ldots \lambda_t) = \\ = (n_2^k, n_3^k, \ldots, n_t^k) \lambda_2 \ldots \lambda_t = \lambda_1^k \lambda_2 \ldots \lambda_t.$$

С другой стороны, каждое из чисел $\lambda_1^k, \lambda_2, \ldots, \lambda_t$ является общим делителем чисел $d^{(2)}, d^{(3)}, \ldots, d^{(t)}$, и, следовательно, является делителем числа d. Поскольку числа $\lambda_1^k, \lambda_2, \ldots, \lambda_t$ являются попарно простыми, то получаем, что $\lambda_1^k \lambda_2 \ldots \lambda_t$ является делителем числа d. Таким образом, $d = \lambda_1^k \lambda_2 \ldots \lambda_t = \lambda_1^{k-1} \lambda$.

Утверждение 14. *Для любого целого b, кратного числу λ, найдутся целые неотрицательные числа α_v^u, где $u, v = 2, 3, \ldots, t$ и $u \neq v$, такие, что $\alpha_v^u < n_1$ и выполняется соотношение*

$$b \equiv \sum_{\substack{u, v = 2, 3, \ldots, t \\ u \neq v}} \alpha_v^u n_u^k n_v \pmod{n_1 \lambda_1}.$$

Доказательство. Поскольку числа $\lambda_2, \ldots, \lambda_t$ являются попарно простыми делителями числа n_1, то n_1 делится на $\lambda_2 \ldots \lambda_t$. Пусть $n_1 = n_1' \lambda_2 \ldots \lambda_t$ и $b = n' \lambda$. Рассмотрим сравнение $\lambda_1^{k-1} x \equiv n' \pmod{n_1'}$. Так как $(n_1, \lambda_1) = (n_1, n_2, \ldots, n_t) = 1$, то $(n_1', \lambda_1^{k-1}) = 1$, поэтому согласно лемме 1 это сравнение является разрешимым. Пусть $x = \beta$ — произвольное решение этого сравнения. Согласно утверждению 12 существуют целые числа α_v^u, где $u = 2, 3, \ldots, t$, $v = 1, 2, \ldots, t$ и $v \neq u$, такие, что

$$\beta \lambda_1^{k-1} \lambda = \beta d = \sum_{u=2}^{t} \sum_{\substack{v=1 \\ v \neq u}}^{t} \alpha_v^u n_u^k n_v. \tag{9}$$

Так как для любых $u, v = 2, 3, \ldots, t$ коэффициент α_v^u в сумме (9) может быть заменен на любое сравнимое с ним по модулю n_1 число за счет

соответствующего изменения коэффициента α_1^u, мы можем полагать в сумме (9) все коэффициенты α_v^u, где $v \neq 1$, удовлетворяющими неравенствам $0 \leqslant \alpha_v^u < n_1$. Положим теперь

$$b' = \sum_{\substack{u,\, v = 2, 3, \ldots, t \\ u \neq v}} \alpha_v^u n_u^k n_v = \beta \lambda_1^{k-1} \lambda - \sum_{u=2}^{t} \alpha_1^u n_u^k n_1.$$

Так как каждое из чисел $n_1 n_2^k, \ldots, n_1 n_t^k$ является кратным числу $n_1 \lambda_1^k$, то $b' \equiv \beta \lambda_1^{k-1} \lambda \pmod{n_1 \lambda_1^k}$. Мы также имеем $\beta \lambda_1^{k-1} \lambda \equiv (n' \lambda = b) \pmod{n_1' \lambda = n_1 \lambda_1}$. Таким образом, $b' \equiv b \pmod{n_1 \lambda_1}$.

Аналогично утверждению 14 докажем

Утверждение 15. *Для любого целого b, кратного числу $\lambda' = \lambda_2 \ldots \lambda_t$, найдутся целые неотрицательные числа α_v^u, где $u, v = 2, 3, \ldots, t$ и $u \neq v$, такие, что $\alpha_v^u < n_1$ и выполняется соотношение*

$$b \equiv \sum_{\substack{u,\, v = 2, 3, \ldots, t \\ u \neq v}} \alpha_v^u n_u^k n_v \pmod{n_1}.$$

Доказательство. Пусть $n_1 = n_1' \lambda'$ и $b = n' \lambda'$. Рассмотрим произвольное решение $x = \beta$ сравнения $\lambda_1^k x \equiv n' \pmod{n_1'}$. Согласно утверждению 12 существуют целые числа α_v^u, где $u = 2, 3, \ldots, t$, $v = 1, 2, \ldots, t$ и $v \neq u$, такие, что

$$\beta \lambda_1^k \lambda' = \beta d = \sum_{u=2}^{t} \sum_{\substack{v=1 \\ v \neq u}}^{t} \alpha_v^u n_u^k n_v.$$

В этой сумме так же, как в сумме (9), мы можем полагать $0 \leqslant \alpha_v^u < n_1$ для $v \neq 1$. Положим теперь

$$b' = \sum_{\substack{u,\, v = 2, 3, \ldots, t \\ u \neq v}} \alpha_v^u n_u^k n_v = \beta \lambda_1^k \lambda' - \sum_{u=2}^{t} \alpha_1^u n_u^k n_1.$$

Из последнего равенства вытекает, что $b' \equiv \beta \lambda_1^k \lambda' \pmod{n_1}$. Кроме того, $\beta \lambda_1^k \lambda' \equiv (n' \lambda' = b) \pmod{n_1' \lambda' = n_1}$. Таким образом, $b' \equiv b \pmod{n_1}$.

Пусть $k \geqslant 2$ и $s \in \{1, \ldots, k-1\}$. Обозначим через d_s наибольший общий делитель всех чисел $n_1^s n_u^{k-s} n_v$, где $u, v = 2, 3, \ldots, t$. Обозначив через $d_s^{(u)}$ наибольший общий делитель чисел $n_1^s n_u^{k-s} n_v$, где $v = 2, 3, \ldots, t$, равный числу $n_1^s n_u^{k-s} \lambda_1$, получим, что

$$d_s = (d_s^{(2)}, d_s^{(3)}, \ldots, d_s^{(t)}) = n_1^s \lambda_1 (n_2^{k-s}, n_3^{k-s}, \ldots, n_t^{k-s}) = n_1^s \lambda_1^{k-s+1}.$$

Утверждение 16. *Пусть для любых $u, v = 2, 3, \ldots, t$ имеется полная система J_v^u вычетов по модулю n_1. Для любого целого b, кратного числу $n_1^s \lambda_1$, найдутся целые числа β_v^u, где $u, v = 2, 3, \ldots, t$, такие, что $\beta_v^u \in J_v^u$ и выполняется соотношение*

$$b \equiv \sum_{u,\, v=2}^{t} \beta_v^u n_1^s n_u^{k-s} n_v \pmod{n_1^{s+1} \lambda_1}.$$

Доказательство. Пусть $b = n' n_1^s \lambda_1$. Рассмотрим сравнение $\lambda_1^{k-s} x \equiv n' \pmod{n_1}$. Так как $(n_1', \lambda_1^{k-s}) = 1$, то согласно лемме 1 это сравнение имеет решение. Пусть $x = \beta$ — произвольное решение этого сравнения.

Согласно утверждению 12 существуют целые числа α_v^u, где $u, v = 2, 3, \ldots, t$, такие, что

$$\beta n_1^s \lambda_1^{k-s+1} = \beta d_s = \sum_{u,\, v=2}^{t} \alpha_v^u n_1^s n_u^{k-s} n_v.$$

Для каждого α_v^u существует β_v^u такой, что $\beta_v^u \equiv \alpha_v^u \pmod{n_1}$ и $\beta_v^u \in J_v^u$. Пусть $b' = \sum_{u,\, v=2}^{t} \beta_v^u n_1^s n_u^{k-s} n_v$. Поскольку для любых $u, v = 2, 3, \ldots, t$ число $n_1^s n_u^{k-s} n_v$ делится на $n_1^s \lambda_1^{k-s+1}$, то из $\beta_v^u \equiv \alpha_v^u \pmod{n_1}$ следует $\beta_v^u n_1^s n_u^{k-s} n_v \equiv \alpha_v^u n_1^s n_u^{k-s} n_v \pmod{n_1^{s+1} \lambda_1^{k-s+1}}$. Поэтому $b' \equiv \beta n_1^s \lambda_1^{k-s+1} \pmod{n_1^{s+1} \lambda_1^{k-s+1}}$. С другой стороны, $\beta n_1^s \lambda_1^{k-s+1} \equiv \equiv (n' n_1^s \lambda_1 = b) \pmod{n_1^{s+1} \lambda_1}$. Таким образом, $b' \equiv b \pmod{n_1^{s+1} \lambda_1}$.

Аналогично утверждению 16 докажем

Утверждение 17. *Пусть для любых $u, v = 2, 3, \ldots, t$ имеется полная система J_v^u вычетов по модулю n_1. Для любого целого b, кратного числу n_1^s, найдутся целые числа β_v^u, где $u, v = 2, 3, \ldots, t$, такие, что $\beta_v^u \in J_v^u$ и выполняется соотношение*

$$b \equiv \sum_{u,\, v=2}^{t} \beta_v^u n_1^s n_u^{k-s} n_v \pmod{n_1^{s+1}}.$$

Доказательство. Пусть $b = n' n_1^s$ и $x = \beta$ — произвольное решение сравнения $\lambda_1^{k-s+1} x \equiv n' \pmod{n_1}$. Согласно утверждению 12 существуют целые числа α_v^u, где $u, v = 2, 3, \ldots, t$, такие, что

$$\beta n_1^s \lambda_1^{k-s+1} = \beta d_s = \sum_{u,\, v=2}^{t} \alpha_v^u n_1^s n_u^{k-s} n_v.$$

Пусть $b' = \sum_{u,\, v=2}^{t} \beta_v^u n_1^s n_u^{k-s} n_v$, где $\beta_v^u \equiv \alpha_v^u \pmod{n_1}$ и $\beta_v^u \in J_v^u$. Тогда $b' \equiv \equiv \beta n_1^s \lambda_1^{k-s+1} \pmod{n_1^{s+1} \lambda_1^{k-s+1}}$. Таким образом, поскольку $\beta n_1^s \lambda_1^{k-s+1} \equiv \equiv (n' n_1^s = b) \pmod{n_1^{s+1}}$, то $b' \equiv b \pmod{n_1^{s+1}}$.

Используя упрощенную модификацию доказательства утверждения 17, мы можем также доказать

Утверждение 18. *Пусть для любого $v = 2, 3, \ldots, t$ имеется полная система J_v вычетов по модулю n_1. Для любого целого b, кратного числу n_1^k, найдутся целые числа β_v, где $v = 2, 3, \ldots, t$, такие, что $\beta_v \in J_v$ и выполняется соотношение*

$$b \equiv \sum_{v=2}^{t} \beta_v n_1^k n_v \pmod{n_1^{k+1}}.$$

§ 4. Порождение стохастических векторов одноэлементными множествами

Отметим, что в силу утверждения 3 для описания замыканий всех конечных множеств стохастических векторов нам достаточно рассмотреть замыкания конечных множеств позитивных векторов.

Выделим сначала случай замыканий одноэлементных множеств стохастических векторов. Пусть $\mathcal{D} = (d_1; \ldots; d_t)$ — произвольный позитивный

вектор из $\boldsymbol{Q}(0, 1)$. Без ограничения общности мы предполагаем, что компоненты вектора $\mathscr{D}$ представлены дробями, приведенными к наименьшему общему знаменателю n, т. е. $d_i = m_i/n$, где $i = 1, \ldots, t$ и $(m_1, \ldots, m_t) = 1$. Положим $\Pi(\mathscr{D}) = \mathscr{J}(n)$. Для $j = 1, \ldots, t$ обозначим через l_j наибольший общий делитель всех чисел $m_1, \ldots, m_t$, кроме числа m_j (в случае $t = 2$ мы полагаем $l_1 = m_2$ и $l_2 = m_1$). Обозначим через $T(\mathscr{D})$ множество $\{l_1, \ldots, l_t\}^{>1}$. Положим $l = \|T(\mathscr{D})\|$.

Утверждение 19. *Множество $T(\mathscr{D})$ является разделимым и взаимно простым с числом n.*

Доказательство. Пусть l_j — произвольное число из $T(\mathscr{D})$. Тогда число $\xi = (l_j, n)$ является делителем числа n и всех чисел m_i, где $i \neq j$. Следовательно, ξ является делителем числа $m_j = n - \sum\limits_{i \neq j} m_i$. Таким образом, ξ является общим делителем всех чисел $m_1, \ldots, m_t$. Поэтому из $(m_1, \ldots, m_t) = 1$ следует, что $(l_j, n) = 1$. Кроме того, заметим, что для любых двух различных чисел $l_{j'}$, $l_{j''}$ из $T(\mathscr{D})$ имеем $(l_{j'}, l_{j''}) = (m_1, \ldots, m_t) = 1$.

В силу утверждения 19 можно рассмотреть множество $G[\Pi(\mathscr{D}); T(\mathscr{D})]$. В [4] доказан следующий факт.

Лемма 2. *Для любого позитивного вектора $\mathscr{D} \in \boldsymbol{Q}(0, 1)$ размерности 2 справедливо соотношение*

$$G[\Pi(\mathscr{D}); T(\mathscr{D})] \subseteq \langle\{\mathscr{D}\}\rangle. \tag{10}$$

Докажем, что соотношение (10) справедливо также для $t > 2$. Рассмотрим отдельно два различных случая в зависимости от количества максимальных элементов среди чисел $m_1, m_2, \ldots, m_t$.

Лемма 3. *Пусть среди чисел $m_1, m_2, \ldots, m_t$, где $t \geqslant 3$, имеется единственный максимальный элемент. Тогда $G[\Pi(\mathscr{D}); T(\mathscr{D})] \subseteq \langle\{\mathscr{D}\}\langle\{\mathscr{D}\}\rangle\rangle$.*

Доказательство. В силу утверждения 2 без ограничения общности мы можем полагать, что $m_1 > m_2 \geqslant m_3 \geqslant \ldots \geqslant m_t$. Пусть $\widehat{\mathscr{D}} = (\widehat{d}_1; \ldots; \widehat{d}_h)$ — произвольный позитивный вектор из $G[\Pi(\mathscr{D}); T(\mathscr{D})]$. Положим $\Delta = \min(\widehat{d}_1, \ldots, \widehat{d}_h)$. Пусть $\widehat{n}$ — общий знаменатель компонент вектора $\widehat{\mathscr{D}}$ такой, что $\mathscr{J}(\widehat{n}) \subseteq \Pi(\mathscr{D})$. Так как $\Pi(\mathscr{D}) = \mathscr{J}(n)$, то $\widehat{n}$ является делителем некоторой достаточно большой степени n^{k_0} числа n. Обозначим через k достаточно большое натуральное число, не меньшее, чем k_0, и удовлетворяющее неравенствам

$$k \geqslant (h - 1)tm_1m_2, \tag{11}$$

$$\left(\frac{m_1}{n}\right)^k < \frac{\Delta}{2t(n - m_1)m_2}, \tag{12}$$

$$\left(\frac{m_1}{n}\right)^k < \frac{\widehat{d}_h}{2m_1m_2^2}. \tag{13}$$

Будем также предполагать $k \geqslant 3$. Пусть $\widehat{d}_i = \frac{\widehat{m}_i}{n^k}$, где $i = 1, \ldots, h$. Положим $\mu_0 = 0$ и $\mu_i = \sum\limits_{j=1}^{i} \widehat{m}_j$ для $i = 1, \ldots, h - 1$. Так как $\widehat{\mathscr{D}} \in G[\Pi(\mathscr{D}); T(\mathscr{D})]$, то существуют подмножества $T_1 \supseteq T_2 \supseteq \ldots \supseteq T_{h-1}$ множества $T(\mathscr{D})$ такие, что для любого $i = 1, \ldots, h - 1$ справедливы соотношения

$$\mu_i \equiv 0 \pmod{\|T_i\|}, \quad \mu_i \equiv n^k \pmod{\|T(\mathscr{D}) \setminus T_i\|}. \tag{14}$$

Положив $T_0 = T(\mathscr{D})$, получим, что соотношения (14) справедливы также для $i = 0$, и, кроме того, имеем

$$T_0 \supseteq T_1 \supseteq \ldots \supseteq T_{h-1}. \tag{15}$$

Для любого множества U наборов из E_t^k обозначим $n^k \boldsymbol{P}_U(\underbrace{\mathscr{D}, \ldots, \mathscr{D}}_{k})$ через $\mathscr{M}(U)$. Из утверждения 6 следует, что $\mathscr{M}(\bigcup_{i=1}^{s} U_i) = \sum_{i=1}^{s} \mathscr{M}(U_i)$ для любых непересекающихся множеств $U_1, \ldots, U_s \subseteq E_t^k$. Для любого неоднородного набора $\tilde{\sigma} \in E_t^k$ из формулы (1) можно получить, что

$$\mathscr{M}(\{\tilde{\sigma}\}) = m_1^{B|0|} m_2^{B|1|} \ldots m_t^{B|t-1|}, \tag{16}$$

где B — слой множества E_t^k, содержащий $\tilde{\sigma}$. В случае однородного набора $\tilde{\sigma} = (i; \ldots; i)$ из E_t^k согласно формуле (1) получаем, что

$$\mathscr{M}(\{\tilde{\sigma}\}) = m_{i+1}^k. \tag{17}$$

Таким образом, величина $\mathscr{M}(U)$ может быть вычислена по следующей формуле:

$$\mathscr{M}(U) = \sum_{\tilde{\sigma} \in U} \mathscr{M}(\{\tilde{\sigma}\}) = \sum_{(i; \ldots; i) \in U \cap C_t^k} m_{i+1}^k + \sum_{B \in \mathscr{B}_t^k} |U \cap B| m_1^{B|0|} m_2^{B|1|} \ldots m_t^{B|t-1|}. \tag{18}$$

Отметим, что, если множество U состоит только из однородных наборов, то тогда

$$\mathscr{M}(U) = \sum_{(i; \ldots; i) \in U} m_{i+1}^k \leqslant \sum_{i=1}^{t} m_i^k < t m_1^k. \tag{19}$$

Из формулы (18) также вытекает, что для любых двух подмножеств U, V множества E_t^k, содержащих одни и те же однородные наборы, справедливо равенство

$$\mathscr{M}(V) = \mathscr{M}(U) + \sum_{B \in \mathscr{B}_t^k} \lambda_B m_1^{B|0|} m_2^{B|1|} \ldots m_t^{B|t-1|}, \tag{20}$$

где $\lambda_B = |V \cap B| - |U \cap B|$. Кроме того, при доказательстве леммы мы будем пользоваться очевидным равенством $\sum_{j=2}^{t} m_j = n - m_1$.

