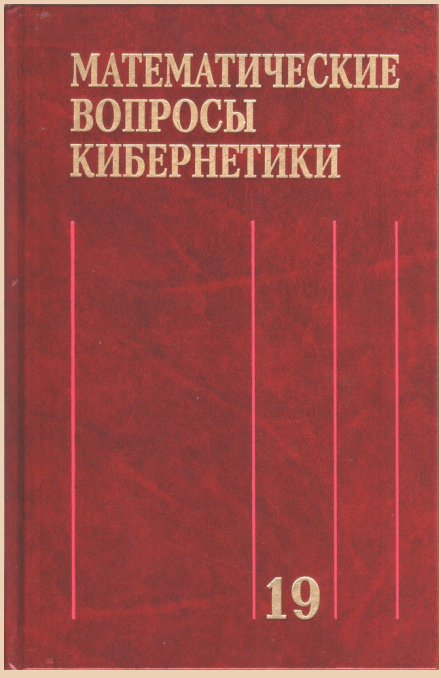
ИПМ им. М.В. Келдыша РАН • Электронная библиотека
Математические вопросы кибернетики • Выпуск 19



Р. М. Колпаков

О дискретных преобразованиях вероятностных распределений

Рекомендуемая форма библиографической ссылки: Колпаков Р. М. О дискретных преобразованиях вероятностных распределений // Математические вопросы кибернетики. Вып. 19. — М.: ФИЗМАТЛИТ, 2019. — С. 5–20. URL: http://library.keldysh.ru/mvk.asp?id=2019-5

О ДИСКРЕТНЫХ ПРЕОБРАЗОВАНИЯХ ВЕРОЯТНОСТНЫХ РАСПРЕДЕЛЕНИЙ*)

Р. М. КОЛПАКОВ

(МОСКВА)

Данная работа представляет обзор результатов, связанных с дискретными преобразованиями независимых вероятностных распределений. Под дискретным преобразованием вероятностных распределений понимается вероятностное распределение конечной случайной величины, значение которой является функцией от значений случайных величин с исходными вероятностными распределениями. Данные преобразования играют важную роль в структурной теории вероятностных автоматов и вопросах реализации управляемых генераторов случайных кодов (см. [1, 44]), поскольку задача реализации таких генераторов фактически заключается в построении некоторой случайной величины ζ_0 с произвольным требуемым распределением из имеющихся в распоряжении исходных источников случайностей $\zeta_1, \ldots, \zeta_k$ с фиксированными вероятностными распределениями, отличными от требуемого распределения. Значение случайной величины ζ_0, очевидно, должно быть функцией от значений случайных величин $\zeta_1, \ldots, \zeta_k$. Поэтому построение величины ζ_0 состоит в задании функции $f : \Omega_1 \times \ldots \times \Omega_k \longrightarrow \Omega_0$, где Ω_i — множество значений случайной величины ζ_i, $i = 0, 1, \ldots, k$. Отметим, что если случайные величины $\zeta_1, \ldots, \zeta_k$ являются независимыми в совокупности, вероятностное распределение случайной величины ζ_0 однозначно определяется функцией f и вероятностными распределениями величин $\zeta_1, \ldots, \zeta_k$. Поэтому в этом случае мы можем говорить о том, что вероятностное распределение величины ζ_0 *порождается* множеством вероятностных распределений величин $\zeta_1, \ldots, \zeta_k$ посредством функции f. Соответственно мы говорим, что вероятностное распределение *порождается* множеством вероятностных распределений, если это распределение порождается данным множеством посредством какой-либо подходящей функции.

При исследовании данного порождения вероятностных распределений мы в первую очередь сталкиваемся с проблемой выразимости, т. е. проблемой, заключающейся в том, чтобы выяснить, порождается ли заданное вероятностное распределение заданным множеством исходных вероятностных распределений. Принципиальная трудность этой проблемы состоит, очевидно, в невозможности непосредственного описания произвольных

*) Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований (проект №14–01–00598).

множеств вероятностных распределений, поскольку даже в случае распределений случайных величин, принимающих только два значения (бинарных вероятностных распределений), мощность множества всех таких распределений равна континууму. Поэтому естественным подходом в исследовании проблемы выразимости является рассмотрение этой проблемы для не более чем счетных подмножеств вероятностных распределений, всюду плотных на множестве всех вероятностных распределений. В случае распределений конечных случайных величин (конечных распределений) наиболее подходящим примером такого подмножества представляется множество $\boldsymbol{SQ}$ всевозможных конечных распределений, состоящих из рациональных вероятностей. В этом случае мы имеем проблему выразимости для распределений из $\boldsymbol{SQ}$, т. е. проблему определения порождаемости заданного вероятностного распределения заданным множеством исходных вероятностных распределений из $\boldsymbol{SQ}$. Для произвольного непустого множества П различных простых чисел во множестве $\boldsymbol{SQ}$ естественным образом выделяется подмножество $SG[\text{П}]$ всевозможных распределений вероятностей, представимых дробями, все простые делители знаменателей которых принадлежат множеству П.

Другой важной проблемой, тесно связанной с проблемой выразимости, является проблема описания всех множеств распределений из $\boldsymbol{SQ}$, замкнутых относительно рассматриваемого порождения распределений. Простейшим примером таких замкнутых множеств представляют упомянутые выше множества $SG[\text{П}]$. Отметим, что с практической точки зрения среди множеств вероятностных распределений наибольший интерес представляют *конечно-порожденные* множества, т. е. множества, порождаемые своими конечными подмножествами.

Важным частным случаем конечных вероятностных распределений являются бинарные вероятностные распределения. Поскольку бинарное вероятностное распределение однозначно определяется какой-либо одной из вероятностей этого распределения, мы имеем взаимно-однозначное соответствие между бинарными распределениями и числами из сегмента $[0; 1]$. Поэтому для удобства вместо бинарных распределений рассматриваются соответствующие этим распределениям числа. В таком случае множеству всех бинарных распределений из $\boldsymbol{SQ}$ соответствует множество $\boldsymbol{PQ}$ всех рациональных чисел из сегмента $[0; 1]$, а множеству всех бинарных распределений из $SG[\text{П}]$ соответствует множество $G[\text{П}]$ всех чисел из $\boldsymbol{PQ}$, представимых дробями, знаменатели которых являются произведениями степеней чисел из множества П. Введенное выше понятие порождения вероятностных распределений из $\boldsymbol{SQ}$ в этом случае естественным образом трансформируется в понятие порождения рациональных чисел из $\boldsymbol{PQ}$. Изучение порождения чисел из $\boldsymbol{PQ}$ было начато Р. Схиртладзе в работе [31], в которой установлено, что множество $G[\{2\}]$ порождается одним числом $\frac{1}{2}$, и показано таким образом, что это множество является конечно-порожденным. Им же в [33] доказан аналогичный результат для множества $G[\{3\}]$. Ф. Салимовым в [26] получено, что для любого конечного П, содержащего числа 2 или 3, существуют двухэлементные подмножества множества $G[\text{П}]$, порождающие это множество. Им же в [29] установлена конечная порожденность множеств $G[\text{П}]$ для любого конечного П, и таким образом показано, что

множество $G[\Pi]$ является конечно-порожденным тогда и только тогда, когда Π конечно.