Слой B множества E_t^k будем называть слоем i-го уровня, где $i = 0, 1, \ldots, k-1$, если B состоит из наборов, содержащих ровно i символов 0. Для $j = 2, 3, \ldots, t$ обозначим через B_{k-1}^j слой $(k-1)$-го уровня из наборов, содержащих $k-1$ символов 0 и один символ $j-1$. Для $i = 0, \ldots, k-2$ и $j, s = 2, 3, \ldots, t$, где $j \neq s$, обозначим через $B_i^{j,s}$ слой i-го уровня из наборов, содержащих помимо символов 0 ровно один символ $s-1$ и $k-i-1$ символов $j-1$ (и соответственно не содержащих никаких других символов). В случае $i = 1, \ldots, k-2$ и $j = s = 2, 3, \ldots, t$ через $B_i^{j,s}$ будем обозначать слой i-го уровня из наборов, содержащих i символов 0 и $k-i$ символов $j-1$. Все обозначенные нами слои будем называть специальными слоями. Согласно утверждению 7 и неравенству (11) в каждом слое множества E_t^k содержится не менее $(h-1)tm_1m_2$ наборов. Поэтому в каждом из слоев $B_{k-1}^1, \ldots, B_{k-1}^{t-1}$ мы можем выделить по $(h-1)tm_1m_2$ различных наборов, приписав каждому из этих наборов некоторый целочисленный ранг

от 1 до $h-1$ так, чтобы в любом из этих слоев содержалось ровно по tm_1m_2 различных наборов каждого ранга. Аналогичным образом мы можем приписать ранги от 1 до $h-1$ наборам всех остальных специальных слоев от нулевого до $k-2$-го уровня так, чтобы в каждом из этих слоев содержалось ровно по m_1 различных наборов каждого ранга. Всем остальным неоднородным наборам множества E_t^k припишем ранг 0. Согласно формуле (16) для любого набора $\tilde{\sigma}$ из слоя i-го уровня, где $i=0, 1, \ldots, k-1$, величина $\mathcal{M}(\{\tilde{\sigma}\})$ делится на m_1^i, т. е. $\mathcal{M}(\{\tilde{\sigma}\})/m_1^i$ является целым числом. Исходя из этого наблюдения, мы разбиваем все неоднородные наборы множества E_t^k на категории $0, 1, \ldots, m_1-1$ следующим образом: неоднородный набор $\tilde{\sigma}$ из слоя i-го уровня принадлежит категории j, если $\mathcal{M}(\{\tilde{\sigma}\})/m_1^i \equiv j \pmod{m_1}$.

Рассмотрим произвольный однородный набор $(i; i; \ldots; i)$ из E_t^k. Если $l_{i+1} > 1$, то $l_{i+1} \in T(\mathcal{D}) = T_0$, т. е. среди множеств $T_0, T_1, \ldots, T_{h-1}$ по крайней мере множество T_0 содержит $l_{i+1} > 1$. Поэтому среди этих множеств найдется содержащее число l_{i+1} множество с максимальным порядковым индексом. Обозначим этот порядковый индекс через $\chi(i)$. В случае $l_{i+1}=1$ положим $\chi(i)=0$. Разобьем множество C_t^k на непересекающиеся подмножества $U_0^0, U_1^0, \ldots, U_{h-1}^0$, где U_j^0 состоит из всех однородных наборов $(i; i; \ldots; i)$ таких, что $\chi(i)=j$. Покажем, что для любого $j=0, 1, \ldots, h-2$ и любого l_i из $T(\mathcal{D})$ выполняется соотношение

$$\mathcal{M}(U_j^0) \equiv \widehat{m}_{j+1} \pmod{l_i}. \tag{21}$$

Для этого выделим три возможных случая.

а) Пусть $j < \chi(i-1)$. Тогда из соотношений (15) вытекает $T_{\chi(i-1)} \subseteq T_{j+1} \subseteq T_j$. Поэтому, учитывая, что $l_i \in T_{\chi(i-1)}$, имеем $l_i \in T_{j+1} \subseteq T_j$. Следовательно, из соотношений (14) получаем, что $\mu_j \equiv 0 \pmod{l_i}$ и $\mu_{j+1} \equiv 0 \pmod{l_i}$. Таким образом, $\widehat{m}_{j+1} = \mu_{j+1} - \mu_j \equiv 0 \pmod{l_i}$. Заметим, что l_i является делителем всех чисел $m_1, \ldots, m_h$, кроме числа m_i, поэтому согласно формуле (17) величина $\mathcal{M}(\{\tilde{\sigma}\})$ делится на l_i для любого однородного набора $\tilde{\sigma}$, отличного от $(i-1; i-1; \ldots; i-1)$. Так как $j \neq \chi(i-1)$, то $(i-1; i-1; \ldots; i-1) \notin U_j^0$. Таким образом, в сумме $\sum\limits_{\tilde{\sigma} \in U_j^0} \mathcal{M}(\{\tilde{\sigma}\})$, равной $\mathcal{M}(U_j^0)$, все слагаемые делятся на l_i. Следовательно, $\mathcal{M}(U_j^0) \equiv 0 \pmod{l_i}$. Сопоставив это сравнение со сравнением $\widehat{m}_{j+1} \equiv 0 \pmod{l_i}$, получим соотношение (21).

б) Пусть $j = \chi(i-1)$. Тогда $l_i \in T_j$ и $l_i \notin T_{j+1}$, т. е. $l_i \in T(\mathcal{D}) \setminus T_{j+1}$. Поэтому согласно соотношениям (14) имеем $\mu_j \equiv 0 \pmod{l_i}$ и $\mu_{j+1} \equiv n^k \pmod{l_i}$. Следовательно, $\widehat{m}_{j+1} = \mu_{j+1} - \mu_j \equiv n^k \pmod{l_i}$. Кроме того, мы имеем, что однородный набор $(i-1; i-1; \ldots; i-1)$ содержится в U_j^0. Поскольку для любого другого однородного набора $\tilde{\sigma}$ величина $\mathcal{M}(\{\tilde{\sigma}\})$ делится на l_i, то $\mathcal{M}(U_j^0) = \sum\limits_{\tilde{\sigma} \in U_j^0} \mathcal{M}(\{\tilde{\sigma}\}) \equiv \mathcal{M}(\{(i-1; i-1; \ldots; i-1)\}) \pmod{l_i}$. Таким образом, учитывая формулу (17), получаем $\mathcal{M}(U_j^0) \equiv m_i^k \pmod{l_i}$. Так как l_i является делителем всех чисел $m_1, \ldots, m_h$, кроме числа m_i, то l_i является также делителем суммы этих чисел, равной $n - m_i$. Следовательно, поскольку $m_i^k \equiv n^k \pmod{n-m_i}$, то $m_i^k \equiv n^k \pmod{l_i}$. Поэтому $\mathcal{M}(U_j^0) \equiv n^k \pmod{l_i}$. Сопоставив это сравнение со сравнением $\widehat{m}_{j+1} \equiv n^k \pmod{l_i}$, получим соотношение (21).

в) Пусть $j > \chi(i-1)$. Тогда $l_i \notin T_j$. Следовательно, $l_i \notin T_{j+1}$ в силу соотношений (15). Таким образом, l_i содержится в обоих множествах $T(\mathcal{D}) \setminus T_j$ и

$T(\mathscr{D})\setminus T_{j+1}$. Поэтому из соотношений (14) получаем, что $\mu_j \equiv n^k \pmod{l_i}$ и $\mu_{j+1} \equiv n^k \pmod{l_i}$. Следовательно, $\widehat{m}_{j+1} = \mu_{j+1} - \mu_j \equiv 0 \pmod{l_i}$. Поскольку $j \neq \chi(i-1)$, то так же, как и в случае а), имеем $\mathscr{M}(U_j^0) \equiv 0 \pmod{l_i}$. Таким образом, из сравнения $\widehat{m}_{j+1} \equiv 0 \pmod{l_i}$ вытекает соотношение (21).

Поскольку все числа из $T(\mathscr{D})$ попарно просты, из соотношений (21) получаем, что для любого $j = 0, 1, \ldots, h-2$ справедливо соотношение

$$\mathscr{M}(U_j^0) \equiv \widehat{m}_{j+1} \pmod{l}. \tag{22}$$

Мы построим h-значную дискретную функцию $f(x_1, \ldots, x_k)$ такую, что

$$\widehat{\mathscr{D}} = \boldsymbol{P}\{f(\mathscr{D}, \ldots, \mathscr{D})\}. \tag{23}$$

Для этого последовательно зададим непересекающиеся подмножества $\mathscr{N}_0(f), \mathscr{N}_1(f), \ldots, \mathscr{N}_{h-2}(f)$ множества E_t^k, удовлетворяющие равенствам

$$\boldsymbol{P}_{\mathscr{N}_i(f)}(\mathscr{D}, \ldots, \mathscr{D}) = \widehat{d}_{i+1}, \quad i = 0, 1, \ldots, h-2. \tag{24}$$

Домножив обе части этих равенств на n^k, получим, что они эквивалентны равенствам

$$\mathscr{M}\big(\mathscr{N}_i(f)\big) = \widehat{m}_{i+1}, \quad i = 0, 1, \ldots, h-2. \tag{25}$$

В процессе построения множества $\mathscr{N}_i(f)$ будем дополнительно требовать, чтобы оно содержало однородные наборы только из множества U_i^0 и не содержало неоднородных наборов ранга, большего $i+1$.

Пусть $i \in \{0, 1, \ldots, h-2\}$ и в случае $i > 0$ уже построены искомые множества $\mathscr{N}_0(f), \ldots, \mathscr{N}_{i-1}(f)$. Положим *) $\Theta = \bigcup\limits_{j<i} \mathscr{N}_j(f)$. Построим последовательность множеств $U_i^1, \ldots, U_i^{k-1}$ таких, что для каждого $s = 1, \ldots, k-1$ множество U_i^s может содержать только однородные наборы из множества U_i^0 и неоднородные наборы $(i+1)$-го ранга из слоев не более чем $(s-1)$-го уровня и при этом выполняется соотношение

$$\mathscr{M}(U_i^s) \equiv \widehat{m}_{i+1} \pmod{m_1^s l_1}. \tag{26}$$

Из соотношения (22) имеем $\widehat{m}_{i+1} - \mathscr{M}(U_i^0) \equiv 0 \pmod{l}$. Поэтому согласно утверждению 14 найдутся целые неотрицательные числа α_v^u, где $u, v = 2, 3, \ldots, t$ и $u \neq v$, такие, что каждое из этих чисел меньше чем m_1, и выполняется соотношение

$$\widehat{m}_{i+1} - \mathscr{M}(U_i^0) \equiv \sum_{\substack{u, v = 2, 3, \ldots, t \\ u \neq v}} \alpha_v^u m_u^{k-1} m_v \pmod{m_1 l_1}. \tag{27}$$

Для любых $u, v = 2, 3, \ldots, t$, где $u \neq v$, слой $B_0^{u,v}$ содержит ровно m_1 наборов $(i+1)$-го ранга и $m_1 > \alpha_v^u$. Поэтому в каждом таком слое мы можем выбрать α_v^u различных наборов $(i+1)$-го ранга. Возьмем в качестве множества U_i^1 объединение всех этих наборов с наборами множества U_i^0. Тогда согласно формуле (20) получаем

$$\mathscr{M}(U_i^1) = \mathscr{M}(U_i^0) + \sum_{\substack{u, v = 2, 3, \ldots, t \\ u \neq v}} \alpha_v^u m_1^{B_0^{u,v}|0|} m_2^{B_0^{u,v}|1|} \ldots m_t^{B_0^{u,v}|t-1|} =$$

$$= \mathscr{M}(U_i^0) + \sum_{\substack{u, v = 2, 3, \ldots, t \\ u \neq v}} \alpha_v^u m_u^{k-1} m_v.$$

*) В случае $i = 0$ полагаем $\Theta = \varnothing$.

Таким образом, множество U_i^1 в силу соотношения (27) удовлетворяет сравнению (26) и содержит только наборы из U_i^0 и наборы $(i+1)$-го ранга из слоев нулевого уровня. Кроме того, учитывая неравенства $\alpha_v^u < m_1$, получим

$$\mathcal{M}(U_i^1) < \mathcal{M}(U_i^0) + \sum_{\substack{u,\, v = 2,\, 3,\, \ldots,\, t \\ u \neq v}} m_1 m_u^{k-1} m_v.$$

Так как $m_2 \geqslant m_3 \geqslant \ldots \geqslant m_t$, то

$$\sum_{\substack{u,\, v = 2,\, 3,\, \ldots,\, t \\ u \neq v}} m_1 m_u^{k-1} m_v \leqslant \sum_{\substack{u,\, v = 2,\, 3,\, \ldots,\, t \\ u \neq v}} m_1 m_2^{k-1} m_v = (t-2) m_1 m_2^{k-1} (n - m_1). \tag{28}$$

Поэтому

$$\mathcal{M}(U_i^1) < \mathcal{M}(U_i^0) + (t-2) m_1 m_2^{k-1} (n - m_1). \tag{29}$$

Предположим, что для некоторого $s \in \{2, \ldots, k-1\}$ нами уже построено искомое множество U_i^{s-1}. Тогда в силу сравнения (26) имеем $\widehat{m}_{i+1} - \mathcal{M}(U_i^{s-1}) \equiv 0 \pmod{m_1^{s-1} l_1}$. Так как числа $0, 1, \ldots, m_1 - 1$ образуют полную систему вычетов по модулю m_1, то согласно утверждению 16 найдутся целые числа β_v^u, где $u, v = 2, 3, \ldots, t$, удовлетворяющие неравенствам $0 \leqslant \beta_v^u < m_1$ и такие, что

$$\widehat{m}_{i+1} - \mathcal{M}(U_i^{s-1}) \equiv \sum_{u,\, v = 2}^{t} \beta_v^u m_1^{s-1} m_u^{k-s} m_v \pmod{m_1^s l_1}. \tag{30}$$

Поскольку для любых $u, v = 2, 3, \ldots, t$ слой $B_{s-1}^{u,v}$ содержит ровно m_1 наборов $(i+1)$-го ранга и $m_1 > \beta_v^u$, то в каждом таком слое мы можем выбрать β_v^u различных наборов $(i+1)$-го ранга. Возьмем в качестве множества U_i^s объединение всех этих наборов с наборами множества U_i^{s-1}. Тогда согласно формуле (20) получаем

$$\mathcal{M}(U_i^s) = \mathcal{M}(U_i^{s-1}) + \sum_{u,\, v = 2}^{t} \beta_v^u m_1^{B_{s-1}^{u,v}|0|} m_2^{B_{s-1}^{u,v}|1|} \ldots m_t^{B_{s-1}^{u,v}|t-1|} =$$

$$= \mathcal{M}(U_i^{s-1}) + \sum_{u,\, v = 2}^{t} \beta_v^u m_1^{s-1} m_u^{k-s} m_v.$$

Таким образом, множество U_i^s в силу соотношения (30) удовлетворяет сравнению (26) и содержит только наборы из U_i^0 и наборы $(i+1)$-го ранга из слоев не более, чем $(s-1)$-го уровня. Кроме того, учитывая неравенства $\beta_v^u < m_1$, получим

$$\mathcal{M}(U_i^s) < \mathcal{M}(U_i^{s-1}) + \sum_{u,\, v = 2}^{t} m_1^s m_u^{k-s} m_v.$$

Аналогично неравенству (28) имеем

$$\sum_{u,\, v = 2}^{t} m_1^s m_u^{k-s} m_v \leqslant (t-1) m_1^s m_2^{k-s} (n - m_1). \tag{31}$$

Поэтому

$$\mathcal{M}(U_i^s) < \mathcal{M}(U_i^{s-1}) + (t-1) m_1^s m_2^{k-s} (n - m_1). \tag{32}$$

Построим теперь конечную последовательность множеств

$$W_0, W_1, \ldots, W_q \tag{33}$$

так, чтобы эти множества состояли только из однородных наборов множества U_i^0 и не содержащихся в Θ неоднородных наборов не более чем $(i+1)$-го ранга из слоев не более чем $(k-2)$-го уровня и удовлетворяли для каждого $s=0, 1, \ldots, q$ соотношениям

$$\mathcal{M}(W_s) \equiv \widehat{m}_{i+1} \pmod{m_1^{k-1} l_1}. \tag{34}$$

В качестве W_0 возьмем множество U_i^{k-1}. Справедливость соотношения (34) для этого множества непосредственно вытекает из соотношения (26). Исходя из неравенств (29) и (32) мы можем оценить величину $\mathcal{M}(W_0)$:

$$\mathcal{M}(W_0) < \mathcal{M}(U_i^0) + (t-2)m_1 m_2^{k-1}(n-m_1) + \sum_{s=2}^{k-1}(t-1)m_1^s m_2^{k-s}(n-m_1) <$$

$$< \mathcal{M}(U_i^0) + (t-1)(n-m_1)\sum_{s=1}^{k-1} m_1^s m_2^{k-s}. \tag{35}$$

Учитывая, что $m_1 > m_2$, имеем

$$\sum_{s=1}^{k-1} m_1^s m_2^{k-s} = m_1^k \sum_{s=1}^{k-1}\left(\frac{m_2}{m_1}\right)^s < m_1^k \sum_{s=1}^{\infty}\left(\frac{m_2}{m_1}\right)^s = m_1^k \frac{m_2}{m_1 - m_2} \leqslant m_1^k m_2. \tag{36}$$

Поэтому из неравенства (35), используя также справедливое для состоящего только из однородных наборов множества U_i^0 неравенство (19), получаем

$$\mathcal{M}(W_0) < t m_1^k + (t-1)(n-m_1)m_1^k m_2.$$

Поэтому

$$\mathcal{M}(W_0) + (n-m_1)m_1^{k-1}m_2 < t m_1^k + t(n-m_1)m_1^k m_2 \leqslant 2t(n-m_1)m_1^k m_2. \tag{37}$$

Предположим, что для некоторого $r>0$ нами уже построены множества $W_0, \ldots, W_{r-1}$. Если для любого $s=0, 1, \ldots, k-2$ среди не содержащихся в $\Theta \cup W_{r-1}$ наборов не более, чем $(i+1)$-го ранга из слоев s-го уровня не найдется m_1 различных наборов одной и той же категории, то завершим построение искомой последовательности множеств, положив $q=r-1$. В противном случае обозначим через $\tau(r)$ минимальное число s такое, что существуют m_1 не содержащихся в $\Theta \cup W_{r-1}$ наборов не более чем $(i+1)$-го ранга из слоев s-го уровня, принадлежащих одной и той же категории. Множество этих наборов обозначим через V. Так как V состоит из наборов слоев $\tau(r)$-го уровня, то согласно формуле (16) для любого набора $\tilde{\sigma}$ из V величина $\mathcal{M}(\{\tilde{\sigma}\})$ делится на $m_1^{\tau(r)}$. Таким образом, величина $\mathcal{M}(V) = \sum_{\tilde{\sigma} \in V} \mathcal{M}(\{\tilde{\sigma}\})$ также делится на $m_1^{\tau(r)}$ и

$$\mathcal{M}(V)/m_1^{\tau(r)} = \sum_{\tilde{\sigma} \in V} \mathcal{M}(\{\tilde{\sigma}\})/m_1^{\tau(r)}. \tag{38}$$

Поскольку все наборы множества V принадлежат одной и той же категории, сумма (38) представляет собой сумму m_1 чисел, принадлежащих одному и тому же вычету по модулю m_1. Следовательно, эта сумма делится на m_1. Таким образом, $\mathcal{M}(V)$ делится на $m_1^{\tau(r)+1}$. Кроме того, поскольку $(0, 0, \ldots, 0) \notin V$, то согласно формуле (16) для любого набора $\tilde{\sigma}$ из V величина $\mathcal{M}(\{\tilde{\sigma}\})$ делится хотя бы на одно из чисел $m_2, \ldots, m_t$ и, следовательно, делится на l_1. Поэтому величина $\mathcal{M}(V)$ также делится на l_1. Так как

$(m_1, l_1) = (m_1, m_2, \ldots, m_t) = 1$, то из одновременной делимости числа $\mathcal{M}(V)$ на $m_1^{\tau(r)+1}$ и l_1 следует, что

$$\mathcal{M}(V) \equiv 0 \pmod{m_1^{\tau(r)+1} l_1}. \tag{39}$$

Из формулы (16) также вытекает очевидная оценка $\mathcal{M}(\{\widetilde{\sigma}\}) \leqslant m_1^{\tau(r)} m_2^{k-\tau(r)}$ для любого набора $\widetilde{\sigma}$ из V. Поэтому

$$\mathcal{M}(V) \leqslant m_1^{\tau(r)+1} m_2^{k-\tau(r)}. \tag{40}$$

Построим последовательность множеств $V^{\tau(r)+1}, \ldots, V^{k-1}$ так, чтобы эти множества состояли только из однородных наборов множества U_i^0 и не содержащихся в Θ неоднородных наборов не более чем $(i+1)$-го ранга из слоев не более чем $(k-2)$-го уровня и удовлетворяли для каждого $s = \tau(r)+1, \ldots, k-1$ соотношениям

$$\mathcal{M}(V^s) \equiv \widehat{m}_{i+1} \pmod{m_1^s l_1}. \tag{41}$$

В качестве $V^{\tau(r)+1}$ возьмем множество $W_{r-1} \cup V$. Так как для непересекающихся множеств W_{r-1} и V имеем

$$\mathcal{M}(V^{\tau(r)+1}) = \mathcal{M}(W_{r-1}) + \mathcal{M}(V),$$

то справедливость соотношения (41) для $V^{\tau(r)+1}$ вытекает из справедливости соотношения (34) для W_{r-1} и соотношения (39) для V. Кроме того, из (40) получаем оценку

$$\mathcal{M}(V^{\tau(r)+1}) \leqslant \mathcal{M}(W_{r-1}) + m_1^{\tau(r)+1} m_2^{n-\tau(r)}. \tag{42}$$

Предположим теперь, что $\tau(r) < k-2$ и для некоторого $s \in \{\tau(r)+2, \ldots, k-1\}$ уже построено искомое множество V^{s-1}. Тогда в силу сравнения (41) имеем

$$\widehat{m}_{i+1} - \mathcal{M}(V^{s-1}) \equiv 0 \pmod{m_1^{s-1} l_1}.$$

Для $u, v = 2, 3, \ldots, t$ обозначим через γ_v^u количество наборов $(i+1)$-го ранга из слоя $B_{s-1}^{u,v}$, содержащихся в V^{s-1}, и через J_v^u — полную систему $-\gamma_v^u + 1, \ldots, m_1 - \gamma_v^u$ вычетов по модулю m_1. Согласно утверждению 16 найдутся целые числа β_v^u, где $u, v = 2, 3, \ldots, t$, такие, что $\beta_v^u \in J_v^u$ и выполнено соотношение

$$\widehat{m}_{i+1} - \mathcal{M}(V^{s-1}) \equiv \sum_{u,v=2}^{t} \beta_v^u m_1^{s-1} m_u^{k-s} m_v \pmod{m_1^s l_1}. \tag{43}$$

Для каждого из чисел β_v^u выполним над множеством V^{s-1} следующую операцию, зависящую от знака этого числа.

а) Пусть $\beta_v^u > 0$. Поскольку в слое $B_{s-1}^{u,v}$ содержится ровно m_1 наборов $(i+1)$-го ранга и $\beta_v^u \leqslant m_1 - \gamma_v^u$, мы можем выбрать в этом слое β_v^u различных наборов, не содержащихся в V^{s-1}. Добавим к V^{s-1} эти наборы.

б) Пусть $\beta_v^u < 0$. Поскольку в этом случае $|\beta_v^u| < \gamma_v^u$, мы можем в V^{s-1} выбрать $|\beta_v^u|$ различных наборов $(i+1)$-го ранга из слоя $B_{s-1}^{u,v}$. Удалим эти наборы из V^{s-1}. Возьмем в качестве V^s множество, получившееся из V^{s-1} в результате этих операций. Согласно формуле (20) получаем

$$\mathcal{M}(V^s) = \mathcal{M}(V^{s-1}) + \sum_{u,v=2}^{t} \beta_v^u m_1^{s-1} m_u^{k-s} m_v.$$

Из этого равенства и соотношения (43) следует, что V^s удовлетворяет сравнению (41). Кроме того, поскольку каждое из чисел β_v^u удовлетворяет неравенству $\beta_v^u \leqslant m_1$, то аналогично оценке (31) можем получить следующую оценку:

$$\sum_{u,\,v=2}^{t} \beta_v^u m_1^{s-1} m_u^{k-s} m_v \leqslant \sum_{u,\,v=2}^{t} m_1^s m_u^{k-s} m_v \leqslant (t-1) m_1^s m_2^{k-s} \sum_{v=2}^{t} m_v.$$

Поэтому

$$\mathcal{M}(V^s) \leqslant \mathcal{M}(V^{s-1}) + (t-1) m_1^s m_2^{k-s} (n - m_1). \tag{44}$$

Положим $W_r = V^{k-1}$. Тогда справедливость соотношения (34) для W_r непосредственно вытекает из соотношения (41) для V^{k-1}. Отметим также, что если множество W_{r-1} состоит только из однородных наборов множества U_i^0 и не содержащихся в Θ неоднородных наборов не более чем $(i+1)$-го ранга из слоев не более чем $(k-2)$-го уровня, то в силу способа построения этим же свойством обладает множество W_r. Исходя из неравенств (42) и (44) мы можем оценить величину $\mathcal{M}(W_r)$:

$$\mathcal{M}(W_r) \leqslant \mathcal{M}(W_{r-1}) + m_1^{\tau(r)+1} m_2^{k-\tau(r)} + \sum_{s=\tau(r)+2}^{k-1} (t-1) m_1^s m_2^{k-s} (n - m_1) <$$

$$< \mathcal{M}(W_{r-1}) + (t-1) \sum_{s=\tau(r)+1}^{k-1} m_1^s m_2^{k-s} (n - m_1) \leqslant$$

$$\leqslant \mathcal{M}(W_{r-1}) + (t-1)(n - m_1) \sum_{s=1}^{k-1} m_1^s m_2^{k-s}.$$

Из этого соотношения, применяя неравенство (36), получим

$$\mathcal{M}(W_r) < \mathcal{M}(W_{r-1}) + (t-1)(n - m_1) m_1^k m_2. \tag{45}$$

Заметим также, что $\tau(r-1) \leqslant \tau(r)$, и в случае $\tau(r-1) = \tau(r)$ среди наборов из слоев $\tau(r)$-го уровня число наборов, не содержащихся в $\Theta \cup W_r$, строго меньше числа наборов, не содержащихся в $\Theta \cup W_{r-1}$. Поэтому последовательность $\tau(0), \tau(1), \tau(2), \ldots$ монотонно возрастает от 0 до $k-2$, и каждое из чисел $0, \ldots, k-2$ может встретиться в этой последовательности только конечное число раз. Тем самым построение искомой последовательности (33) обязательно завершится.

Пусть S — подмножество всех множеств W_j последовательности (33) таких, что

$$\mathcal{M}(W_j) > \widehat{m}_{i+1} - (n - m_1) m_1^{k-1} m_2.$$

Если S непусто, то выберем в S множество, имеющее минимальный порядковый индекс. Обозначим этот индекс через j^*. Из неравенств (37) и (12) следует, что

$$\mathcal{M}(W_0) + (n - m_1) m_1^{k-1} m_2 < \Delta n^k \leqslant \widehat{d}_{i+1} n^k = \widehat{m}_{i+1}.$$

Поэтому $W_0 \notin S$. Следовательно, $j^* > 1$. Таким образом, мы можем рассмотреть множество W_{j^*-1}. Из соотношений (34) имеем

$$\widehat{m}_{i+1} - \mathcal{M}(W_{j^*-1}) \equiv 0 \pmod{m_1^{k-1} l_1},$$

т. е. $\left(\widehat{m}_{i+1} - \mathcal{M}(W_{j^*-1})\right) / m_1^{k-1}$ является целым числом, кратным числу l_1. При этом, поскольку $W_{j^*-1} \notin S$,

$$\widehat{m}_{i+1} - \mathcal{M}(W_{j^*-1}) \geqslant (n - m_1) m_1^{k-1} m_2$$

и, следовательно,

$$\left(\widehat{m}_{i+1} - \mathcal{M}(W_{j^*-1})\right)/m_1^{k-1} \geqslant (n - m_1)m_2 = m_2 \sum_{v=2}^{t} m_v.$$

Поэтому согласно следствию 1 найдутся положительные числа $\delta_2, \ldots, \delta_t$ такие, что

$$\sum_{v=2}^{t} \delta_v m_v = \left(\widehat{m}_{i+1} - \mathcal{M}(W_{j^*-1})\right)/m_1^{k-1} \tag{46}$$

и

$$\max_{v=2,\ldots,t} \delta_v \leqslant \frac{\widehat{m}_{i+1} - \mathcal{M}(W_{j^*-1})}{m_1^{k-1} \sum\limits_{v=2}^{t} m_v} + m_2. \tag{47}$$

Из неравенства $\mathcal{M}(W_{j^*}) > \widehat{m}_{i+1} - (n - m_1)m_1^{k-1}m_2$ и неравенства (45) для $r = j^*$ вытекает, что

$$\widehat{m}_{i+1} - \mathcal{M}(W_{j^*-1}) < (n - m_1)m_1^{k-1}m_2\left((t-1)m_1 + 1\right).$$

Подставляя это неравенство в (47) и учитывая, что $m_1 \geqslant 2$, получим

$$\max_{v=2,\ldots,t} \delta_v \leqslant m_2\left((t-1)m_1 + 1\right) + m_2 \leqslant tm_1m_2.$$

Поскольку в каждом из слоев $B^2_{k-1}, \ldots, B^t_{k-1}$ содержится ровно tm_1m_2 наборов $(i+1)$-го ранга, то из последнего неравенства следует, что для каждого $v = 2, 3, \ldots, t$ мы можем выбрать δ_v различных наборов $(i+1)$-го ранга в слое B^v_{k-1}.