Мы даем для любого множества чисел из $\boldsymbol{PQ}$ явное описание всех чисел, порождаемых этим множеством, и тем самым получаем полное решение проблемы выразимости для бинарных распределений из $\boldsymbol{SQ}$. Для этого введем ряд вспомогательных понятий и обозначений.

Для натурального n через $\mathcal{J}(n)$ обозначим множество всех простых делителей числа n. Для множества натуральных чисел T через $T^{>k}$ обозначается подмножество всех чисел из T, больших числа k, и через $|T|$ обозначается мощность множества T. Если множество T конечно, через $\|T\|$ обозначается произведение всех чисел множества T. Для пустого множества полагаем $\|\varnothing\| = 1$. Множество натуральных чисел, больших 1, называется *разделимым*, если оно содержит меньше двух чисел либо все его числа попарно просты. Множество натуральных чисел называется *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. Непустое разделимое множество B называется *делителем* разделимого множества A, если для любого числа b из B множество A содержит число, кратное числу b. Пустое множество считается делителем любого разделимого множества. Кроме того, далее мы используем 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.

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

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

состоящее из отличных от 1 наибольших общих делителей всевозможных выборок из s чисел по одному числу из каждого множества $A_1, \ldots, A_s$. Если хотя бы одно из множеств $A_1, \ldots, A_s$ является пустым, то $(A_1, \ldots, A_s) = \varnothing$.

Понятие наибольшего общего делителя можно также ввести для бесконечного числа конечных разделимых множеств. Пусть $A_1, A_2, \ldots$ — конечные разделимые множества. Тогда *наибольшим общим делителем* $(A_1, A_2, \ldots)$ этих множеств называется множество

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

состоящее из всех тех чисел из $\mathbb{N}^{>1}$, которые являются наибольшими общими делителями бесконечных выборок чисел из множеств $A_1, A_2, \ldots$ по одному числу из каждого множества. Если хотя бы одно из множеств $A_1, A_2, \ldots$ пусто, то $(A_1, A_2, \ldots) = \varnothing$.

Пусть H — множество чисел из $\boldsymbol{PQ}$. Число $a \in [0; 1]$ порождается множеством H, если существует булева функция $f(x_1, \ldots, x_k)$ такая, что для некоторых $\rho_1, \ldots, \rho_k$ из H выполняется соотношение

$$a = \sum_{(\sigma_1, \ldots, \sigma_k) \in \{0,1\}^k} (\rho_1)_{\sigma_1} \cdot \ldots \cdot (\rho_k)_{\sigma_k} f(\sigma_1, \ldots, \sigma_k),$$

где

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

Через $\langle H \rangle$ обозначается замыкание множества H, т.е. множество всех чисел, порождаемых множеством H. Множество $A \subseteq [0;1]$ порождается множеством H, если $A \subseteq \langle H \rangle$. Множество H называется *замкнутым*, если $H = \langle H \rangle$.

Пусть t_1, t_2 — взаимно простые натуральные числа, Π — произвольное непустое множество различных простых чисел, взаимно простых с t_1 и t_2. Через $G[\Pi; t_1 : t_2]$ обозначается следующее подмножество множества $G[\Pi]$:

$$G[\Pi; t_1 : t_2] = \left\{ a = \frac{m}{n} \;\middle|\; \begin{array}{l} 0 \leqslant a \leqslant 1,\ m \in \mathbb{Z}^+,\ n \in \mathbb{N}^{>1},\ \mathscr{J}(n) \subseteq \Pi, \\ m \equiv 0 \pmod{t_1},\ m \equiv n \pmod{t_2} \end{array} \right\}.$$

Пусть T — конечное разделимое множество натуральных чисел, взаимно простых с множеством Π. Через $G[\Pi; T]$ обозначается следующее подмножество множества $G[\Pi]$:

$$G[\Pi; T] = \bigcup_{T' \subseteq T} G[\Pi; \|T'\| : \|T \setminus T'\|],$$

где объединение берется по всем (в том числе и несобственным) подмножествам T' множества T. В случае $T = \varnothing$ полагаем $G[\Pi; \varnothing] = G[\Pi]$. Можно показать, что любое множество $G[\Pi; T]$ является замкнутым.

Обозначим через $\boldsymbol{G}$ совокупность всех множеств $G[\Pi; T]$. Отношение включения между любыми множествами из $\boldsymbol{G}$ определяется следующим образом. Пусть $G[\Pi_1; T_1]$, $G[\Pi_2; T_2]$ — два множества из $\boldsymbol{G}$. Тогда

1. $G[\Pi_1; T_1] \subseteq G[\Pi_2; T_2]$ тогда и только тогда, когда $\Pi_1 \subseteq \Pi_2$ и $T_2^{>2}$ является делителем множества T_1;
2. $G[\Pi_1; T_1] = G[\Pi_2; T_2]$ тогда и только тогда, когда $\Pi_1 = \Pi_2$ и $T_1^{>2} = T_2^{>2}$.

Без ограничения общности в качестве чисел из множества $\boldsymbol{PQ}$ можно рассматривать только несократимые дроби из интервала $(0;1)$. Пусть $\frac{l}{n}$ — произвольная несократимая дробь из этого интервала. Тогда множество $\{l, n-l\}^{>2}$ является разделимым множеством, взаимно простым с числом n. Поэтому можно рассмотреть множество $G[\mathscr{J}(n); \{l, n-l\}^{>2}]$.

Т е о р е м а 1. *Для любой несократимой дроби* $\frac{l}{n}$ *из интервала* $(0;1)$ *выполняется соотношение*

$$\left\langle \left\{ \frac{l}{n} \right\} \right\rangle = G[\mathscr{J}(n); \{l, n-l\}^{>2}].$$

Теорему 1 можно обобщить на случай произвольных конечных подмножеств множества $\boldsymbol{PQ}$. Пусть $H = \left\{ \frac{m_1}{n_1}, \ldots, \frac{m_s}{n_s} \right\}$ — произвольное конечное множество несократимых дробей из интервала $(0;1)$. Положим

$$T(H) = \begin{cases} \left(\{m_1, n_1 - m_1\}^{>1}, \ldots, \{m_s, n_s - m_s\}^{>1} \right), & \text{если } s \geqslant 2; \\ \{m_1, n_1 - m_1\}^{>1}, & \text{если } s = 1; \end{cases}$$

и $\Pi(H) = \bigcup_{i=1}^{s} \mathscr{J}(n_i)$. Можно показать, что множество $T(H)$ является разделимым и взаимно простым с любым числом из $\Pi(H)$. Поэтому можно рассмотреть множество $G[\Pi(H); T(H)^{>2}]$.

Т е о р е м а 2. *Для любого конечного множества H несократимых дробей из интервала* $(0; 1)$ *выполняется соотношение*

$$\langle H\rangle = G[\Pi(H); T(H)^{>2}].$$

Из теоремы 2 вытекает следующий критерий порождаемости множества $G[\Pi]$, где Π конечно, заданным конечным подмножеством.