Возьмем в качестве множества $\mathcal{N}_i(f)$ объединение всех этих наборов с наборами множества W_{j^*-1}. Тогда, воспользовавшись формулой (20) и учитывая соотношение (46), получим

$$\mathcal{M}\left(\mathcal{N}_i(f)\right) = \mathcal{M}(W_{j^*-1}) + \sum_{v=2}^{t} \delta_v m_1^{B^v_{k-1}|0|} m_2^{B^v_{k-1}|1|} \ldots m_t^{B^v_{k-1}|t-1|} =$$

$$= \mathcal{M}(W_{j^*-1}) + \sum_{v=2}^{t} \delta_v m_v m_1^{k-1} = \mathcal{M}(W_{j^*-1}) + \left(\widehat{m}_{i+1} - \mathcal{M}(W_{j^*-1})\right) = \widehat{m}_{i+1}.$$

Пусть теперь множество S является пустым. Это означает, что

$$\mathcal{M}(W_q) \leqslant \widehat{m}_{i+1} - (n - m_1)m_1^{k-1}m_2. \tag{48}$$

Обозначим через V' множество всех не содержащихся в Θ наборов не более чем i-го ранга из слоев $(k-1)$-го уровня. Положим

$$\overline{W} = E_t^k \setminus (\Theta \cup W_q \cup V').$$

Для оценки величины $\mathcal{M}(\overline{W})$ разобьем $\overline{W}$ на подмножества $\overline{V}, \overline{V_0}, \overline{V_1}, \ldots$ $\ldots, \overline{V_{k-1}}$, где $\overline{V}$ — множество всех однородных наборов из $\overline{W}$ и $\overline{V_s}$ — множество наборов из $\overline{W}$, принадлежащих слоям s-го уровня, $s = 0, 1\ldots, k-1$. Для $s = 0, 1\ldots, k-2$ множество $\overline{V_s}$ в свою очередь разобьем на подмножество $\overline{V_s'}$ всех наборов более чем $(i+1)$-го ранга из слоев s-го уровня и подмножество $\overline{V_s''}$ всех остальных наборов. Тогда

$$\mathcal{M}(\overline{W}) = \mathcal{M}(\overline{V}) + \sum_{s=0}^{k-2} \mathcal{M}(\overline{V_s'}) + \sum_{s=0}^{k-2} \mathcal{M}(\overline{V_s''}) + \mathcal{M}(\overline{V_{k-1}}). \tag{49}$$

Согласно формуле (18) имеем

$$\mathcal{M}(\overline{V_0'}) = \sum_{\substack{u,\,v=2,3,\ldots,t\\ u\neq v}} \big((h-1)-(i+1)\big)\, m_1 m_1^{B_0^{u,v}|0|} m_2^{B_0^{u,v}|1|} \ldots m_t^{B_0^{u,v}|t-1|} =$$

$$= \sum_{\substack{u,\,v=2,3,\ldots,t\\ u\neq v}} (h-i-2) m_1 m_u^{k-1} m_v,$$

$$\mathcal{M}(\overline{V_s'}) = \sum_{u,\,v=2}^{t} \big((h-1)-(i+1)\big)\, m_1 m_1^{B_s^{u,v}|0|} m_2^{B_s^{u,v}|1|} \ldots m_t^{B_s^{u,v}|t-1|} =$$

$$= \sum_{u,\,v=2}^{t} (h-i-2) m_1^{s+1} m_u^{k-s-1} m_v, \quad s=1,\ldots,k-2.$$

Применяя к этим соотношениям неравенства (28) и (31) соответственно, получим

$$\mathcal{M}(\overline{V_0'}) \leqslant (h-i-2)(t-2) m_1 m_2^{k-1}(n-m_1),$$
$$\mathcal{M}(\overline{V_s'}) \leqslant (h-i-2)(t-1) m_1^{s+1} m_2^{k-s-1}(n-m_1), \quad s=1,\ldots,k-2.$$

Таким образом,

$$\sum_{s=0}^{k-2} \mathcal{M}(\overline{V_s'}) \leqslant (h-i-2)(t-1)(n-m_1) \sum_{s=1}^{k-1} m_1^s m_2^{k-s}.$$

Поэтому, используя неравенство (36), получаем

$$\sum_{s=0}^{k-2} \mathcal{M}(\overline{V_s'}) \leqslant (h-i-2)(t-1)(n-m_1) m_1^k m_2. \tag{50}$$

Множество $\overline{V_{k-1}}$ состоит из всех наборов более, чем i-го ранга из слоев s-го уровня, поэтому согласно формуле (18) имеем

$$\mathcal{M}(\overline{V_{k-1}}) = \sum_{v=2}^{t} \big((h-1)-i)\big)\, t m_1 m_2 m_1^{B_{k-1}^{v}|0|} m_2^{B_{k-1}^{v}|1|} \ldots m_t^{B_{k-1}^{v}|t-1|} =$$
$$= \sum_{v=2}^{t} (h-i-1) t m_1^k m_2 m_v = (h-i-1) t (n-m_1) m_1^k m_2.$$

Складывая это равенство с неравенством (50) и используя неравенство (12), получим

$$\sum_{s=0}^{k-2} \mathcal{M}(\overline{V_s'}) + \mathcal{M}(\overline{V_{k-1}}) \leqslant$$
$$\leqslant (h-i-2)(2t-1)(n-m_1) m_1^k m_2 + t(n-m_1) m_1^k m_2 \leqslant$$
$$\leqslant (h-i-2)\Delta n^k + t(n-m_1) m_1^k m_2. \tag{51}$$

Для любого $s=0,1,\ldots,k-2$ множество $\overline{V_s''}$ не может содержать не менее чем m_1 наборов, принадлежащих одной и той же из m_1 возможных категорий, поэтому $|\overline{V_s''}| < m_1^2$. Из формулы (16) следует, что для любого набора $\widetilde{\sigma}$ из слоя s-го уровня справедливо неравенство

$$\mathcal{M}(\{\widetilde{\sigma}\}) \leqslant m_1^s m_2^{k-s}.$$

Тем самым это неравенство выполняется для любого набора $\tilde{\sigma}$ из $\overline{V_s''}$. Таким образом,

$$\mathcal{M}(\overline{V_s''}) = \sum_{\tilde{\sigma} \in \overline{V_s''}} \mathcal{M}(\{\tilde{\sigma}\}) \leqslant |\overline{V_s''}| \cdot m_1^s m_2^{k-s} < m_1^{s+2} m_2^{k-s}.$$

Поэтому

$$\sum_{s=0}^{k-2} \mathcal{M}(\overline{V_s''}) < \sum_{s=0}^{k-2} m_1^{s+2} m_2^{k-s} = m_1 m_2 \sum_{s=1}^{k-1} m_1^s m_2^{k-s}.$$

Применяя к правой части этого неравенства неравенства (36) и (13), получим

$$\sum_{s=0}^{k-2} \mathcal{M}(\overline{V_s''}) < m_1^{k+1} m_2^2 < \frac{d_h}{2} n^k. \tag{52}$$

Используя справедливое для множества $\overline{V}$ неравенство (19) и учитывая, что $t \leqslant n - m_1 + 1 < 2(n - m_1)$, имеем

$$\mathcal{M}(\overline{V}) + (n - m_1) m_1^k m_2 < t m_1^k + (n - m_1) m_1^k m_2 < \\ < 3(n - m_1) m_1^k m_2 \leqslant t(n - m_1) m_1^k m_2.$$

Следовательно, в силу неравенства (12)

$$\mathcal{M}(\overline{V}) + (n - m_1) m_1^k m_2 < \frac{\Delta}{2} n^k \leqslant \frac{d_h}{2} n^k. \tag{53}$$

Учитывая в соотношении (49) неравенства (51), (52), и (53), получим

$$\mathcal{M}(\overline{W}) < (h - i - 2)\Delta n^k + t(n - m_1) m_1^k m_2 + \frac{d_h}{2} n^k + \frac{d_h}{2} n^k - (n - m_1) m_1^k m_2 = \\ = \left((h - i - 2)\Delta + d_h\right) n^k + (t - 1)(n - m_1) m_1^k m_2 \leqslant \\ \leqslant n^k \sum_{j=i+2}^{h} d_j + (t - 1)(n - m_1) m_1^k m_2 = \sum_{j=i+2}^{h} \hat{m}_j + (t - 1)(n - m_1) m_1^k m_2. \tag{54}$$

Так как множества Θ, W_q, V' и $\overline{W}$ не пересекаются, то

$$\mathcal{M}(\Theta) + \mathcal{M}(W_q) + \mathcal{M}(V') + \mathcal{M}(\overline{W}) = \mathcal{M}(E_t^k) = n^k$$

и, с учетом справедливых для множеств $\mathcal{N}_j(f)$ при $j < i$ равенств (25),

$$\mathcal{M}(\Theta) = \sum_{j<i} \mathcal{M}(\mathcal{N}_j(f)) = \sum_{j \leqslant i} \hat{m}_j.$$

Поэтому

$$\mathcal{M}(W_q) + \mathcal{M}(V') + \mathcal{M}(\overline{W}) = n^k - \sum_{j \leqslant i} \hat{m}_j = \sum_{j=1}^{h} \hat{m}_j - \sum_{j \leqslant i} \hat{m}_j = \sum_{j=i+1}^{h} \hat{m}_j. \tag{55}$$

Таким образом, из неравенства (54) следует, что

$$\mathcal{M}(W_q) + \mathcal{M}(V') = \sum_{j=i+1}^{h} \hat{m}_j - \mathcal{M}(\overline{W}) > \hat{m}_{i+1} - (t - 1)(n - m_1) m_1^k m_2. \tag{56}$$

Обозначим через a число $\hat{m}_{i+1} - \mathcal{M}(W_q) - (n - m_1) m_1^{k-1} m_2$. В силу неравенства (48) это чисдо неотрицательно, поэтому мы можем найти в V'

максимальное подмножество V'', удовлетворяющее неравенству $\mathcal{M}(V'') \leqslant a$, т. е. $V'' = V'$, если $\mathcal{M}(V') \leqslant a$, и в противном случае V' является строгим подмножеством V' таким, что $\mathcal{M}(V'' \cup \{\tilde{\sigma}\}) > a$ для любого набора $\tilde{\sigma} \in V' \setminus V''$. Согласно формуле (16) для любого набора $\tilde{\sigma}$ из слоя $(k-1)$-го уровня величина $\mathcal{M}(\{\tilde{\sigma}\})$ делится на m_1^{k-1} и на одно из чисел $m_2, \ldots, m_t$ и, следовательно, делится на l_1. Таким образом, поскольку $(m_1, l_1) = 1$, эта величина делится на $m_1^{k-1} l_1$. Поэтому для состоящего из наборов слоев $(k-1)$-го уровня множества V'' величина $\mathcal{M}(V'') = \sum\limits_{\tilde{\sigma} \in V''} \mathcal{M}(\{\tilde{\sigma}\})$ делится на $m_1^{k-1} l_1$.

Следовательно, из соотношения $\mathcal{M}(W_q) \equiv \hat{m}_{i+1} \pmod{m_1^{k-1} l_1}$ вытекает, что число $c = \hat{m}_{i+1} - \mathcal{M}(W_q) - \mathcal{M}(V'')$ также делится на $m_1^{k-1} l_1$. Кроме того, из неравенства $\mathcal{M}(V'') \leqslant a$ следует, что $c \geqslant (n - m_1) m_1^{k-1} m_2$. Таким образом, $c/m_1^{k-1} \geqslant m_2 \sum\limits_{v=2}^{t} m_v$ и c/m_1^{k-1} делится на l_1. Поэтому согласно следствию 1 найдутся положительные числа $\delta_2, \ldots, \delta_t$ такие, что

$$\sum_{v=2}^{t} \delta_v m_v = \frac{c}{m_1^{k-1}} \tag{57}$$

и

$$\max_{v=2,\ldots,t} \delta_v \leqslant \frac{c}{m_1^{k-1} \sum\limits_{v=2}^{t} m_v} + m_2. \tag{58}$$

Покажем, что

$$\mathcal{M}(V'') > \hat{m}_{i+1} - \mathcal{M}(W_q) - (t-1)(n - m_1) m_1^k m_2. \tag{59}$$

Заметим для этого, что в случае $V'' = V'$ данное неравенство непосредственно следует из (56). Пусть $V'' \neq V'$. Из формулы (16) вытекает, что для любого набора $\tilde{\sigma}$ из слоя $(k-1)$-го уровня справедливо неравенство $\mathcal{M}(\{\tilde{\sigma}\}) \leqslant m_1^{k-1} m_2$. Поэтому если $\tilde{\sigma} \in V' \setminus V''$, то

$$\mathcal{M}(V'' \cup \{\tilde{\sigma}\}) = \mathcal{M}(V'') + \mathcal{M}(\{\tilde{\sigma}\}) \leqslant \mathcal{M}(V'') + m_1^{k-1} m_2.$$

Таким образом, в этом случае имеем неравенство $\mathcal{M}(V'') + m_1^{k-1} m_2 > a$, из которого очевидным образом вытекает неравенство (59). Из неравенства (59) получаем, что $c < (t-1)(n - m_1) m_1^k m_2$. Подставляя эту оценку для c в (58), имеем

$$\max_{v=2,\ldots,t} \delta_v < (t-1) m_1 m_2 + m_2 < t m_1 m_2.$$

Из данного неравенства следует, что для каждого $v = 2, 3, \ldots, t$ мы можем выбрать δ_v различных наборов $(i+1)$-го ранга в слое B_{k-1}^v. Возьмем в качестве множества $\mathcal{N}_i(f)$ объединение всех этих наборов с наборами множества $W_q \cup V''$. Тогда, воспользовавшись формулой (20) и учитывая соотношение (57), получим

$$\mathcal{M}\big(\mathcal{N}_i(f)\big) = \mathcal{M}(W_q \cup V'') + \sum_{v=2}^{t} \delta_v m_1^{B_{k-1}^v |0|} m_2^{B_{k-1}^v |1|} \ldots m_t^{B_{k-1}^v |t-1|} =$$

$$= \mathcal{M}(W_q) + \mathcal{M}(V'') + \sum_{v=2}^{t} \delta_v m_v m_1^{k-1} =$$

$$= \mathcal{M}(W_q) + \mathcal{M}(V'') + c = \hat{m}_{i+1}.$$

Таким образом, в любом случае множество $\mathcal{N}_i(f)$ удовлетворяет соотношению (24). Кроме того, очевидно, множество $\mathcal{N}_i(f)$ состоит из однородных наборов множества U_i^0 и неоднородных наборов ранга, не большего чем $i+1$.

Построив искомые множества $\mathcal{N}_0(f), \ldots, \mathcal{N}_{h-2}(f)$ и применив утверждение 5, получим соотношение (23), из которого следует, что $\widehat{\mathcal{D}} \in \langle\{\mathcal{D}\}\rangle$. Поэтому

$$G[\Pi(\mathcal{D}); T(\mathcal{D})] \subseteq \langle\{\mathcal{D}\}\rangle$$

в силу утверждения 4.

Лемма 4. *Пусть среди чисел $m_1, m_2, \ldots, m_t$ имеется не менее двух максимальных элементов.*

Тогда

$$G[\Pi(\mathcal{D}); T(\mathcal{D})] \subseteq \langle\mathcal{D}\rangle.$$

Доказательство. Пусть среди чисел $m_1, m_2, \ldots, m_t$ имеется $p \geqslant 2$ максимальных элементов. В силу утверждения 2 без ограничения общности мы можем полагать, что $m_1 = \ldots = m_p > m_{p+1} \geqslant \ldots \geqslant m_t$. Тогда для любого $i = 1, \ldots, p$ имеем $l_i = (m_1, m_{p+1}, \ldots, m_t) = (m_1, m_2, \ldots, m_t) = 1$, поэтому $T(\mathcal{D}) = \{l_{p+1}, \ldots, l_t\}^{>1}$. Пусть $\widehat{\mathcal{D}} = (\widehat{d}_1; \ldots; \widehat{d}_h)$ — произвольный позитивный вектор из $G[\Pi(\mathcal{D}); T(\mathcal{D})]$. Положим $\Delta = \min(\widehat{d}_1, \ldots, \widehat{d}_h)$. Аналогично доказательству леммы 3 мы построим удовлетворяющую соотношению (23) дискретную функцию $f(x_1, \ldots, x_k)$, последовательно определяя удовлетворяющие равенствам (24) непересекающиеся множества $\mathcal{N}_0(f), \mathcal{N}_1(f), \ldots, \mathcal{N}_{h-2}(f)$. Выберем достаточно большое целое k_0 такое, что n^{k_0} является общим кратным знаменателей компонент вектора $\widehat{\mathcal{D}}$.

Рассмотрим отдельно два возможных случая.