Т е о р е м а 3. *Пусть Π — произвольное конечное множество различных простых чисел, $H = \left\{\frac{m_1}{n_1}, \ldots, \frac{m_s}{n_s}\right\}$ — конечное множество несократимых дробей из $G[\Pi]$, $d = \big(m_1(n_1 - m_1), \ldots, m_s(n_s - m_s)\big)$ при $s \geqslant 2$ и $d = m_1(n_1 - m_1)$ при $s = 1$. Для того чтобы $\langle H\rangle = G[\Pi]$, необходимо и достаточно выполнение следующих двух условий:*

а) *для любого $p \in \Pi$ во множестве $\{n_1, \ldots, n_s\}$ найдется число, кратное p;*

б) $d \leqslant 2$.

Теорема 2 позволяет также предложить эффективный алгоритм решения задачи выразимости в $\boldsymbol{PQ}$. Пусть множество H состоит из s несократимых дробей $\frac{m_1}{n_1}, \ldots, \frac{m_s}{n_s}$ из интервала $(0; 1)$. Обозначим через Λ_H величину $\max(m_1, \ldots, m_s, n_1 - m_1, \ldots, n_s - m_s)$. Пусть число a также задано некоторой несократимой дробью $\frac{m}{n}$ (если $a \notin \boldsymbol{PQ}$, то, очевидно, $a \notin \langle H\rangle$). Положим $\eta_a = n$. На основании теоремы 2 проверка соотношения $a \in \langle H\rangle$ требует выполнения не более $O\big(s \log \Lambda_H + \log\log \eta_a\big)$ арифметических операций. Таким образом, получаем, что задача выразимости в $\boldsymbol{PQ}$ разрешима за полиномиальное время.

Теорема 2 может быть модифицирована для случая замыканий произвольных бесконечных множеств чисел из $\boldsymbol{PQ}$. Пусть $H = \left\{\frac{m_1}{n_1}, \frac{m_2}{n_2}, \ldots\right\}$ — бесконечное множество несократимых дробей из интервала $(0; 1)$. Тогда положим

$$T(H) = \big(\{m_1, n_1 - m_1\}^{>1}, \{m_2, n_2 - m_2\}^{>1}, \ldots\big),$$

и $\Pi(H) = \bigcup_{i=1}^{\infty} \mathscr{J}(n_i)$. В таком случае множество $T(H)$ также является разделимым и взаимно простым с любым числом из $\Pi(H)$. Поэтому снова можно рассмотреть множество $G[\Pi(H); T(H)^{>2}]$.

Т е о р е м а 4. *Для любого бесконечного множества H несократимых дробей из интервала* $(0; 1)$ *выполняется соотношение*

$$\langle H\rangle = G[\Pi(H); T(H)^{>2}].$$

Таким образом, теоремы 2 и 4 дают полное решение проблемы выразимости для чисел из $\boldsymbol{PQ}$.

Ряд исследований также был посвящен вопросам описания замкнутых множеств чисел из $\boldsymbol{PQ}$ и выяснения структуры диаграммы включений для этих множеств. Ф. Салимовым в [29] доказано, что в случае бинарных распределений для любого множества Π различных простых чисел и любого

числа p из Π множество $G[\Pi \setminus \{p\}]$ является предполным (замкнутое множество A называется *предполным* классом в множестве B, если $A \subset B$ и не существует замкнутого множества C такого, что $A \subset C \subset B$) замкнутым классом в множестве $G[\Pi]$. Таким образом, была установлена структура диаграммы включений для множеств $G[\Pi]$. Кроме того, в [29] было показано, что существуют замкнутые множества бинарных распределений из $\boldsymbol{SQ}$, отличные от множеств $G[\Pi]$.

Отметим, что любой из замкнутых классов чисел из $\boldsymbol{PQ}$ является замыканием некоторого своего подмножества (например, самого этого класса). Поэтому из теорем 2 и 4 следует, что любой замкнутый класс чисел из $\boldsymbol{PQ}$ является элементом множества $\boldsymbol{G}$. Таким образом, $\boldsymbol{G}$ — множество всех замкнутых подмножеств множества $\boldsymbol{PQ}$. Можно показать, что любое замкнутое множество чисел из $\boldsymbol{PQ}$ имеет базис (порождающее подмножество некоторого множества называется *базисом*, если любое собственное подмножество этого подмножества не является порождающим для данного множества). Кроме того, для каждого замкнутого множества чисел из $\boldsymbol{PQ}$ можно дать следующее описание всех его предполных классов. Для случая множества $G[\Pi]$ мы полагаем

$$S_0[\Pi] = \begin{cases} \bigcup\limits_{p \in \Pi} \{G[\Pi \setminus \{p\}]\}, & \text{если } |\Pi| > 1; \\ \varnothing, & \text{если } |\Pi| = 1. \end{cases}$$

Через $\mathbb{P}$ обозначаем множество всех простых чисел.

У т в е р ж д е н и е 1. *Пусть S — множество всех предполных классов в множестве $G[\Pi]$. Тогда*

1. *Если Π содержит число 2, то*

$$S = S_0[\Pi] \cup \bigcup_{t \in \mathbb{P} \setminus \Pi} \{G[\Pi; \{t\}]\};$$

2. *Если Π не содержит числа 2, то*

$$S = S_0[\Pi] \cup \{G[\Pi; \{4\}]\} \cup \bigcup_{t \in \mathbb{P} \setminus (\Pi \cup \{2\})} \{G[\Pi; \{t\}]\}.$$

Для случая множества $G[\Pi; T]$, где $T = \{t_1, \ldots, t_q\}$, $q \geqslant 1$, мы полагаем

$$S_0[\Pi; T] = \begin{cases} \bigcup\limits_{p \in \Pi} \{G[\Pi \setminus \{p\}; T]\}, & \text{если } |\Pi| > 1; \\ \varnothing, & \text{если } |\Pi| = 1; \end{cases}$$

$$S_1[\Pi; T] = \bigcup_{r \in \mathcal{I}(\|T\|)} \{G[\Pi; T \cup \{t^{(r)} \cdot r\} \setminus \{t^{(r)}\}]\},$$

где через $t^{(r)}$ обозначается единственное число из T, кратное r, и

$$S_2[\Pi; T] = \bigcup_{1 \leqslant i < j \leqslant q} \{\{G[\Pi; T \cup \{t_i t_j\} \setminus \{t_i, t_j\}]\}.$$

Утверждение 2. *Пусть S — множество всех предполных классов в множестве $G[\Pi; T]$, где T непусто. Тогда*

1. *Если либо* Π, *либо* $\mathscr{I}(\|T\|)$ *содержит число* 2, *то*

$$S = S_0[\Pi; T] \cup \bigcup_{t \in \mathbb{P} \setminus (\Pi \cup \mathscr{I}(\|T\|))} \{G[\Pi; T \cup \{t\}]\} \cup S_1[\Pi; T] \cup S_2[\Pi; T];$$

2. *Если ни* Π, *ни* $\mathscr{I}(\|T\|)$ *не содержит числа* 2, *то*

$$S = S_0[\Pi; T] \cup \{G[\Pi; T \cup \{4\}]\} \cup \bigcup_{t \in \mathbb{P} \setminus (\Pi \cup \mathscr{I}(\|T\|) \cup \{2\})} \{G[\Pi; T \cup \{t\}]\} \cup$$
$$\cup \bigcup_{t \in T} \{G[\Pi; T \cup \{2t\} \setminus \{t\}]\} \cup S_1[\Pi; T] \cup S_2[\Pi; T].$$

Таким образом, в каждом из замкнутых подмножеств множества $\boldsymbol{PQ}$ имеется счетное число предполных классов.