1. Пусть $t \geqslant p+1$. Тогда положим $\mu = \sum_{j=p+1}^{t} m_j$, и возьмем в качестве k достаточно большое натуральное число, не меньшее k_0 и удовлетворяющее неравенствам

$$k \geqslant (h-1)m_1, \tag{60}$$

$$p^k \geqslant (h-1)(t-p)\mu m_1, \tag{61}$$

$$\left(\frac{m_1}{n}\right)^k < \frac{\Delta}{2(t-p)\mu m_1}, \tag{62}$$

$$\left(\frac{m_1}{n}\right)^k < \frac{\widehat{d}_h}{\mu m_1^2}. \tag{63}$$

Будем также предполагать $k \geqslant 3$. Аналогично доказательству леммы 3 определим числа $\widehat{m}_i$ и μ_j, где $i = 1, \ldots, h$, $j = 0, 1, \ldots, h-1$, и подмножества $T_0, T_1, \ldots, T_{h-1}$ множества $T(\mathcal{D})$, удовлетворяющие соотношениям (14) и (15). Будем также обозначать $n^k \boldsymbol{P}_U(\underbrace{\mathcal{D}, \ldots, \mathcal{D}}_{k})$ через $\mathcal{M}(U)$ для любого множества U наборов из E_t^k.

Обозначим через $\overline{C}_t^k$ множество всех наборов $(i; i; \ldots; i)$ из C_t^k, где $i \geqslant p$. Поскольку $m_{p+1} \geqslant m_{p+2} \geqslant \ldots \geqslant m_t$, для любого подмножества $\overline{U}$ множества $\overline{C}_t^k$ справедлива оценка

$$\mathcal{M}(U) = \sum_{(i;\ldots;i)\in U} m_{i+1}^k \leqslant \sum_{i=p+1}^{t} m_i^k \leqslant (t-p)m_{p+1}^k. \tag{64}$$

Наборы из E_t^k, не содержащиеся в $\overline{C}_t^k$, мы группируем во множества, состоящие из всех наборов, имеющих одинаковый состав символов, если символы $0, 1, \ldots, p-1$ рассматривать как один и тот же символ. Мы будем называть такие множества *квазислоями* множества E_t^k. Если $\overline{B}$ — квазислой, каждый из наборов которого содержит c_j символов j, где $j = p, p+1, \ldots, t-1$, и в общей сложности c символов $0, 1, \ldots, p-1$, то мы обозначаем через $\overline{B}|j|$ число c_j и через $\overline{B}|*|$ число c. Совокупность всех квазислоев множества E_t^k обозначим через $\overline{\mathscr{B}}_t^k$. Из равенств (16) и (17) вытекает справедливая для любого $U \subseteq E_t^k$ формула

$$\mathscr{M}(U) = \sum_{(i;\ldots;i)\in U\cap\overline{C}_t^k} m_{i+1}^k + \sum_{\overline{B}\in\overline{\mathscr{B}}_t^k} |U\cap\overline{B}| m_1^{\overline{B}|*|} m_{p+1}^{\overline{B}|p|} m_{p+2}^{\overline{B}|p+1|} \ldots m_t^{\overline{B}|t-1|}. \quad (65)$$

Из этой формулы получаем, что для любых двух подмножеств U, V множества E_t^k таких, что $U\cap\overline{C}_t^k = V\cap\overline{C}_t^k$, выполняется равенство

$$\mathscr{M}(V) = \mathscr{M}(U) + \sum_{\overline{B}\in\overline{\mathscr{B}}_t^k} \lambda_{\overline{B}} m_1^{\overline{B}|*|} m_{p+1}^{\overline{B}|p|} m_{p+2}^{\overline{B}|p+1|} \ldots m_t^{\overline{B}|t-1|}, \quad (66)$$

где $\lambda_{\overline{B}} = |V\cap\overline{B}| - |U\cap\overline{B}|$.

Квазислой $\overline{B}$ множества E_t^k назовем *квазислоем i-го уровня*, где $i = 0, 1, \ldots, k$, если набор из $\overline{B}$ содержит в общей сложности ровно i символов $0, 1, \ldots, p-1$. Для $j = p+1, \ldots, t$ обозначим через $\overline{B}_{k-1}^j$ квазислой $(k-1)$-го уровня из наборов, содержащих помимо символов $0, 1, \ldots, p-1$ один символ $j-1$. Если $t > p+1$, то для $i = 0, \ldots, k-2$ и $j, s = p+1, \ldots, t$, где $j \neq s$, обозначим через $\overline{B}_i^{j,s}$ квазислой i-го уровня из наборов, содержащих помимо символов $0, 1, \ldots, p-1$ ровно один символ $s-1$ и $k-i-1$ символов $j-1$. В случае $i = 1, \ldots, k-2$ и $j = p+1, \ldots, t$ через $\overline{B}_i^{j,j}$ будем обозначать квазислой i-го уровня из наборов, содержащих помимо символов $0, 1, \ldots, p-1$ только символы $j-1$. Отметим, что в каждом квазислое множества E_t^k целиком содержится по крайней мере один слой этого множества, поэтому согласно утверждению 7 каждый квазислой содержит по крайней мере k различных наборов. Следовательно, в силу неравенства (60) в каждом из обозначенных нами квазислоев мы можем выделить по $(h-1)m_1$ различных наборов, приписав каждому из этих наборов некоторый целочисленный ранг от 1 до $h-1$ так, чтобы в любом из этих квазислоев содержалось ровно по m_1 различных наборов каждого ранга. Обозначим через $\overline{B}_k$ квазислой k-го уровня, т. е. квазислой из наборов, содержащих только символы $0, 1, \ldots, p-1$. Заметим, что $|\overline{B}_k| = p^k$, поэтому в силу неравенства (61) мы можем выделить $(h-1)(t-p)\mu m_1$ различных наборов из $\overline{B}_k$, приписав каждому из этих наборов некоторый целочисленный ранг от 1 до $h-1$ так, чтобы в $\overline{B}_k$ содержалось ровно по $(t-p)\mu m_1$ различных наборов каждого ранга. Наборам из $E_t^k \setminus \overline{C}_t^k$, которым не было приписано никакого ранга, припишем ранг 0. Согласно формуле (16) для любого набора $\tilde{\sigma}$ из квазислоя i-го уровня величина $\mathscr{M}(\{\tilde{\sigma}\})$ делится на m_1^i, т. е. $\mathscr{M}(\{\tilde{\sigma}\})/m_1^i$ является целым числом. Мы разбиваем все наборы из $E_t^k \setminus \overline{C}_t^k$ на категории $0, 1, \ldots, m_1 - 1$ следующим образом: набор $\tilde{\sigma}$ из квазислоя i-го уровня принадлежит категории j, если $\mathscr{M}(\{\tilde{\sigma}\})/m_1^i \equiv j \pmod{m_1}$.

Для каждого $i = p, p+1, \ldots, t-1$ аналогично доказательству леммы 3 определим величину $\chi(i)$ и разобьем множество $\overline{C}_t^k$ на непересекающиеся подмножества $\overline{U}_0^0, \overline{U}_1^0, \ldots, \overline{U}_{h-1}^0$, где $\overline{U}_j^0$ состоит из всех наборов $(i; i; \ldots; i)$

множества $\overline{C}_t^k$ таких, что $\chi(i)=j$. Аналогично соотношениям (22) можно доказать для любого $j=0, 1, \ldots, h-2$ соотношение

$$\mathcal{M}(\overline{U}_j^0) \equiv \widehat{m}_{j+1} \pmod{l}. \tag{67}$$

В процессе построения множества $\mathcal{N}_i(f)$ будем дополнительно требовать, чтобы оно не содержало наборов ранга, большего $i+1$, и удовлетворяло соотношению $\mathcal{N}_i(f) \cap \overline{C}_t^k = \overline{U}_i^0$.

Пусть $i \in \{0, 1, \ldots, h-2\}$. Аналогично доказательству леммы 3 мы предполагаем, что нами уже определено множество Θ, и строим последовательность множеств $\overline{U}_i^1, \ldots, \overline{U}_i^k$ таких, что для каждого $s=1, \ldots, k$ множество U_i^s содержит только наборы из множества $\overline{U}_i^0$ и наборы $(i+1)$-го ранга из квазислоев не более чем $(s-1)$-го уровня и при этом выполняется соотношение

$$\mathcal{M}(\overline{U}_i^s) \equiv \widehat{m}_{i+1} \pmod{m_1^s}. \tag{68}$$

Выделим два возможных подслучая.

а) Пусть $t > p+1$. Из соотношения (67) имеем $\widehat{m}_{i+1} - \mathcal{M}(\overline{U}_i^0) \equiv 0 \pmod{l = l_{p+1} \ldots l_t}$. Поэтому согласно утверждению 15 найдутся целые неотрицательные числа α_v^u, где $u, v = p+1, p+2, \ldots, t$ и $u \neq v$, такие, что каждое из этих чисел меньше, чем m_1, и выполняется соотношение

$$\widehat{m}_{i+1} - \mathcal{M}(\overline{U}_i^0) \equiv \sum_{\substack{u, v = p+1, \ldots, t \\ u \neq v}} \alpha_v^u m_u^{k-1} m_v \pmod{m_1}. \tag{69}$$

В каждом квазислое $\overline{B}_0^{u,v}$, где $u, v = p+1, p+2, \ldots, t$ и $u \neq v$, мы можем выбрать α_v^u различных наборов $(i+1)$-го ранга и взять в качестве множества $\overline{U}_i^1$ объединение всех этих наборов с наборами множества $\overline{U}_i^0$. Тогда согласно формуле (66) получаем

$$\mathcal{M}(\overline{U}_i^1) = \mathcal{M}(\overline{U}_i^0) + \sum_{\substack{u, v = p+1, \ldots, t \\ u \neq v}} \alpha_v^u m_1^{\overline{B}_0^{u,v}|*|} m_{p+1}^{\overline{B}_0^{u,v}|p|} m_{p+2}^{\overline{B}_0^{u,v}|p+1|} \ldots m_t^{\overline{B}_0^{u,v}|t-1|} =$$

$$= \mathcal{M}(\overline{U}_i^0) + \sum_{\substack{u, v = p+1, \ldots, t \\ u \neq v}} \alpha_v^u m_u^{k-1} m_v.$$

Таким образом, множество $\overline{U}_i^1$ в силу соотношения (69) удовлетворяет сравнению (68) и содержит только наборы из $\overline{U}_i^0$ и наборы $(i+1)$-го ранга из квазислоев нулевого уровня. Кроме того, учитывая неравенства $\alpha_v^u < m_1$, получим

$$\mathcal{M}(\overline{U}_i^1) < \mathcal{M}(\overline{U}_i^0) + \sum_{\substack{u, v = p+1, \ldots, t \\ u \neq v}} m_1 m_u^{k-1} m_v.$$

Аналогично неравенству (28) имеем

$$\sum_{\substack{u, v = p+1, \ldots, t \\ u \neq v}} m_1 m_u^{k-1} m_v \leqslant (t-p-1) m_1 m_{p+1}^{k-1} \mu. \tag{70}$$

Поэтому

$$\mathcal{M}(\overline{U}_i^1) < \mathcal{M}(\overline{U}_i^0) + (t-p-1) m_1 m_{p+1}^{k-1} \mu. \tag{71}$$

Предположим, что для некоторого $s \in \{2, \ldots, k-1\}$ нами уже построено искомое множество $\overline{U}_i^{s-1}$. Тогда в силу сравнения (68) имеем

$$\widehat{m}_{i+1} - \mathcal{M}(\overline{U}_i^{s-1}) \equiv 0 \pmod{m_1^{s-1}}.$$

Так как числа $0, 1, \ldots, m_1 - 1$ образуют полную систему вычетов по модулю m_1, то согласно утверждению 17 найдутся целые числа β_v^u, где $u, v = p+1, p+2, \ldots, t$, удовлетворяющие неравенствам $0 \leqslant \beta_v^u < m_1$ и такие, что

$$\widehat{m}_{i+1} - \mathcal{M}(\overline{U}_i^{s-1}) \equiv \sum_{u,\, v=p+1}^{t} \beta_v^u m_1^{s-1} m_u^{k-s} m_v \pmod{m_1^s}. \tag{72}$$

В каждом квазислое $\overline{B}_{s-1}^{u,v}$, где $u, v = p+1, p+2, \ldots, t$, мы можем выбрать β_v^u различных наборов $(i+1)$-го ранга и взять в качестве множества $\overline{U}_i^s$ объединение всех этих наборов с наборами множества $\overline{U}_i^{s-1}$. Тогда согласно формуле (66) получаем

$$\mathcal{M}(\overline{U}_i^s) = \mathcal{M}(\overline{U}_i^{s-1}) + \sum_{u,\, v=p+1}^{t} \beta_v^u m_1^{B_{s-1}^{u,v}|*|} m_{p+1}^{B_{s-1}^{u,v}|p|} m_{p+2}^{B_{s-1}^{u,v}|p+1|} \ldots m_t^{B_{s-1}^{u,v}|t-1|} =$$

$$= \mathcal{M}(\overline{U}_i^{s-1}) + \sum_{u,\, v=p+1}^{t} \beta_v^u m_1^{s-1} m_u^{k-s} m_v.$$

Таким образом, множество $\overline{U}_i^s$ в силу соотношения (72) удовлетворяет сравнению (68) и содержит только наборы из $\overline{U}_i^0$ и наборы $(i+1)$-го ранга из квазислоев не более чем $(s-1)$-го уровня. Кроме того, учитывая неравенства $\beta_v^u < m_1$, получим

$$\mathcal{M}(\overline{U}_i^s) < \mathcal{M}(\overline{U}_i^{s-1}) + \sum_{u,\, v=p+1}^{t} m_1^s m_u^{k-s} m_v.$$

Аналогично неравенству (28) имеем

$$\sum_{u,\, v=p+1}^{t} m_1^s m_u^{k-s} m_v \leqslant (t-p) m_1^s m_{p+1}^{k-s} \mu. \tag{73}$$

Поэтому

$$\mathcal{M}(\overline{U}_i^s) < \mathcal{M}(\overline{U}_i^{s-1}) + (t-p) m_1^s m_{p+1}^{k-s} \mu. \tag{74}$$

Пусть, наконец, нами построено искомое множество $\overline{U}_i^{k-1}$. Тогда в силу сравнения (68) имеем

$$\widehat{m}_{i+1} - \mathcal{M}(\overline{U}_i^{k-1}) \equiv 0 \pmod{m_1^{k-1}}.$$

Согласно утверждению 18 найдутся целые числа β_v, где $v = p+1, p+2, \ldots, t$, удовлетворяющие неравенствам $0 \leqslant \beta_v^u < m_1$ и такие, что

$$\widehat{m}_{i+1} - \mathcal{M}(\overline{U}_i^{k-1}) \equiv \sum_{v=p+1}^{t} \beta_v m_1^{k-1} m_v \pmod{m_1^k}. \tag{75}$$

В каждом квазислое $\overline{B}_{s-1}^{v}$, где $v = p+1, p+2, \ldots, t$, мы можем выбрать β_v различных наборов $(i+1)$-го ранга и взять в качестве множества $\overline{U}_i^k$ объединение всех этих наборов с наборами множества $\overline{U}_i^{k-1}$. Тогда согласно формуле (66) получаем

$$\mathcal{M}(\overline{U}_i^k) = \mathcal{M}(\overline{U}_i^{k-1}) + \sum_{v=p+1}^{t} \beta_v m_1^{B_{k-1}^{v}|*|} m_{p+1}^{B_{k-1}^{v}|p|} m_{p+2}^{B_{k-1}^{v}|p+1|} \ldots m_t^{B_{k-1}^{v}|t-1|} =$$

$$= \mathcal{M}(\overline{U}_i^{k-1}) + \sum_{v=p+1}^{t} \beta_v m_1^{k-1} m_v.$$

Таким образом, множество $\overline{U}_i^k$ в силу соотношения (75) удовлетворяет сравнению (68) и содержит только наборы из $\overline{U}_i^0$ и наборы $(i+1)$-го ранга из квазислоев не более чем $(k-1)$-го уровня. Кроме того, учитывая неравенства $\beta_v < m_1$, получим

$$\mathcal{M}(\overline{U}_i^k) < \mathcal{M}(\overline{U}_i^{k-1}) + \sum_{v=p+1}^{t} m_1^k m_v = \mathcal{M}(\overline{U}_i^{k-1}) + m_1^k \mu. \tag{76}$$

б) Пусть $t = p+1$. В этом случае $T(\mathcal{D}) = \{l_t\} = \{m_1\}$, поэтому $l = m_1$. Следовательно, из соотношения (67) имеем $\widehat{m}_{i+1} - \mathcal{M}(\overline{U}_i^0) \equiv 0 \pmod{l = m_1}$. Таким образом, в качестве $\overline{U}_i^1$ мы можем взять множество $\overline{U}_i^0$.