Обозначим через $\boldsymbol{G_{fin}}$ подмножество множества $\boldsymbol{G}$, состоящее из всех множеств $G[\Pi; T]$ таких, что Π конечно. Можно показать, что замкнутое подмножество множества $\boldsymbol{PQ}$ является конечно-порожденным тогда и только тогда, когда это подмножество является элементом множества $\boldsymbol{G_{fin}}$. Таким образом, $\boldsymbol{G_{fin}}$ является множеством всех конечно-порожденных замкнутых подмножеств множества $\boldsymbol{PQ}$. Более того, можно доказать, что любое множество $G[\Pi, T]$ из $\boldsymbol{G_{fin}}$ порождается некоторым своим подмножеством, содержащим не более $|T|+2$ чисел.

Рассмотрим теперь случай произвольных распределений из $\boldsymbol{SQ}$. Заметим, что каждому конечному вероятностному распределению может быть сопоставлен вектор вероятностей этого распределения. Отметим, что этот вектор является *стохастическим*, т. е. все его компоненты неотрицательны и их сумма равна 1. Таким образом, без ограничения общности вероятностные распределения из $\boldsymbol{SQ}$ могут рассматриваться как стохастические векторы, все компоненты которых являются рациональными числами. Случай произвольных распределений из $\boldsymbol{SQ}$ исследовался ранее Ф. Салимовым в работах [27, 28, 30]. В [27] им было показано, что все множества $SG[\Pi]$, где Π конечно, порождаются одноэлементными подмножествами, и тем самым установлено, что множество $SG[\Pi]$ является конечно-порожденным тогда и только тогда, когда Π конечно. Им же в [28] доказано, что для любого множества Π различных простых чисел и любого числа p из Π множество $SG[\Pi \setminus \{p\}]$ является предполным классом в множестве $SG[\Pi]$. Таким образом, диаграмма включений для множеств $SG[\Pi]$ полностью совпадает с диаграммой включений для множеств $G[\Pi]$. Кроме того, в [28] было найдено дополнительное семейство замкнутых множеств распределений из SQ, являющихся предполными классами в множествах $SG[\Pi]$, и показано таким образом, что в каждом множестве $SG[\Pi]$ имеется по крайней мере счетное число предполных классов. Из полученных нами результатов вытекает, что никаких других предполных классов, кроме найденных в [28], в множествах $SG[\Pi]$ не существует, т. е. что в [28] были в действительности найдены все предполные классы в множествах $SG[\Pi]$.

Результаты, полученные нами для бинарных распределений, могут быть также обобщены на случай произвольных распределений из $\boldsymbol{SQ}$. В частности, для любого множества распределений из $\boldsymbol{SQ}$ мы даем явное описание всех распределений, порождаемых этим множеством. Для этого дополнительно введем ряд вспомогательных понятий и обозначений.

Пусть $\mathscr{D}_1, \ldots, \mathscr{D}_k$ — стохастические векторы размерности $h_1, \ldots, h_k$ соответственно. Через $\mathscr{D}[j]$ будем обозначать j-ю компоненту стохастического вектора $\mathscr{D}$. Обозначим через $\Omega(\mathscr{D}_1, \ldots, \mathscr{D}_k)$ множество $\{0, 1, \ldots, h_1 - 1\} \times \ldots \times \{0, 1, \ldots, h_k - 1\}$. Для любого непустого подмножества E этого множества положим

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

В случае $E = \varnothing$ полагаем $\boldsymbol{P}_{\varnothing}(\mathscr{D}_1, \ldots, \mathscr{D}_k) = 0$. Для функции $f : \Omega(\mathscr{D}_1, \ldots, \mathscr{D}_k) \longrightarrow \{0, 1, \ldots, h - 1\}$ будем обозначать через $\mathscr{N}_i(f)$, где $i = 0, 1, \ldots, h - 1$, множество всех наборов из $\Omega(\mathscr{D}_1, \ldots, \mathscr{D}_k)$, на которых функция f принимает значение i. Пусть H — множество различных стохастических векторов. Стохастический вектор $\mathscr{D}$ размерности h порождается множеством H, если для некоторых $\mathscr{D}_1, \ldots, \mathscr{D}_k$ из H найдется функция $f : \Omega(\mathscr{D}_1, \ldots, \mathscr{D}_k) \longrightarrow \{0, 1, \ldots, h-1\}$ такая, что

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

Через $\langle H \rangle$ обозначается замыкание множества H, т. е. множество всех стохастических векторов, порождаемых множеством H. Множество H называется *замкнутым*, если $\langle H \rangle = H$. Множество A стохастических векторов порождается множеством H, если $A \subseteq \langle H \rangle$.

Пусть Π — произвольное непустое множество различных простых чисел, T — конечное разделимое множество натуральных чисел, взаимно простых со множеством Π. Обозначим через $SG[\Pi; T]$ следующее подмножество множества $SG[\Pi]$:

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

при этом рассматриваемые здесь подмножества $T_1 \ldots, T_{h-1}$ множества T могут быть несобственными. В случае $T = \varnothing$ полагаем $SG[\Pi; \varnothing] = SG[\Pi]$. Можно показать, что любое множество $SG[\Pi; T]$ является замкнутым.

Через $\boldsymbol{SG}$ обозначим совокупность всех множеств $SG[\Pi; T]$. Отношение включения между любыми множествами из $\boldsymbol{SG}$ определяется следующим образом. Пусть $SG[\Pi'; T']$, $SG[\Pi''; T'']$ — два множества из $\boldsymbol{SG}$. Тогда

1. $SG[\Pi'; T'] \subseteq SG[\Pi''; T'']$ тогда и только тогда, когда $\Pi' \subseteq \Pi''$ и T'' является делителем множества T';

2. $SG[\Pi'; T'] = SG[\Pi''; T'']$ тогда и только тогда, когда $\Pi' = \Pi''$ и $T' = T''$.

Отметим, что в общем случае диаграмма включений для замкнутых множеств бинарных распределений из $\boldsymbol{SQ}$ является сужением диаграммы включений для замкнутых множеств произвольных распределений из $\boldsymbol{SQ}$.