Пусть для некоторого $s \in \{2, \ldots, k\}$ нами уже построено искомое множество $\overline{U}_i^{s-1}$. Обозначим через a число $(\widehat{m}_{i+1} - \mathcal{M}(\overline{U}_i^{s-1}))/m_1^{s-1}$, которое является целым в силу соотношения (68) для U_{s-1}. Так как $(m_1, m_t) = 1$ и, следовательно, $(m_1, m_t^{k-s+1}) = 1$, то согласно утверждению 10 в полной системе вычетов $\{0, 1, \ldots, m_1 - 1\}$ по модулю m_1 найдется такое число α, что выполняется соотношение $\alpha m_t^{k-s+1} \equiv a \pmod{m_1}$. Следовательно,

$$\alpha m_1^{s-1} m_t^{k-s+1} \equiv (a m_1^{s-1} = \widehat{m}_{i+1} - \mathcal{M}(\overline{U}_i^{s-1}) \pmod{m_1^s}. \tag{77}$$

Поскольку $\alpha < m_1$, в квазислое $\overline{B}_{s-1}^{t,t}$ (в случае $s = k$ в квазислое $\overline{B}_{k-1}^t$) мы можем выбрать α различных наборов $(i+1)$-го ранга и взять в качестве множества $\overline{U}_i^s$ объединение всех этих наборов с наборами множества $\overline{U}_i^{s-1}$. Используя формулу (66), имеем

$$\mathcal{M}(\overline{U}_i^s) = \mathcal{M}(\overline{U}_i^{s-1}) + \alpha m_1^{s-1} m_t^{k-s+1}, \tag{78}$$

поэтому из соотношения (77) получаем, что U_s удовлетворяет соотношению (68). При этом U_s содержит только наборы из $\overline{U}_i^0$ и наборы $(i+1)$-го ранга из квазислоев не более, чем $(s-1)$-го уровня.

Аналогично доказательству леммы 3 построим теперь конечную последовательность множеств

$$\overline{W}_0, \overline{W}_1, \ldots, \overline{W}_q \tag{79}$$

так, чтобы эти множества состояли только из наборов множества $\overline{U}_i^0$ и не содержащихся в Θ наборов не более чем $(i+1)$-го ранга из квазислоев не более чем $(k-1)$-го уровня и удовлетворяли для каждого $s = 0, 1, \ldots, q$ соотношениям

$$\mathcal{M}(\overline{W}_s) \equiv \widehat{m}_{i+1} \pmod{m_1^k}. \tag{80}$$

В качестве $\overline{W}_0$ возьмем множество $\overline{U}_i^k$. Справедливость соотношения (80) для этого множества непосредственно вытекает из соотношения (68). В случае $t > p+1$, исходя из неравенств (71), (74) и (76) и учитывая справедливое для $\overline{U}_i^0$ неравенство (64), мы можем оценить величину $\mathcal{M}(\overline{W}_0)$:

$$\mathcal{M}(\overline{W}_0) < \mathcal{M}(\overline{U}_i^0) + (t-p-1) m_1 m_{p+1}^{k-1} \mu + \sum_{s=2}^{k-1} (t-p) m_1^s m_{p+1}^{k-s} \mu + m_1^k \mu <$$

$$< (t-p) m_{p+1}^k + (t-p)\mu \sum_{s=1}^{k} m_1^s m_{p+1}^{k-s} \leqslant (t-p)\mu \sum_{s=0}^{k} m_1^s m_{p+1}^{k-s}. \tag{81}$$

Учитывая, что $m_1 > m_{p+1}$, имеем

$$\sum_{s=0}^{k} m_1^s m_{p+1}^{k-s} = m_1^k \sum_{s=0}^{k} \left(\frac{m_{p+1}}{m_1}\right)^s < m_1^k \sum_{s=0}^{\infty} \left(\frac{m_{p+1}}{m_1}\right)^s = m_1^k \frac{m_1}{m_1 - m_{p+1}} \leqslant m_1^{k+1}. \tag{82}$$

Поэтому из неравенства (81) получаем

$$\mathcal{M}(\overline{W}_0) < (t-p)\mu m_1^{k+1}. \tag{83}$$

В случае $t = p+1$, учитывая неравенство $\alpha < m_1$ в соотношении (78), имеем неравенства $\mathcal{M}(\overline{U}_i^s) < \mathcal{M}(\overline{U}_i^{s-1}) + m_1^s m_t^{k-s+1}$, из которых следует, что

$$\mathcal{M}(\overline{W}_0) < \mathcal{M}(\overline{U}_i^0) + \sum_{s=2}^{k} m_1^s m_t^{k-s+1}.$$

Применяя к этому неравенству вытекающую из (64) оценку $\mathcal{M}(\overline{U}_i^0) \leqslant m_t^k$ и вытекающее из (82) неравенство $\sum_{s=1}^{k} m_1^s m_t^{k-s} < m_1^{k+1}$, получим

$$\mathcal{M}(\overline{W}_0) < m_t^k + \sum_{s=2}^{k} m_1^s m_t^{k-s+1} < \sum_{s=1}^{k} m_1^s m_t^{k-s+1} < m_t m_1^{k+1}.$$

Таким образом, в этом случае $\mathcal{M}(\overline{W}_0)$ также удовлетворяет соотношению (83).

Предположим, что для некоторого $r > 0$ нами уже построены множества $\overline{W}_0, \ldots, \overline{W}_{r-1}$. Пусть $\tau(r) \in \{0, 1, \ldots, k-1\}$ — минимально возможное число такое, что в $E_t^k \setminus (\Theta \cup \overline{W}_{r-1})$ найдутся m_1 различных наборов не более, чем $(i+1)$-го ранга из квазислоев $\tau(r)$-го уровня, принадлежащих одной и той же категории. Если $\tau(r)$ существует, обозначим множество этих наборов через V. Аналогично соотношению (39) мы можем получить, что

$$\mathcal{M}(V) \equiv 0 \pmod{m_1^{\tau(r)+1}}. \tag{84}$$

Из формулы (16) вытекает очевидная оценка $\mathcal{M}(\{\widetilde{\sigma}\}) \leqslant m_1^{\tau(r)} m_{p+1}^{k-\tau(r)}$ для любого набора $\widetilde{\sigma}$ из V. Поэтому

$$\mathcal{M}(V) = \sum_{\widetilde{\sigma} \in V} \mathcal{M}(\{\widetilde{\sigma}\}) \leqslant m_1^{\tau(r)+1} m_{p+1}^{k-\tau(r)}. \tag{85}$$

Построим последовательность множеств $\overline{V}^{\tau(r)+1}, \ldots, \overline{V}^k$ так, чтобы эти множества состояли только из наборов множества $\overline{U}_i^0$ и не содержащихся в Θ наборов не более чем $(i+1)$-го ранга из квазислоев не более чем $(k-1)$-го уровня и удовлетворяли для каждого $s = \tau(r)+1, \ldots, k$ соотношениям

$$\mathcal{M}(\overline{V}^s) \equiv \widehat{m}_{i+1} \pmod{m_1^s}. \tag{86}$$

В качестве $\overline{V}^{\tau(r)+1}$ возьмем множество $\overline{W}_{r-1} \cup V$. Так как $\mathcal{M}(\overline{V}^{\tau(r)+1}) = \mathcal{M}(\overline{W}_{r-1}) + \mathcal{M}(V)$, то справедливость соотношения (86) для $\overline{V}^{\tau(r)+1}$ вытекает из справедливости соотношения (80) для $\overline{W}_{r-1}$ и соотношения (84) для V. Кроме того, из (85) получаем оценку

$$\mathcal{M}(\overline{V}^{\tau(r)+1}) \leqslant \mathcal{M}(\overline{W}_{r-1}) + m_1^{\tau(r)+1} m_{p+1}^{k-\tau(r)}. \tag{87}$$

Допустим, что $\tau(r) < k-1$ и для некоторого $s \in \{\tau(r)+2, \ldots, k\}$ уже построено искомое множество $\overline{V}^{s-1}$. Выделим снова два возможных подслучая.

а) Пусть $t > p+1$. Предположим сначала, что $s < k$. В силу сравнения (86) имеем $\widehat{m}_{i+1} - \mathcal{M}(\overline{V}^{s-1}) \equiv 0 \pmod{m_1^{s-1}}$. Для $u, v = p+1, p+2, \ldots, t$

обозначим через J_v^u полную систему $-\gamma_v^u+1, \ldots, m_1-\gamma_v^u$ вычетов по модулю m_1, где γ_v^u — количество наборов $(i+1)$-го ранга из квазислоя $\overline{B}_{s-1}^{u,v}$, содержащихся в $\overline{V}^{s-1}$. Согласно утверждению 17 найдутся целые числа β_v^u, где $u, v=p+1, p+2, \ldots, t$, такие, что $\beta_v^u \in J_v^u$ и выполнено соотношение

$$\widehat{m}_{i+1} - \mathcal{M}(\overline{V}^{s-1}) \equiv \sum_{u,\, v=p+1}^{t} \beta_v^u m_1^{s-1} m_u^{k-s} m_v \pmod{m_1^s}. \tag{88}$$

Для каждого из чисел β_v^u добавим β_v^u различных не содержащихся в $\overline{V}^{s-1}$ наборов $(i+1)$-го ранга из квазислоя $\overline{B}_{s-1}^{u,v}$ ко множеству $\overline{V}^{s-1}$, если $\beta_v^u > 0$, или удалим из этого множества $|\beta_v^u|$ различных принадлежащих квазислою $\overline{B}_{s-1}^{u,v}$ наборов $(i+1)$-го ранга, если $\beta_v^u < 0$. Возьмем в качестве $\overline{V}^s$ множество, получившееся из $\overline{V}^{s-1}$ в результате этих операций. Согласно формуле (66) получаем

$$\mathcal{M}(\overline{V}^s) = \mathcal{M}(\overline{V}^{s-1}) + \sum_{u,\, v=p+1}^{t} \beta_v^u m_1^{s-1} m_u^{k-s} m_v.$$

Из этого равенства и соотношения (88) следует, что $\overline{V}^s$ удовлетворяет сравнению (86). Кроме того, аналогично оценке (73) можем получить следующую оценку:

$$\sum_{u,\, v=p+1}^{t} \beta_v^u m_1^{s-1} m_u^{k-s} m_v \leqslant \sum_{u,\, v=p+1}^{t} m_1^s m_u^{k-s} m_v \leqslant (t-p) m_1^s m_{p+1}^{k-s} \mu.$$

Поэтому

$$\mathcal{M}(\overline{V}^s) \leqslant \mathcal{M}(V^{s-1}) + (t-p) m_1^s m_{p+1}^{k-s} \mu. \tag{89}$$

Предположим теперь, что нами построено искомое множество $\overline{V}^{k-1}$. Тогда в силу сравнения (86) имеем $\widehat{m}_{i+1} - \mathcal{M}(\overline{V}^{k-1}) \equiv 0 \pmod{m_1^{k-1}}$. Для $v=p+1, p+2, \ldots, t$ обозначим через J_v полную систему $-\gamma_v+1, \ldots, m_1-\gamma_v$ вычетов по модулю m_1, где γ_v — количество наборов $(i+1)$-го ранга из квазислоя $\overline{B}_{k-1}^{v}$, содержащихся в $\overline{V}^{k-1}$. Согласно утверждению 18 найдутся целые числа β_v, где $v=p+1, p+2, \ldots, t$, такие, что $\beta_v \in J_v$ и выполнено соотношение

$$\widehat{m}_{i+1} - \mathcal{M}(\overline{V}^{k-1}) \equiv \sum_{v=p+1}^{t} \beta_v m_1^{k-1} m_v \pmod{m_1^k}. \tag{90}$$

Для каждого из чисел β_v добавим β_v различных не содержащихся в $\overline{V}^{k-1}$ наборов $(i+1)$-го ранга из квазислоя $\overline{B}_{k-1}^{v}$ ко множеству $\overline{V}^{k-1}$, если $\beta_v > 0$, или удалим из этого множества $|\beta_v|$ различных принадлежащих квазислою $\overline{B}_{k-1}^{v}$ наборов $(i+1)$-го ранга, если $\beta_v < 0$. Возьмем получившееся в результате множество в качестве $\overline{V}^k$. Согласно формуле (66) получаем

$$\mathcal{M}(\overline{V}^k) = \mathcal{M}(\overline{V}^{k-1}) + \sum_{v=p+1}^{t} \beta_v m_1^{\overline{B}_{k-1}^{v}|*|} m_{p+1}^{\overline{B}_{k-1}^{v}|p|} m_{p+2}^{\overline{B}_{k-1}^{v}|p+1|} \ldots m_t^{\overline{B}_{k-1}^{v}|t-1|} =$$

$$= \mathcal{M}(\overline{V}^{k-1}) + \sum_{v=p+1}^{t} \beta_v m_1^{k-1} m_v.$$

Таким образом, множество $\overline{V}^k$ в силу соотношения (90) удовлетворяет сравнению (86). Кроме того,

$$\mathcal{M}(\overline{V}^k) \leqslant \mathcal{M}(\overline{V}^{k-1}) + \sum_{v=p+1}^{t} m_1^k m_v = \mathcal{M}(\overline{V}^{k-1}) + m_1^k \mu. \tag{91}$$

б) Пусть $t = p+1$. Обозначим через b число $(\widehat{m}_{i+1} - \mathcal{M}(\overline{V}^{s-1}))/m_1^{s-1}$, которое является целым в силу соотношения (86). Обозначим через $\overline{B}^t$ квазислой $\overline{B}^{t,t}_{s-1}$ в случае $s < k$ либо квазислой $\overline{B}^t_{s-1}$ в случае $s = k$. Так как $(m_1, m_t^{k-s+1}) = 1$, то, согласно утверждению 10, в полной системе $-\gamma+1, \ldots$ $\ldots, m_1 - \gamma$ вычетов по модулю m_1, где γ — количество наборов $(i+1)$-го ранга из квазислоя $\overline{B}^t$, содержащихся в $\overline{V}^{s-1}$, найдется такое число β, что выполняется соотношение $\beta m_t^{k-s+1} \equiv b \pmod{m_1}$. Следовательно,

$$\beta m_1^{s-1} m_t^{k-s+1} \equiv (b m_1^{s-1} = \widehat{m}_{i+1} - \mathcal{M}(\overline{V}^{s-1})) \pmod{m_1^s} \tag{92}$$

Если $\beta > 0$, то добавим β различных не содержащихся в $\overline{V}^{s-1}$ наборов $(i+1)$-го ранга из квазислоя $\overline{B}^t$ ко множеству $\overline{V}^{s-1}$. Если $\beta_v^u < 0$, то удалим из этого множества $|\beta|$ различных принадлежащих квазислою $\overline{B}^t$ наборов $(i+1)$-го ранга. Возьмем получившееся в результате множество в качестве $\overline{V}^s$. Тогда согласно формуле (66) получим

$$\mathcal{M}(\overline{V}^s) = \mathcal{M}(\overline{M}^{s-1}) + \beta m_1^{s-1} m_t^{k-s+1}, \tag{93}$$

поэтому из соотношения (92) следует, что $\overline{V}^s$ удовлетворяет соотношению (86). Заметим также, что $\beta \leqslant m_1$, поэтому из равенства (93) получаем оценку

$$\mathcal{M}(\overline{V}^s) \leqslant \mathcal{M}(\overline{M}^{s-1}) + m_1^s m_t^{k-s+1}, \tag{94}$$

Положим $\overline{W}_r = \overline{V}^k$. Тогда справедливость соотношения (80) для W_r непосредственно вытекает из соотношения (86) для $\overline{V}^k$. Отметим также, что, если множество $\overline{W}_{r-1}$ состоит только из наборов множества $\overline{U}_i^0$ и не содержащихся в Θ наборов не более чем $(i+1)$-го ранга из квазислоев не более чем $(k-1)$-го уровня, то в силу способа построения этим же свойством обладает множество $\overline{W}_r$. В случае $t > p+1$, исходя из неравенств (87), (89) и (91), мы можем оценить величину $\mathcal{M}(\overline{W}_r)$:

$$\mathcal{M}(\overline{W}_r) \leqslant \mathcal{M}(\overline{W}_{r-1}) + m_1^{\tau(r)+1} m_{p+1}^{k-\tau(r)} + \sum_{s=\tau(r)+2}^{k-1} (t-p) m_1^s m_{p+1}^{k-s} \mu <$$

$$< \mathcal{M}(\overline{W}_{r-1}) + m_1^{\tau(r)+1} m_{p+1}^{k-\tau(r)-1} \mu + (t-p)\mu \sum_{s=\tau(r)+1}^{k} m_1^s m_{p+1}^{k-s} (n - m_1) <$$

$$< \mathcal{M}(\overline{W}_{r-1}) + (t-p)\mu \sum_{s=\tau(r)+1}^{k} m_1^s m_{p+1}^{k-s} \leqslant \mathcal{M}(\overline{W}_{r-1}) + (t-p)\mu \sum_{s=1}^{k} m_1^s m_{p+1}^{k-s}.$$

Из неравенства (82) вытекает, что $\sum_{s=1}^{k} m_1^s m_{p+1}^{k-s} < m_1^{k+1}$. Таким образом, получаем, что

$$\mathcal{M}(\overline{W}_r) < \mathcal{M}(\overline{W}_{r-1}) + (t-p)\mu m_1^{k+1}. \tag{95}$$

В случае $t = p+1$ оценка для $\mathcal{M}(\overline{W}_r)$ следует из неравенств (87) и (94):

$$\mathcal{M}(\overline{W}_r) \leqslant \mathcal{M}(\overline{W}_{r-1}) + \sum_{s=\tau(r)+1}^{k} m_1^s m_t^{k-s+1} \leqslant$$

$$\leqslant \mathcal{M}(\overline{W}_{r-1}) + m_t \sum_{s=1}^{k} m_1^s m_t^{k-s}.$$

Учитывая в этом неравенстве неравенство $\sum_{s=1}^{k} m_1^s m_t^{k-s} < m_1^{k+1}$, получим

$$\mathcal{M}(\overline{W}_r) < \mathcal{M}(\overline{W}_{r-1}) + m_t m_1^{k+1}.$$

Таким образом, в этом случае $\mathcal{M}(\overline{W}_r)$ также удовлетворяет соотношению (95).