Заметим, что для решения задачи выразимости в множестве $\boldsymbol{SQ}$ без ограничения общности можно рассматривать только замыкания множеств, состоящих из *позитивных* векторов, т. е. векторов, все компоненты которых отличны от чисел 0 и 1. Рассмотрим сначала простейший случай замыкания множества, состоящего из одного двумерного позитивного вектора $\mathscr{D} \in \boldsymbol{SQ}$. Без ограничения общности можно полагать, что $\mathscr{D} = \left(1 - \frac{l}{n}; \frac{l}{n}\right)$, где $l, n \in \mathbb{N}$, $(l, n) = 1$. Положим $T(\mathscr{D}) = \{l, n-l\}^{>1}$ и $\Pi(\mathscr{D}) = \mathscr{I}(n)$. Множество $T(\mathscr{D})$ является разделимым и взаимно простым с любым числом из $\Pi(\mathscr{D})$, поэтому мы можем рассмотреть множество $SG[T(\mathscr{D}); T(\mathscr{D})]$. Можно доказать, что $\langle\{\mathscr{D}\}\rangle = SG[\Pi(\mathscr{D}); T(\mathscr{D})]$. Данное соотношение можно обобщить на случай замыканий произвольных одноэлементных множеств векторов из $\boldsymbol{SQ}$. Для этого рассматривается произвольный позитивный вектор $\mathscr{D} = (d_1; \ldots; d_t)$ из $\boldsymbol{SQ}$, где $t \geqslant 3$. Без ограничения общности можно предполагать, что компоненты вектора $\mathscr{D}$ представлены дробями, приведенными к наименьшему общему знаменателю n, т. е. $d_i = \frac{m_i}{n}$, где $i = 1, \ldots, t$ и $(m_1, \ldots, m_t) = 1$. Для $j = 1, \ldots, t$ обозначим через l_j наибольший общий делитель всех чисел $m_1, \ldots, m_t$, кроме числа m_j. Положим $T(\mathscr{D}) = \{l_1, \ldots, l_t\}^{>1}$ и $\Pi(\mathscr{D}) = \mathscr{I}(n)$. Тогда, как и для случая двумерного вектора, множество $T(\mathscr{D})$ является разделимым и взаимно простым с любым числом из $\Pi(\mathscr{D})$. Поэтому мы снова можем рассмотреть множество $SG[T(\mathscr{D}); T(\mathscr{D})]$. Можно доказать, что в этом случае также выполняется равенство $\langle\{\mathscr{D}\}\rangle = SG[\Pi(\mathscr{D}); T(\mathscr{D})]$. Таким образом, имеет место

Т е о р е м а 5. *Для любого позитивного вектора $\mathscr{D}$ из $\boldsymbol{SQ}$ справедливо соотношение $\langle\{\mathscr{D}\}\rangle = SG[\Pi(\mathscr{D}); T(\mathscr{D})]$.*

Рассмотрим теперь случай замыканий конечных множеств двумерных векторов. Пусть $M = \{\mathscr{D}_1, \ldots, \mathscr{D}_s\}$ — произвольное конечное множество двумерных позитивных векторов из $\boldsymbol{SQ}$. Как и для случая одноэлементного множества, мы полагаем

$$\mathscr{D}_i = \left(1 - \frac{m_i}{n_i}; \frac{m_i}{n_i}\right),$$

где $m_i, n_i \in \mathbb{N}$, $(m_i, n_i) = 1$, $i = 1, \ldots, s$. Положим

$$T(M) = \begin{cases} \big(T(\mathscr{D}_1), \ldots, T(\mathscr{D}_s)\big), & \text{если } s \geqslant 2; \\ T(\mathscr{D}_1), & \text{если } s = 1. \end{cases}$$

и $\Pi(M) = \bigcup\limits_{i=1}^{s} \mathscr{I}(n_i)$. Отметим, что множество $T(M)$ является разделимым и взаимно простым с любым числом из $\Pi(M)$. Рассмотрим множество $SG\big[\Pi(M); T(M)\big]$. Можно доказать, что $\langle M\rangle = SG[\Pi(M); T(M)]$. Данное соотношение также можно обобщить на случай замыканий конечных множеств векторов из $\boldsymbol{SQ}$ произвольной размерности. Пусть $M = \{\mathscr{D}_1, \ldots, \mathscr{D}_s\}$ — произвольное конечное множество позитивных стохастических векторов из $\boldsymbol{SQ}$ размерности $h_1, \ldots, h_s$ соответственно. Как и для случая одноэлементного множества, мы полагаем, что каждый вектор $\mathscr{D}_i$ представлен в виде

$$\mathscr{D}_i = \left(\frac{m_1^{(i)}}{n_i}; \ldots; \frac{m_{h_i}^{(i)}}{n_i}\right),$$

где $(m_1^{(i)}, \ldots, m_{h_i}^{(i)}) = 1$. Положим $T(M) = (T(\mathscr{D}_1), \ldots, T(\mathscr{D}_s))$ в случае $s \geqslant 2$ и $T(M) = T(\mathscr{D}_1)$ в случае $s = 1$. Положим также $\Pi(M) = \bigcup\limits_{i=1}^{s} \mathscr{I}(n_i)$. Можно показать, что множество $T(M)$ является разделимым и взаимно простым с любым числом из $\Pi(M)$. Поэтому можно рассмотреть множество $SG\left[\Pi(M); T(M)\right]$, для которого справедлива

Теорема 6. *Для любого конечного множества M позитивных стохастических векторов из $\boldsymbol{SQ}$ выполняется соотношение $\langle M\rangle = SG\left[\Pi(M); T(M)\right]$.*

На основании теоремы 6 можно предложить эффективный алгоритм решения задачи выразимости в $\boldsymbol{SQ}$. Пусть множество M состоит из позитивных векторов $\mathscr{D}_1, \ldots, \mathscr{D}_s$ размерности $h_1, \ldots, h_s$ соответственно. Предполагается, что все компоненты этих векторов изначально заданы несократимыми дробями. Пусть компоненты вектора $\mathscr{D}_i$ заданы несократимыми дробями, знаменателями которых являются числа $n_1^{(i)}, \ldots, n_{h_i}^{(i)}$, $i = 1, \ldots, s$. Положим $\eta_M = \max\limits_{i,j} n_j^{(i)}$, $h_M = \max\limits_i h_i$ и $\Sigma_M = \sum\limits_{i=1}^{s} h_i$. Отметим, что если $\mathscr{D} \notin \boldsymbol{SQ}$, то, очевидно, $\mathscr{D} \notin \langle M\rangle$. Поэтому можно предполагать, что $\mathscr{D} \in \boldsymbol{SQ}$. Пусть вектор $\mathscr{D}$ имеет размерность h и все компоненты этого вектора заданы несократимыми дробями, знаменателями которых являются числа $n_1^{(0)}, \ldots, n_h^{(0)}$. Положим $\eta_{\mathscr{D}} = \max\limits_j n_j^{(0)}$. Тогда проверка соотношения $\mathscr{D} \in \langle M\rangle$ с помощью теоремы 6 требует выполнения не более $O\big((\Sigma_M + h)h_M \log \eta_M + \log\log \eta_{\mathscr{D}}\big)$ арифметических операций. Таким образом, задача выразимости в $\boldsymbol{SQ}$ разрешима за полиномиальное время.

Теорема 6 может быть модифицирована для случая замыканий произвольных бесконечных множеств стохастических векторов из $\boldsymbol{SQ}$. Пусть $M = \{\mathscr{D}_1, \mathscr{D}_2, \ldots\}$ — бесконечное множество позитивных векторов из $\boldsymbol{SQ}$. Тогда мы также можем рассмотреть множество $SG\left[\Pi(M); T(M)\right]$, где $T(M) = (T(\mathscr{D}_1), T(\mathscr{D}_2), \ldots)$ и $\Pi(M) = \bigcup\limits_{i=1}^{\infty} \mathscr{I}(n_i)$.