Если $\tau(r)$ не существует, т. е. для любого $s=0, 1, \ldots, k-1$ среди не содержащихся в $\Theta \cup \overline{W}_{r-1}$ наборов не более чем $(i+1)$-го ранга из квазислоев s-го уровня не найдется m_1 наборов одной и той же категории, то завершим построение искомой последовательности множеств, положив $q=r-1$. Аналогично доказательству конечности последовательности множеств (33) можно показать, что построение последовательности (79) обязательно завершится.

Пусть S — подмножество всех множеств $\overline{W}_j$ последовательности (79) таких, что $\mathcal{M}(\overline{W}_j) \geqslant \widehat{m}_{i+1}$. Если S непусто, то обозначим через j^* минимальный порядковый индекс множеств из S. Из неравенств (83) и (62) следует, что

$$\mathcal{M}(\overline{W}_0) < \frac{\Delta}{2} n^k < \widehat{d}_{i+1} n^k = \widehat{m}_{i+1}.$$

Поэтому $\overline{W}_0 \notin S$. Следовательно, $j^* > 1$. Таким образом, мы можем рассмотреть множество $\overline{W}_{j^*-1}$. Из (80) имеем $\widehat{m}_{i+1} - \mathcal{M}(\overline{W}_{j^*-1}) \equiv 0 \pmod{m_1^k}$. Обозначим через c целое число $\left(\widehat{m}_{i+1} - \mathcal{M}(\overline{W}_{j^*-1})\right)/m_1^k$. Поскольку $\overline{W}_{j^*-1} \notin S$, то $\widehat{m}_{i+1} - \mathcal{M}(\overline{W}_{j^*-1}) > 0$ и, следовательно, $c > 0$. Кроме того, из неравенства $\mathcal{M}(\overline{W}_{j^*}) \geqslant \widehat{m}_{i+1}$ и неравенства (95) для $r = j^*$ вытекает, что $\widehat{m}_{i+1} - \mathcal{M}(\overline{W}_{j^*-1}) < (t-p)\mu m_1^{k+1}$, поэтому $c < (t-p)\mu m_1$. Таким образом, мы можем выбрать c различных наборов $(i+1)$-го ранга в квазислое $\overline{B}_k$ и взять в качестве множества $\mathcal{N}_i(f)$ объединение всех этих наборов с наборами множества $\overline{W}_{j^*-1}$. Воспользовавшись формулой (66), получим

$$\mathcal{M}\left(\mathcal{N}_i(f)\right) = \mathcal{M}(\overline{W}_{j^*-1}) + c m_1^{\overline{B}_k|*|} m_{p+1}^{\overline{B}_k|p|} m_{p+2}^{\overline{B}_k|p+1|} \ldots m_t^{\overline{B}_k|t-1|} = \\ = \mathcal{M}(\overline{W}_{j^*-1}) + c m_1^k = \widehat{m}_{i+1}. \quad (96)$$

Пусть теперь множество S является пустым. Это означает, что

$$\mathcal{M}(W_q) < \widehat{m}_{i+1}. \quad (97)$$

Обозначим через V' множество всех не содержащихся в Θ наборов не более чем $(i+1)$-го ранга из квазислоя $\overline{B}_k$. Положим $\overline{W} = E_t^k \setminus (\Theta \cup \overline{W}_q \cup V')$. Аналогично доказательству леммы 3 оценим величину $\mathcal{M}(\overline{W})$, разбив $\overline{W}$ на подмножества:

$$\overline{W} = \overline{V} \cup \bigcup_{s=0}^{k-1} \overline{V}'_s \cup \bigcup_{s=0}^{k-1} \overline{V}''_s \cup \overline{V}_k,$$

где $\overline{V} = \overline{W} \cap \overline{C}_t^k$, $\overline{V}'_s$ ($\overline{V}''_s$) — множество всех наборов более чем $(i+1)$-го ранга (не более чем $(i+1)$-го ранга) из $\overline{W}$, принадлежащих квазислоям s-го уровня, $s=0, 1\ldots, k-1$, и $\overline{V}_k = \overline{W} \cap \overline{B}_k$. Тогда

$$\mathcal{M}(\overline{W}) = \mathcal{M}(\overline{V}) + \sum_{s=0}^{k-1} \mathcal{M}(\overline{V}'_s) + \sum_{s=0}^{k-1} \mathcal{M}(\overline{V}''_s) + \mathcal{M}(\overline{V}_k). \quad (98)$$

Чтобы оценить $\mathcal{M}(\overline{V}'_s)$ для $s=0,1,\ldots,k-2$, рассмотрим снова два возможных подслучая.

а) Пусть $t>p+1$. Тогда согласно формуле (65) имеем

$$\mathcal{M}(\overline{V}'_0)=$$

$$=\sum_{\substack{u,\,v=p+1,\ldots,\,t\\ u\neq v}}\big((h-1)-(i+1)\big)m_1 m_1^{\overline{B}_0^{u,v}|*|}m_{p+1}^{\overline{B}_0^{u,v}|p|}m_{p+2}^{\overline{B}_0^{u,v}|p+1|}\ldots m_t^{\overline{B}_0^{u,v}|t-1|}=$$

$$=\sum_{\substack{u,\,v=p+1,\ldots,\,t\\ u\neq v}}(h-i-2)m_1 m_u^{k-1}m_v,$$

$$\mathcal{M}(\overline{V}'_s)=$$

$$=\sum_{u,\,v=p+1}^{t}\big((h-1)-(i+1)\big)m_1 m_1^{\overline{B}_s^{u,v}|*|}m_{p+1}^{\overline{B}_s^{u,v}|p|}m_{p+2}^{\overline{B}_s^{u,v}|p+1|}\ldots m_t^{\overline{B}_s^{u,v}|t-1|}=$$

$$=\sum_{u,\,v=p+1}^{t}(h-i-2)m_1^{s+1}m_u^{k-s-1}m_v,\quad s=1,\ldots,k-2.$$

Применяя к этим соотношениям неравенства (70) и (73) соответственно, получим

$$\mathcal{M}(\overline{V}'_0)\leqslant(h-i-2)(t-p-1)m_1 m_{p+1}^{k-1}\mu, \tag{99}$$

$$\mathcal{M}(\overline{V}'_s)\leqslant(h-i-2)(t-p)m_1^{s+1}m_{p+1}^{k-s-1}\mu,\quad s=1,\ldots,k-2. \tag{100}$$

б) Пусть $t=p+1$. Отметим, что тогда единственным набором, не содержащим символов $0,1,\ldots,p-1$, является набор $(p;p;\ldots;p)$, принадлежащий множеству $\overline{C}_t^k$. Таким образом, в этом случае E_t^k не содержит квазислоев нулевого уровня. Следовательно, $\overline{V}'_0=\varnothing$ и $\mathcal{M}(\overline{V}'_0)=0$, т. е. неравенство (99) справедливо и в этом случае. Справедливость неравенств (100) в этом случае вытекает из равенств, получаемых применением к $\mathcal{M}(\overline{V}'_s)$ формулы (65):

$$\mathcal{M}(\overline{V}'_s)=\big((h-1)-(i+1)\big)m_1 m_1^{\overline{B}_s^{t,t}|*|}m_{p+1}^{\overline{B}_s^{t,t}|p|}m_{p+2}^{\overline{B}_s^{t,t}|p+1|}\ldots m_t^{\overline{B}_s^{t,t}|t-1|}=$$

$$=(h-i-2)m_1^{s+1}m_t^{k-s}.$$

Применяя формулу (65) к $\overline{V'_{k-1}}$, имеем

$$\mathcal{M}(\overline{V'_{k-1}})=\sum_{v=p+1}^{t}\big((h-1)-(i+1)\big)m_1 m_1^{\overline{B}_{k-1}^{v}|*|}m_{p+1}^{\overline{B}_{k-1}^{v}|p|}m_{p+2}^{\overline{B}_{k-1}^{v}|p+1|}\ldots m_t^{\overline{B}_{k-1}^{v}|t-1|}=$$

$$=\sum_{v=p+1}^{t}(h-i-2)m_1^k m_v=(h-i-2)m_1^k\mu.$$

Суммируя данное равенство с неравенствами (99) и (100), получим

$$\sum_{s=0}^{k-1}\mathcal{M}(\overline{V}'_s)\leqslant(h-i-2)(t-p-1)m_1 m_{p+1}^{k-1}\mu+\sum_{s=2}^{k-1}(h-i-2)(t-p)m_1^s m_{p+1}^{k-s}\mu+$$

$$+(h-i-2)m_1^k\mu\leqslant(h-i-2)(t-p)\mu\sum_{s=1}^{k}m_1^s m_{p+1}^{k-s}.$$

Поскольку $\sum\limits_{s=1}^{k}m_1^s m_{p+1}^{k-s}<m_1^{k+1}$, получаем тогда, что

$$\sum_{s=0}^{k-1}\mathcal{M}(\overline{V}'_s)\leqslant(h-i-2)(t-p)\mu m_1^{k+1}. \tag{101}$$

Множество $\overline{V}_k$ состоит из всех наборов более, чем $(i+1)$-го ранга из квазислоя $\overline{B}_k$, поэтому согласно формуле (65) имеем

$$\mathcal{M}(\overline{V}_k) = \big((h-1)-(i+1)\big)(t-p)\mu m_1 m_1^{B_k|*|} m_{p+1}^{B_k|p|} m_{p+2}^{B_k|p+1|} \dots m_t^{B_k|t-1|} = \\ = (h-i-2)(t-p)\mu m_1^{k+1}.$$

Складывая это равенство с неравенством (101) и используя неравенство (62), получим

$$\sum_{s=0}^{k-1} \mathcal{M}(\overline{V}'_s) + \mathcal{M}(\overline{V}_k) \leqslant 2(h-i-2)(t-p)\mu m_1^{k+1} \leqslant (h-i-2)\Delta n^k. \quad (102)$$

Аналогично доказательству леммы 3 для любого $s=0, 1, \dots, k-1$ имеем $|\overline{V}''_s| < m_1^2$. Кроме того, из формулы (16) следует, что для любого набора $\widetilde{\sigma}$ из $\overline{V}''_s$ справедливо неравенство $\mathcal{M}(\{\widetilde{\sigma}\}) \leqslant m_1^s m_{p+1}^{k-s}$. Таким образом,

$$\mathcal{M}(\overline{V}''_s) = \sum_{\widetilde{\sigma} \in \overline{V}''_s} \mathcal{M}(\{\widetilde{\sigma}\}) \leqslant |\overline{V}''_s| \cdot m_1^s m_{p+1}^{k-s} < m_1^{s+2} m_{p+1}^{k-s}.$$

Следовательно, используя также справедливое для множества $\overline{V}$ неравенство (64), получаем, что

$$\mathcal{M}(\overline{V}) + \sum_{s=0}^{k-1} \mathcal{M}(\overline{V}''_s) < (t-p)m_{p+1}^k + \sum_{s=0}^{k-1} m_1^{s+2} m_{p+1}^{k-s} \leqslant \\ \leqslant \mu m_{p+1}^k + m_1 m_{p+1} \sum_{s=1}^{k} m_1^s m_{p+1}^{k-s} < \mu m_1 \sum_{s=0}^{k} m_1^s m_{p+1}^{k-s}.$$

Применяя (82) и (63) к правой части этого неравенства, получим

$$\mathcal{M}(\overline{V}) + \sum_{s=0}^{k-1} \mathcal{M}(\overline{V}''_s) < \mu m_1^{k+2} < \widehat{d}_h n^k. \quad (103)$$

Учитывая в соотношении (98) неравенства (102) и (103), имеем

$$\mathcal{M}(\overline{W}) < (h-i-2)\Delta n^k + \widehat{d}_h n^k \leqslant n^k \sum_{j=i+2}^{h} \widehat{d}_j = \sum_{j=i+2}^{h} \widehat{m}_j. \quad (104)$$

Аналогично равенству (55) мы можем доказать, что

$$\mathcal{M}(\overline{W}_q) + \mathcal{M}(V') + \mathcal{M}(\overline{W}) = \sum_{j=i+1}^{h} \widehat{m}_j.$$

Поэтому из неравенства (104) следует, что

$$\mathcal{M}(W_q) + \mathcal{M}(V') > \sum_{j=i+1}^{h} \widehat{m}_j - \sum_{j=i+2}^{h} \widehat{m}_j = \widehat{m}_{i+1}. \quad (105)$$

Обозначим через a число $\big(\widehat{m}_{i+1} - \mathcal{M}(\overline{W}_q)\big)/m_1^k$, которое является целым в силу соотношения (80) для $s=q$ и положительным в силу неравенства (97). Согласно формуле (65) для V' выполняется соотношение $\mathcal{M}(V') = |V'| \cdot m_1^k$. Поэтому из неравенства (105) следует, что $a < |V'|$. Таким образом, мы можем выбрать a различных наборов из множества V' и

взять в качестве множества $\mathcal{N}_i(f)$ объединение всех этих наборов с наборами множества $\overline{W}_q$. Аналогично равенству (96) получаем

$$\mathcal{M}\big(\mathcal{N}_i(f)\big) = \mathcal{M}(\overline{W}_q) + am_1^k = \widehat{m}_{i+1}.$$

Таким образом, в любом случае множество $\mathcal{N}_i(f)$ удовлетворяет равенству (25), которое эквивалентно соотношению (24). Кроме того, это множество, очевидно, не содержит наборов ранга, большего $i+1$, и удовлетворяет соотношению

$$\mathcal{N}_i(f) \cap \overline{C}_t^k = \overline{U}_i^0.$$

2. Пусть $t = p$. Тогда, очевидно, $m_1 = \ldots = m_t = 1$, поэтому $n = t$. Положим $k = k_0$. Поскольку для любого множества U наборов из E_t^k очевидным образом выполняется соотношение

$$\boldsymbol{P}_U(\mathcal{D}, \ldots, \mathcal{D}) = \frac{|U|}{n^k},$$

в качестве искомых множеств $\mathcal{N}_0(f), \mathcal{N}_1(f), \ldots, \mathcal{N}_{h-2}(f)$ мы можем взять произвольные непересекающиеся подмножества $U_0, U_1, \ldots, U_{h-2}$ множества E_t^k такие, что $|U_i| = \widehat{d}_{i+1} n^k$.

Построив искомые множества $\mathcal{N}_0(f), \ldots, \mathcal{N}_{h-2}(f)$ и применив утверждение 5, получим соотношение (23), из которого следует, что $\widehat{\mathcal{D}} \in \langle \mathcal{D} \rangle$. Поэтому $G[\Pi(\mathcal{D}); T(\mathcal{D})] \subseteq \langle \mathcal{D} \rangle$ в силу утверждения 4.

Объединяя вместе леммы 2, 3 и 4, получаем

Следствие 2. *Для любого позитивного вектора $\mathcal{D}$ из $\boldsymbol{Q}(0, 1)$ справедливо соотношение* (10).