Теорема 7. *Для каждого бесконечного множества M позитивных векторов из $\boldsymbol{SQ}$ выполняется равенство $\langle M\rangle = SG\left[\Pi(M); T(M)\right]$.*

Поскольку любой из замкнутых классов векторов из $\boldsymbol{SQ}$ является замыканием некоторого своего подмножества (например, самого этого класса), из теорем 6 и 7 следует, что любой замкнутый класс векторов из $\boldsymbol{SQ}$ является элементом множества $\boldsymbol{SG}$. Таким образом, множество $\boldsymbol{SG}$ является множеством всех замкнутых подмножеств множества $\boldsymbol{SQ}$. Можно показать, что любое замкнутое множество векторов из $\boldsymbol{SQ}$ имеет базис. Кроме того, для каждого замкнутого множества векторов из $\boldsymbol{SQ}$ можно дать описание всех его предполных классов. Для множеств $SG[\Pi]$ все предполные классы описываются следующим образом.

Утверждение 3. *Совокупностью всех предполных классов в множестве $SG[\Pi]$ является множество*

$$S_0[\Pi] \cup \bigcup_{t \in \mathbb{P}\setminus\Pi} \{SG[\Pi; \{t\}]\},$$

где

$$S_0[\Pi] = \begin{cases} \bigcup\limits_{p\in\Pi} \{SG[\Pi \setminus \{p\}]\}, & \text{если } |\Pi| > 1; \\ \varnothing, & \text{если } |\Pi| = 1. \end{cases}$$

В случае множества $SG[\Pi; T]$, где T непусто, для каждого числа r из $\mathcal{J}(\|T\|)$ мы обозначаем через $t^{(r)}$ единственное число из T, кратное r. В таком случае имеем

Утверждение 4. *Совокупностью всех предполных классов во множестве* $SG[\Pi, T]$, *где* $T = \{t_1, \ldots, t_q\}$, $q \geqslant 1$, *является множество*

$$S_0[\Pi; T] \cup \bigcup_{t \in \mathbb{P} \setminus (\Pi \cup \mathcal{J}(\|T\|))} \{SG[\Pi; T \cup \{t\}]\} \cup$$

$$\cup \bigcup_{r \in \mathcal{J}(\|T\|)} \{SG[\Pi; T \cup \{t^{(r)} \cdot r\} \setminus \{t^{(r)}\}]\} \cup \bigcup_{1 \leqslant i < j \leqslant q} \{\{SG[\Pi; T \cup \{t_i t_j\} \setminus \{t_i, t_j\}]\},$$

где

$$S_0[\Pi; T] = \begin{cases} \bigcup\limits_{p \in \Pi} \{SG[\Pi \setminus \{p\}; T]\}, & \text{если } |\Pi| > 1; \\ \varnothing, & \text{если } |\Pi| = 1, \end{cases}$$

Из утверждений 3 и 4 вытекает, что в каждом из замкнутых подмножеств множества $\boldsymbol{SQ}$ имеется счетное число предполных классов.

Через $\boldsymbol{SG_{fin}}$ мы обозначаем подмножество множества $\boldsymbol{SG}$, состоящее из всех множеств $SG[\Pi; T]$ таких, что Π конечно. Можно доказать, что замкнутое подмножество множества $\boldsymbol{SQ}$ является конечно-порожденным тогда и только тогда, когда это подмножество является элементом множества $\boldsymbol{SG_{fin}}$. Таким образом, $\boldsymbol{SG_{fin}}$ является множеством всех конечно-порожденных замкнутых подмножеств множества $\boldsymbol{SQ}$. Кроме того, для каждого множества $SG[\Pi, T]$ из $\boldsymbol{SG_{fin}}$ можно непосредственно предъявить одноэлементное подмножество, порождающее это множество.

Следует отметить, что в ряде работ рассматривалось порождение вероятностных распределений с наложенными на него дополнительными ограничениями. Одним из таких ограничений является ограничение на класс функций, используемых для порождения распределений. Например, в [31] рассматривалось порождение бинарных распределений в классе $F_{\text{ппкс}}$ всех булевых функций, реализуемых бесповторными формулами над базисом $\{\&, \vee\}$ (отметим, что $F_{\text{ппкс}}$ можно также определить как класс всех булевых функций, реализуемых бесповторными параллельно-последовательными контактными схемами). Было показано, что множества $G[\{2\}]$ и $G[\{3\}]$ порождаются в данном классе подмножествами $\left\{\frac{1}{2}\right\}$ и $\left\{\frac{1}{3}, \frac{2}{3}\right\}$ соответственно. В [4] было показано, что в классе $F_{\text{ппкс}}$ конечно-порожденным является любое множество $G[\Pi]$, где Π конечно и содержит по крайней мере два числа. Остается открытым вопрос о конечной порожденности в классе $F_{\text{ппкс}}$ множеств $G[\{p\}]$, где p — простое число, большее 3. Ряд результатов, связанных с порождением бинарных распределений в более широком классе $F_{\text{кс}}$ всех булевых функций, реализуемых бесповторными контактными схемами, получен в [5]. В частности, доказана конечная порожденность в $F_{\text{кс}}$ множеств $G[\{5\}]$ и $G[\{7\}]$. Кроме того, приведен пример множества, не являющегося конечно-порожденным в $F_{\text{ппкс}}$, но конечно-порожденного в $F_{\text{кс}}$. Из этих результатов вытекает, что в плане своих выразительных возможностей класс $F_{\text{ппкс}}$ является более слабым, чем $F_{\text{кс}}$. Представляется интересным выявление классов булевых функций, сопоставимых по выразительности с классом всех булевых функций. Таким классом может оказаться класс всех монотонных булевых функций, поскольку для некоторых

конечных систем бинарных распределений замыкания этих систем относительно порождения в классе всех монотонных булевых функций совпадают с их замыканиями относительно порождения в классе всех булевых функций [8].

Другим естественным ограничением, которое может быть наложено на порождение вероятностных распределений, является ограничение на число исходных случайных величин. Для справедливости изложенных выше результатов предполагается, что для порождения распределений можно использовать неограниченное число независимых копий случайных величин с вероятностными распределениями из исходного множества распределений. Если ограничить возможное число таких копий, то мы имеем задачу оценки сложности порождения вероятностных распределений, где под сложностью порождения распределения понимается минимальное число исходных случайных величин, необходимое для порождения данного распределения. Такая сложность, очевидно, существенным образом зависит от исходного множества распределений. В работах [5–7,9,10,31,33,37] был получен ряд оценок сложности порождения бинарных распределений из $\boldsymbol{SQ}$ как в классах $F_{\text{ппкс}}$ и $F_{\text{кс}}$, так и в классе всех булевых функций. В частности, в [31,33] было установлено, что при $k=2$ ($k=3$) сложность порождения числа m/k^n подмножеством $\{1/2\}$ ($\{1/3, 2/3\}$) в классе $F_{\text{ппкс}}$ равна n. В [37] была вычислена сложность порождения в классе всех булевых функций бинарных распределений k-ично-рациональных вероятностей системами чисел $\left\{\frac{1}{k}, \frac{2}{k}, \ldots, \frac{k-1}{k}\right\}$ для любого натурального $k>3$. В [6,7] были получены оценки сложности порождения в классе $F_{\text{ппкс}}$ чисел из множеств $G[\Pi]$, где Π конечно и содержит по крайней мере два числа, конечными порождающими подмножествами этих множеств. Эти результаты были усилены в [9]: при условии, что Π конечно и содержит по крайней мере два числа, для любого $\varepsilon>0$ было непосредственно предъявлено конечное порождающее подмножество множества $G[\Pi]$ такое, что сложность порождения в классе $F_{\text{ппкс}}$ любого числа $\frac{m}{n}$ из $G[\Pi]$ этим подмножеством не превосходит $1+\varepsilon\log n$. В [5] были получены оценки сложности порождения в классе $F_{\text{кс}}$ чисел из множеств $G[\{5\}]$ и $G[\{7\}]$ порождающими эти множества конечными подмножествами. В [10] найдена асимптотика сложности порождения бинарных распределений в классе всех булевых функций одноэлементными множествами бинарных распределений из $\boldsymbol{SQ}$. Однако в общем случае задача оценки сложности порождения вероятностных распределений из $\boldsymbol{SQ}$ остается нерешенной даже для класса всех булевых функций. Отметим, что используемые для получения изложенных выше результатов методы порождения вероятностных распределений являются экономными в плане использования исходных случайных величин и поэтому могут оказаться полезными для решения данной проблемы. Другим сложностным аспектом порождения вероятностных распределений, изучавшимся ранее в литературе [3,24], является минимальная сложность схемной реализации функций, применяемых для порождения этих распределений. В частности, в [3] решена задача оптимального синтеза детерминированного преобразователя в базисе $\{\&, \vee, {}^{-}\}$, генерирующего значения 0 и 1 с вероятностью, зависящей от некоторого управляющего параметра, и дан анализ точности данного преобразования. В [24] получена асимптотика функции Шеннона для сложности схемной реализации в произвольном конечном базисе для исходного

множества бинарных распределений, состоящего из единственного распределения $(1-p;p)$, в случае, если p является трансцендентным. Для случая, когда p не является трансцендентным, в данной работе получены точные по порядку верхние оценки исследуемой функции Шеннона.

Тесно связанной с задачей оценки сложности порождения вероятностных распределений является задача приближенного порождения вероятностных распределений, заключающаяся в том, чтобы из заданного числа исходных случайных величин с заданными распределениями построить случайную величину с распределением, наиболее близким к требуемому вероятностному распределению. Интересные результаты, касающиеся приближенного порождения распределений, получены Р. Схиртладзе и Н. Нурмеевым в работах [23, 32]. В частности, в [23] найдены точные значения максимальной погрешности реализации бинарных случайных величин булевыми функциями с заданным числом переменных исходя из множества, состоящего ровно из одного бинарного распределения. Важной задачей, близкой по тематике к рассматриваемым вопросам, является также задача о минимальном имплицирующем векторе [22]. Под имплицирующим вектором для стохастической матрицы понимается набор коэффициентов выпуклого разложения этой матрицы на вырожденные (состоящие только из нулей и единиц) стохастические матрицы того же размера. Минимальным имплицирующим вектором для стохастической матрицы называется имплицирующий вектор минимальной длины. В [2] отмечена NP-полнота задачи нахождения минимального имплицирующего вектора. В [22] получены близкие друг к другу верхние и нижние оценки функций Шеннона от размера матрицы для иерархии различных классов стохастических матриц.

Отметим, что в данной работе мы рассматриваем порождение распределений посредством функций, все значения которых являются значениями реализуемых ими случайных величин. Такое порождение можно назвать *синхронным*. Начиная с середины прошлого века в ряде работ [25, 34, 36, 40] рассматривалось порождение распределений посредством функций, которые, кроме значений реализуемых случайных величин, принимают также «неопределенное» значение. «Неопределенное» значение функции означает, что мы не можем получить значение реализуемой случайной величины на данном наборе значений исходных случайных величин и поэтому надо использовать новую порцию исходных случайных величин для повторной попытки реализации требуемой случайной величины. Поскольку в таком случае требуемая случайная величина может быть получена с некоторой задержкой, пропорциональной числу повторных попыток ее реализации, в отличие от рассматриваемого синхронного порождения такое порождение можно назвать *асинхронным*. Первый простейший метод асинхронного преобразования последовательности независимых бинарных случайных величин, имеющих некоторое фиксированное распределение, в последовательность независимых бинарных случайных величин, принимающих оба значения с вероятностью $1/2$, был предложен в [40]. В [25, 34] предложены более эффективные реализации данного метода. Асинхронное порождение распределений является практичным в случае, если реализуется большая серия случайных величин и допускается неограниченно большая задержка в реализации между двумя последовательными случайными величинами из этой серии. В противном случае такой подход к порождению

распределений является неприемлемым. Одним из возможных путей устранения этого недостатка асинхронного порождения представляется комбинирование асинхронного порождения с синхронным порождением, заключающееся в том, чтобы в случае достаточно большой задержки при реализации случайной величины применять синхронное порождение, т. е. функцию, не принимающую «неопределенное» значение.

Еще раз отметим, что в данной работе все исходные случайные величины, используемые для порождения распределений, предполагаются независимыми в совокупности. Н. Нисаном и Д. Зукерманом в [42] было показано, что для приближенного порождения распределений с произвольной точностью могут также использоваться исходные случайные величины, не являющиеся независимыми. Функции, применяемые в таком случае, называются *экстракторами*. В последние годы за рубежом проводились активные исследования экстракторов (см., например, [41, 43–45]). Существенным недостатком экстракторов является их сравнительно высокая сложность: экстракторы требуют большого числа исходных случайных величин и, соответственно, большой оказывается также сложность вычисления значений экстрактора.

СПИСОК ЛИТЕРАТУРЫ

1. Бухараев Р. Г. Основы теории вероятностных автоматов. — М.: Наука, 1985.
2. Габбасов Н. З. О минимальном имплицирующем векторе для линейных автоматов // Вероятностные автоматы и их приложения. — Казань: Изд-во КГУ, 1986.
3. Захаров В. М., Салимов Ф. И. К теории структурного синтеза детерминированных преобразователей вероятности // Problems of Control and Information Theory. — 1977. — V. 6, № 2. — P. 137–148.
4. Колпаков Р. М. О порождении некоторых классов рациональных чисел вероятностными π-сетями // Вестник МГУ. Серия 1. Математика. Механика. — 1991. — № 2. — С. 27–30.
5. Колпаков Р. М. О порождении рациональных чисел вероятностными контактными сетями // Вестник МГУ. Серия 1. Математика. Механика. — 1992. — № 5. — С. 46–52.
6. Колпаков Р. М. Об оценках сложности порождения рациональных чисел вероятностными контактными π-сетями // Вестник МГУ. Серия 1. Математика. Механика. — 1992. — № 6. — С. 62–65.
7. Колпаков Р. М. О порождении рациональных чисел вероятностными контактными π-сетями // Дискретная математика. — 1994. — Т. 6, № 3. — С. 18–38.
8. Колпаков Р. М. О порождении рациональных чисел монотонными функциями // Теоретические и прикладные аспекты матем. исследований (Сб. научных трудов). — М.: Изд-во МГУ, 1994. — С. 13–17.
9. Колпаков Р. М. О верхних оценках сложности порождения рациональных чисел вероятностными π-сетями // Вестник МГУ. Серия 1. Математика. Механика. — 1995. — № 5. — С. 99–102.
10. Колпаков Р. М. О сложности порождения рациональных чисел одноэлементными множествами в классе всех булевых функций // Материалы VII Межгосударственной школы-семинара «Синтез и сложность управляющих систем». — М.: Изд-во МГУ, 1996. — С. 13–14.
11. Колпаков Р. М. Критерий порождаемости некоторых множеств рациональных чисел булевыми функциями // Тезисы докладов XI Международной конференции «Проблемы теоретической кибернетики» (Ульяновск, 10–14 июня 1996 г.). — М.: Изд-во РГГУ, 1996. — С. 96–97.
12. Колпаков Р. М. Критерий порождения множеств рациональных вероятностей в классе булевых функций // Дискретный анализ и исследование операций. Серия 1. — 1999. — Т. 6, № 2. — С. 41–61.