§ 5. Замыкания конечных множеств стохастических векторов

Рассмотрим теперь произвольное конечное множество $M = \{\mathcal{D}_1, \ldots, \mathcal{D}_s\}$ позитивных стохастических векторов из $\boldsymbol{Q}(0, 1)$ размерности $h_1, \ldots, h_s$ соответственно. Как и в случае одноэлементных множеств, без ограничения общности мы можем представить каждый вектор $\mathcal{D}_i$ в виде $\left(\frac{m_1^{(i)}}{n_i}, \ldots, \frac{m_{h_i}^{(i)}}{n_i}\right)$, где $(m_1^{(i)}, \ldots, m_{h_i}^{(i)}) = 1$. Для $i = 1, \ldots, s$ и $j = 1, \ldots, h_i$ обозначим через $l_j^{(i)}$ наибольший общий делитель всех чисел $m_1^{(i)}, \ldots, m_{h_i}^{(i)}$, кроме числа $m_j^{(i)}$. В предыдущем параграфе было показано, что множества $T(\mathcal{D}_i) = \{l_1^{(i)}, \ldots, l_{h_i}^{(i)}\}^{>1}$ являются разделимыми и взаимно простыми с n_i. Положим $T(M) = (T(\mathcal{D}_1), \ldots, T(\mathcal{D}_s))$ в случае $s \geqslant 2$ и $T(M) = T(\mathcal{D}_1)$ в случае $s = 1$. Согласно утверждениям 19 и 8 имеем

Утверждение 20. *Множество $T(M)$ является разделимым и взаимно простым с каждым из чисел $n_1, \ldots, n_s$.*

Обозначим через $\Pi(M)$ множество простых чисел $\bigcup_{i=1}^{s} \mathcal{J}(n_i)$. В силу утверждения 20 мы можем рассмотреть множество $G\left[\Pi(M); T(M)\right]$. Основным результатом данной работы является

Теорема 1. $\langle M \rangle = G\left[\Pi(M); T(M)\right]$.

Для доказательства теоремы 1 мы воспользуемся двумя вспомогательными утверждениями, доказанными в [5].

Лемма 5. *Пусть* П *— множество простых чисел, A — конечное разделимое множество чисел, взаимно простых с множеством* П,

и H — замкнутое множество стохастических векторов, содержащее множество $G[\{p\}; A]$ для каждого p из Π. Тогда $G[\Pi; A] \subseteq H$.

Лемма 6. *Пусть p, q — два возможно одинаковых простых числа, A — конечное разделимое множество чисел, взаимно простых с p, B — взаимно простое с числом q разделимое множество, состоящее из не более чем двух чисел, H — замкнутое множество стохастических векторов, содержащее множества $G[\{p\}; A]$ и $G[\{q\}; B]$.*

Тогда

$$G[\{p\}; (A, B)] \subseteq H.$$

Лемма 6 может быть обобщена следующим образом.

Лемма 7. *Пусть p, q — два возможно одинаковых простых числа, A, B — конечные разделимые множества чисел, взаимно простые с числами p и q соответственно, H — замкнутое множество стохастических векторов, содержащее множества $G[\{p\}; A]$ и $G[\{q\}; B]$.*

Тогда

$$G[\{p\}; (A, B)] \subseteq H.$$

Доказательство. Для доказательства леммы применим индукцию по мощности $|B|$ множества B.

Базисом индукции для $|B| \leqslant 2$ служит лемма 6.

Пусть $i \geqslant 2$, и утверждение леммы доказано для всех множеств B таких, что $|B| \leqslant i$. Рассмотрим произвольное множество $B = \{b_1, \ldots, b_{i+1}\}$ из $i+1$ элементов. Обозначим через B' и B'' разделимые множества $\{b_1 b_2, b_3, \ldots, b_{i+1}\}$ и $\{b_1, \ldots, b_{i-1}, b_i b_{i+1}\}$ соответственно. Заметим, что $B = (B', B'')$, поэтому согласно утверждению 9 множества $G[\{q\}; B']$ и $G[\{q\}; B'']$ содержатся в $G[\{q\}; B]$. Следовательно, эти множества содержатся в H. Поэтому согласно индуктивному предположению множества $G[\{p\}; (A, B')]$ и $G[\{p\}; ((A, B'), B'')]$ также содержатся в H. Пользуясь ассоциативностью операции взятия наибольшего общего делителя разделимых множеств, имеем

$$((A, B'), B'') = (A, (B', B'')) = (A, B).$$

Таким образом,

$$G[\{p\}; (A, B)] = G[\{p\}; ((A, B'), B'')] \subseteq H.$$

Применяя индукцию по числу разделимых множеств, из леммы 7 получаем

Следствие 3. *Пусть $p_1, \ldots, p_s$ — возможно одинаковые простые числа, $A_1, \ldots, A_s$ — конечные разделимые множества, взаимно простые с числами $p_1, \ldots, p_s$ соответственно, H — замкнутое множество стохастических векторов, содержащее множества $G[\{p_i\}; A_i]$, $i = 1, \ldots, s$.*

Тогда

$$G[\{p_1\}; (A_1, \ldots, A_s)] \subseteq H.$$

Доказательство теоремы 1. Пусть $\mathscr{D} = (d_1; \ldots; d_h)$ — произвольный стохастический вектор из $\langle M \rangle$. Это означает, что для некоторой h-значной функции $f(x_1, \ldots, x_k)$ и некоторых векторов $\mathscr{D}_{\lambda(1)}, \ldots, \mathscr{D}_{\lambda(k)}$ из M выполняется соотношение $\mathscr{D} = \boldsymbol{P}\{f(\mathscr{D}_{\lambda(1)}, \ldots, \mathscr{D}_{\lambda(k)})\}$, т. е. согласно формулам (2) для каждого $i = 1, \ldots, h$ справедливо равенство

$$d_i = \boldsymbol{P}_{\mathscr{N}_{i-1}(f)}(\mathscr{D}_{\lambda(1)}, \ldots, \mathscr{D}_{\lambda(k)}). \tag{106}$$

Положим $R = n_{\lambda(1)} \dots n_{\lambda(k)}$ и для любого множества U наборов из $\Omega(\mathscr{D}_{\lambda(1)}, \dots, \mathscr{D}_{\lambda(k)})$ обозначим через $\mathscr{M}(U)$ число $R \cdot \boldsymbol{P}_U\left(\mathscr{D}_{\lambda(1)}, \dots, \mathscr{D}_{\lambda(k)}\right)$. Из формулы (1) вытекает, что

$$\mathscr{M}(U) = \sum_{(\sigma_1; \dots; \sigma_k) \in U} m_{(\sigma_1+1)}^{\lambda(1)} \dots m_{(\sigma_k+1)}^{\lambda(k)} \tag{107}$$

Таким образом, для любого U величина $\mathscr{M}(U)$ является целым числом, и согласно равенствам (106) для каждого $i = 1, \dots, h$ число d_i представимо дробью $\frac{\mathscr{M}(\mathscr{N}_{i-1}(f))}{R}$.

Пусть l — произвольное число из $T(M)$. Тогда $l = (l_{j_1}^{(1)}, \dots, l_{j_s}^{(s)})$ для некоторых $j_1, \dots, j_s$. Обозначим через $\widetilde{\sigma}(l)$ набор $(j_{\lambda(1)} - 1; \dots; j_{\lambda(k)} - 1)$ из $\Omega(\mathscr{D}_{\lambda(1)}, \dots, \mathscr{D}_{\lambda(k)})$. Пусть $\widetilde{\sigma} = (\sigma_1; \dots; \sigma_k)$ — произвольный набор из $\Omega(\mathscr{D}_{\lambda(1)}, \dots, \mathscr{D}_{\lambda(k)})$, отличный от $\widetilde{\sigma}(l)$. Тогда для некоторого i выполняется $\sigma_i \neq j_{\lambda(i)} - 1$. Заметим, что $m_{(\sigma_i+1)}^{\lambda(i)}$ делится на $l_{j_i}^{(i)}$, и, следовательно, делится на l. Таким образом, для любого набора $\widetilde{\sigma}$, отличного от $\widetilde{\sigma}(l)$, соответствующее этому набору слагаемое $m_{(\sigma_1+1)}^{\lambda(1)} \dots m_{(\sigma_k+1)}^{\lambda(k)}$ в сумме (107) содержит сомножитель $m_{(\sigma_i+1)}^{\lambda(i)}$, делителем которого является число l. Поэтому величина $\mathscr{M}(U)$ кратна числу l для любого множества U, не содержащего набора $\widetilde{\sigma}(l)$.

Для $i = 1 \dots, h-1$ обозначим через T_i подмножество множества $T(M)$, содержащее число $l \in T(M)$ в том и только том случае, когда $i \leqslant f\left(\widetilde{\sigma}(l)\right)$. Пусть $l \in T_i$. Тогда любое множество $\mathscr{N}_j(f)$, где $j < i$, не содержит набора $\widetilde{\sigma}(l)$. Поэтому любая величина $\mathscr{M}(\mathscr{N}_j(f))$, где $j < i$, является кратной числу l. Следовательно, сумма $\sum_{j=1}^{i} \mathscr{M}(\mathscr{N}_{j-1}(f))$ также является кратной числу l. Таким образом, эта сумма является кратной любому числу из T_i. Так как T_i состоит из попарно простых чисел, получаем тогда, что

$$\sum_{j=1}^{i} \mathscr{M}(\mathscr{N}_{j-1}(f)) \equiv 0 \pmod{\|T_i\|}. \tag{108}$$

Пусть теперь $l \in T(M) \setminus T_i$, т. е. $i > f\left(\widetilde{\sigma}(l)\right)$. Тогда любое множество $\mathscr{N}_j(f)$, где $j \geqslant i$, не содержит набора $\widetilde{\sigma}(l)$. Поэтому любая величина $\mathscr{M}(\mathscr{N}_j(f))$, где $j \geqslant i$, является кратной числу l. Тем самым сумма $\sum_{j=i+1}^{h} \mathscr{M}(\mathscr{N}_{j-1}(f))$ также является кратной числу l. Таким образом, эта сумма является кратной любому числу из $T(M) \setminus T_i$, при этом все числа из $T(M) \setminus T_i$ попарно просты.

Следовательно,

$$\sum_{j=i+1}^{h} \mathscr{M}(\mathscr{N}_{j-1}(f)) \equiv 0 \pmod{\|T(M) \setminus T_i\|}. \tag{109}$$

Из равенства $\sum_{j=1}^{h} d_j = 1$ вытекает, что $\sum_{j=1}^{h} \mathscr{M}(\mathscr{N}_{j-1}(f)) = R$, поэтому из соотношения (109) получаем, что

$$\sum_{j=1}^{i} \mathscr{M}(\mathscr{N}_{j-1}(f)) \equiv R \pmod{\|T(M) \setminus T_i\|}. \tag{110}$$

Кроме того, из определения множеств $T_1, \ldots, T_{h-1}$ следует, что

$$T_1 \supseteq T_2 \supseteq \ldots \supseteq T_{h-1}. \tag{111}$$

В силу соотношений (108), (110), (111) и очевидного соотношения $\mathcal{J}(R) \subseteq \subseteq \Pi(M)$ стохастический вектор

$$\mathcal{D} = \left(\frac{\mathcal{M}(\mathcal{N}_0(f))}{R}; \frac{\mathcal{M}(\mathcal{N}_1(f))}{R}; \ldots; \frac{\mathcal{M}(\mathcal{N}_{h-1}(f))}{R}\right)$$

принадлежит $G\left[\Pi(M); T(M)\right]$. Таким образом, $\langle M\rangle \subseteq G\left[\Pi(M); T(M)\right]$.

Покажем теперь, что $G[\Pi(M); T(M)] \subseteq \langle M\rangle$. В силу следствия 2 это соотношение верно для $s = 1$, поэтому будем предполагать, что $s \geqslant 2$. Пусть p_1 — произвольное простое число из $\Pi(M)$. Без ограничения общности мы можем считать, что p_1 является делителем числа n_1. Обозначим через $p_2, \ldots, p_s$ произвольные простые делители чисел $n_2, \ldots, n_s$ соответственно. Отметим, что согласно утверждению 1 множество $\langle M\rangle$ является замкнутым. Согласно следствию 2 для каждого $i = 1, \ldots, s$ имеем $G[\mathcal{J}(n_i); T(\mathcal{D}_i)] \subseteq \langle\{\mathcal{D}_i\}\rangle \subseteq \langle M\rangle$. Следовательно, $\langle M\rangle$ содержит для каждого $i = 1, \ldots, s$ подмножество $G[\{p_i\}; T(\mathcal{D}_i)]$ множества $G[\mathcal{J}(n_i); T(\mathcal{D}_i)]$. Поэтому, применяя следствие 3, получаем, что $G[\{p_1\}; T(M)] \subseteq \langle M\rangle$ для любого p_1 из $\Pi(M)$. Тогда из леммы 5 вытекает, что $G[\Pi(M); T(M)] \subseteq \langle M\rangle$.

Исходя из теоремы 1, мы можем для любого стохастического вектора $\mathcal{D}$ эффективно определить, порождается ли этот вектор множеством M. Отметим, что, поскольку $\langle M\rangle \subseteq \boldsymbol{SQ}$, из $\mathcal{D} \notin \boldsymbol{SQ}$ следует $\mathcal{D} \notin \langle M\rangle$. Предположим, что $\mathcal{D} \in \boldsymbol{SQ}$, и все компоненты вектора $\mathcal{D}$ заданы несократимыми дробями. Будем также предполагать, что все компоненты векторов из M заданы изначально несократимыми дробями. Пусть h — размерность вектора $\mathcal{D}$ и $\eta_{\mathcal{D}}$ — произведение знаменателей всех компонент этого вектора. Положим $\Lambda_M = \max\limits_{i,j} m_j^{(i)}$, $h_M = \max\limits_i h_i$ и $p_M = \prod\limits_i h_i$. В [5] получено явное описание множества $\langle M\rangle$ в случае, если M состоит из двумерных векторов, и на основе этого результата показано, как проверить в этом случае принадлежность вектора $\mathcal{D}$ множеству $\langle M\rangle$ с помощью $O\left(2^s(\log \Lambda_M + h) + \log\log \eta_{\mathcal{D}}\right)$ арифметических операций.

Используя аналогичные рассуждения и теорему 1, мы можем обобщить алгоритм проверки на случай множества M, состоящего из векторов произвольной размерности.

Теорема 2. *Если все компоненты векторов из M и вектора $\mathcal{D}$ заданы несократимыми дробями, то для проверки соотношения $\mathcal{D} \in \langle M\rangle$ достаточно выполнить не более чем $O\left(p_M(\log \Lambda_M + h_M + h) + \log\log \eta_{\mathcal{D}}\right)$ арифметических операций.*

§ 6. Заключение

Интересным направлением дальнейших исследований является возможное обобщение полученных результатов на случай замыканий произвольных множеств стохастических векторов из $\boldsymbol{SQ}$ и описание всех замкнутых подмножеств множества $\boldsymbol{SQ}$.

СПИСОК ЛИТЕРАТУРЫ

1. Бухараев Р. Г. Основы теории вероятностных автоматов. — М.: Наука, 1985.
2. Виноградов И. М. Основы теории чисел. — М.: Наука, 1981.
3. Колпаков Р. М. Замкнутые классы булевых случайных величин с рациональнозначными распределениями // Математические вопросы кибернетики. Вып. 10. — М.: Физматлит, 2001. — С. 215–224.
4. Колпаков Р. М. О многозначных преобразованиях одноэлементных множеств бинарных распределений с рациональными вероятностями // Математические вопросы кибернетики. Вып. 11. — М.: Физматлит, 2002. — С. 63–76.
5. Колпаков Р. М. О многозначных преобразованиях конечных множеств бинарных распределений с рациональными вероятностями // Дискретная математика. (в печати).
6. Нурмеев Н. Н. О булевых функциях с аргументами, принимающими случайные значения // Тез. докл. VIII Всесоюзн. конф. «Проблемы теоретической кибернетики». Горький, 1988. — Ч. 2. — С. 59–60.
7. 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.
8. Салимов Ф. И. Конечная порожденность некоторых алгебр над случайными величинами // Вопросы кибернетики. Вып. 86. — М., 1982. — С. 122–130.
9. Салимов Ф. И. О максимальных подалгебрах алгебр распределений // Известия вузов. Сер. Математика. — 1985. — № 7. — С. 14–20.
10. Салимов Ф. И. Об одном семействе алгебр распределений // Известия вузов. Сер. Матем. — 1988. — № 7. — С. 64–72.
11. Схиртладзе Р. Л. О синтезе p-схемы из контактов со случайными дискретными состояниями // Сообщ. АН ГрССР. — 1961. — Т. 26, № 2. — С. 181–186.
12. 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.
13. Srinivasan A., Zuckerman D. Computing with very weak random Sources // SIAM J. on Computing. — 1999. — V. 28. — № 4. — P. 1433–1459.

Поступило в редакцию 27 XI 2003