13. Колпаков Р. М. О преобразованиях булевых случайных величин // Математические вопросы кибернетики. Вып. 9. — М.: ФИЗМАТЛИТ, 2000. — С. 227–252.
14. Колпаков Р. М. О преобразованиях вероятностных распределений булевыми операторами // Материалы X Межгосударственной школы-семинара «Синтез и сложность управляющих систем». — М.: Изд-во МГУ, 2000. — С. 8–11.
15. Колпаков Р. М. Замкнутые классы булевых случайных величин с рациональнозначными распределениями // Математические вопросы кибернетики. Вып. 10. — М.: ФИЗМАТЛИТ, 2001. — С. 215–224.
16. Колпаков Р. М. Замыкания одноэлементных множеств бинарных распределений с рациональными вероятностями для многозначных преобразований // Математические вопросы кибернетики. Вып. 11. — М.: ФИЗМАТЛИТ, 2002. — С. 63–76.
17. Колпаков Р. М. О дискретных преобразованиях конечных рациональнозначных вероятностных распределений // Тезисы докладов XIII Международной конференции «Проблемы теоретической кибернетики», Казань. Часть I. — М.: Изд-во МГУ, 2002. — С. 92.
18. Колпаков Р. М. О многозначных преобразованиях конечных множеств бинарных распределений с рациональными вероятностями // Дискретная математика. — 2005. — Т. 17, № 1. — С. 102–128.
19. Колпаков Р. М. О дискретных преобразованиях конечных распределений с рациональными вероятностями // Математические вопросы кибернетики. Вып. 12. — М.: ФИЗМАТЛИТ, 2003. — С. 109–146.
20. Колпаков Р. М. Замкнутые классы конечных распределений рациональных вероятностей // Дискретный анализ и исследование операций. Серия 1. — 2004. — Т. 11, № 3. — С. 16–31.
21. Колпаков Р. М. Полиномиальный алгоритм проверки порождаемости конечных распределений рациональных вероятностей // Материалы XV Международной школы-семинара «Синтез и сложность управляющих систем». — Новосибирск: ИМ СО РАН, 2004. — С. 45–50.
22. Кузнецов С. Е., Нурмеев Н. Н., Салимов Ф. И. Задача о минимальном имплицирующем векторе // Математические вопросы кибернетики. Вып. 3. — М.: Наука, 1991. — С. 199–216.
23. Нурмеев Н. Н. О булевых функциях с аргументами, принимающими случайные значения // Тезисы докладов VIII Всесоюзной конференции «Проблемы теоретической кибернетики», Горький. Часть 2. — 1988. — С. 59–60.
24. Нурмеев Н. Н. О сложности реализации преобразователей вероятностей схемами из функциональных элементов // Методы и системы технической диагностики. Вып. 18. — Саратов: Саратовский гос. университет, 1993. — С. 131–132.
25. Рябко Б. Я., Мачикина Е. П. Эффективное преобразование случайных последовательностей в равновероятные и независимые // Проблемы передачи информации. — 1999. — Т. 36, № 2. — С. 23–28.
26. Салимов Ф. И. К вопросу моделирования булевых случайных величин функциями алгебры логики // Вероятностные методы и кибернетика. Вып. 15. — Казань: Изд-во Казанского университета, 1979. — С. 68–89.
27. Салимов Ф. И. Конечная порожденность некоторых алгебр над случайными величинами // Вопросы кибернетики. Вып. 86. — М., 1982. — С. 122–130.
28. Салимов Ф. И. О максимальных подалгебрах алгебр распределений // Известия вузов. Математика. — 1985. — № 7. — С. 14–20.
29. Салимов Ф. И. Об одном семействе алгебр распределений // Известия вузов. Математика. — 1988. — № 7. — С. 64–72.
30. Салимов Ф. И. Конечная порожденность алгебр распределений // Дискретный анализ и исследование операций. Серия 1. — 1997. — Т. 4, № 2. — С. 43–50.
31. Схиртладзе Р. Л. О синтезе p-схемы из контактов со случайными дискретными состояниями // Сообщ. АН ГрССР. — 1961. — Т. 26, № 2. — С. 181–186.
32. 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.
33. Схиртладзе Р. Л. Моделирование случайных величин функциями алгебры логики. — Автореф. дисс. . . . канд. физ.-мат. наук. — Тбилиси, 1966.
34. Elias P. The efficient construction of unbiased random sequence // Annals of Math. Statistics. — 1972. — V. 43, No. 3. — P. 865–870.

35. Hailperin Th. Boole's logic and probability: a critical exposition from the standpoint of contemporary algebra, logic and probability theory. — Amsterdam: North-Holland Publishing Co., 1976. (Studies in logic and the foundations of mathematics, V. 85.)
36. Hoeffding W., Simons G. Unbiased coin tossing with a biased coin // Annals of Math. Statistics. — 1970. — V. 41. — P. 341–352.
37. Kolpakov R. M. On the complexity of generation of rational numbers by Boolean functions // Fundamenta Informaticae. — 1995. — V. 22. — P. 289–298.
38. Kolpakov R. M. Criterion of generativeness of sets of rational probabilities by a class of Boolean functions // Discrete Applied Mathematics. — 2003. — V. 135. — P. 125–142.
39. Kolpakov R. M. Classes of binary rational distributions closed under discrete transformations // Stochastic Algorithms: Foundations and Applications (SAGA'03). Lecture Notes in Computer Science, V. 2827. — Springer Verlag, 2003. — P. 157–166.
40. von Neumann J. Various technique used in connection with random digits // J. Res. National Bureau of Standards. Applied Math. Series. — 1951. — No. 12. — P. 36–38.
41. Nisan N., Ta-Shma A. Extracting randomness: A survey and new constructions // J. of Computer and System Sciences. — 1999. — V. 58, No. 1. — P. 148–173.
42. Nisan N., Zuckerman D. Randomness is linear in space // J. of Computer and System Sciences. — 1996. — V. 52, No. 1. — P. 43–52.
43. Raz R., Reingold O., Vadhan S. Error reduction for extractors // Proceedings of 40th Symposium on Foundations of Computer Science, New York (USA). — 1999. — P. 191–201.
44. Srinivasan A., Zuckerman D. Computing with very weak random sources // SIAM J. on Computing. — 1999. — V. 28, No. 4. — P. 1433–1459.
45. Trevisan L. Construction of extractors using pseudo-random generators // Proceedings of 31th ACM Symposium on Theory of Computing, Atlanta (USA). — 1999. — P. 141–148.

Поступило в редакцию 10 II 2015