ДИСКРЕТНЫЙ АНАЛИЗ И ИССЛЕДОВАНИЕ ОПЕРАЦИЙ
Июль–сентябрь 2021. Т. 28, № 3. С. 90–103

УДК 519.716+519.214.7 DOI 10.33048/daio.2021.28.707

О ПРЕОБРАЗОВАНИЯХ ТРЁХЗНАЧНЫХ СЛУЧАЙНЫХ ВЕЛИЧИН ФУНКЦИЯМИ ДВУХ ПЕРЕМЕННЫХ

А. Д. Яшунский

Институт прикладной математики им. М. В. Келдыша РАН,
Миусская пл., 4, 125047 Москва, Россия

E-mail: yashunsky@keldysh.ru

Аннотация. Рассматриваются преобразования трёхзначных случайных величин функциями трёхзначной логики. Для всевозможных систем функций от двух переменных, содержащих все функции с несущественными переменными, описаны классы распределений случайных величин, аппроксимируемых путём подстановки в имеющиеся операции независимых случайных величин, выпускающих хотя бы одно из трёх значений. Ил. 2, библиогр. 11.

Ключевые слова: трёхзначная логика, случайная величина, распределение, аппроксимация.

Введение

Задачи о построении дискретных преобразователей конечных случайных величин рассматриваются по меньшей мере с 1960-х гг. Среди различных типов преобразователей выделяется класс систем, в которых конечные наборы случайных величин преобразуются операциями из некоторого заданного множества. Исследование подобных систем, мотивированное изначально, в частности, задачами синтеза вероятностных автоматов [1], в настоящее время находит применение при анализе «биохимических» вычислительных систем [2] и криптографических схем [3].

К настоящему моменту наиболее завершёнными выглядят исследования по выразимости случайных величин с рациональными распределениями в системах, где в качестве операций могут использоваться произвольные функции k-значной логики: Р. М. Колпаков в [4] описал все классы рациональных распределений, замкнутые относительно указанных преобразований.

Исследование выполнено при поддержке гранта Российского научного фонда (проект № 19–71–30004).

Для более слабых, чем совокупность всех функций k-значной логики, наборов операций возможности точного выражения случайных величин с заданными распределениями изучены достаточно слабо. Вместе с тем, имеются важные результаты о возможности приближения случайных величин по распределению с любой наперёд заданной точностью. Уже в работе [5] Р. Л. Схиртладзе в 1966 г. показал, что при преобразованиях невырожденных независимых одинаково распределённых булевых случайных величин операциями конъюнкции, дизъюнкции и отрицания можно приблизить по распределению *любую* булеву случайную величину. Этот результат был впоследствии усилен А. Д. Яшунским в [6] и независимо Х. Жу, П.-Л. Ло и Дж. Браком в [7]. В [6] также показано, что сходные возможности по аппроксимации случайных величин могут возникать и при использовании других систем функций. Описание всевозможных наборов функций k-значной логики, $k \geqslant 2$, обладающих подобными свойствами, именуемыми далее *аппроксимационной полнотой*, представляет несомненный интерес, однако на данный момент говорить о наличии эффективных критериев проверки аппроксимационной полноты не приходится. Тем не менее, в [6] имеется (не вполне эффективный) критерий для систем булевых функций, а в [8] получены некоторые достаточные условия аппроксимационной полноты для систем функций k-значной логики.

Доказательство аппроксимационной полноты или неполноты, существенно облегчаемое в булевом случае критерием из [6], уже в случае трёхзначной логики может оказаться нетривиальной задачей. Получение для функций трёхзначной логики хотя бы критерия, аналогичного булеву случаю, существенно помогло бы в исследовании аппроксимирующих свойств систем функций трёхзначной логики. В настоящей работе исследуются некоторые преобразования трёхзначных случайных величин, представляющие интерес с точки зрения проверки аппроксимационной полноты систем функций.

1. Аппроксимация случайных величин

Приведём основные определения и обозначения, связанные с задачей преобразования и аппроксимации конечных случайных величин (подробнее см. [8]). Будем рассматривать случайные величины, принимающие значения из конечного множества $E_k = \{0, 1, \ldots, k-1\}$. Распределение такой случайной величины X есть набор $\mathsf{P}(X) = (p_0, p_1, \ldots, p_{k-1})$, где p_i — вероятность обращения X в $i \in E_k$. Совокупность всевозможных распределений k-значных случайных величин образует в пространстве $\mathbb{R}^k$ симплекс, определяемый условиями $p_0+p_1+\cdots+p_{k-1} = 1$ и $p_i \geqslant 0$ для $i \in E_k$. Обозначим этот симплекс через $\mathbf{S}^{(k)}$ и будем называть *стохастическим*, а его элементы — распределения на множестве E_k — будем

обозначать через $\mathbf{p} = (p_0, p_1, \ldots, p_{k-1})$. *Носителем* $\mu(\mathbf{p})$ распределения $\mathbf{p}$ называется множество $\{i \in E_k \mid p_i > 0\}$.

Обозначим множество n-местных функций на E_k через $P_k(n)$ и положим $P_k = \bigcup\limits_{n=0}^{\infty} P_k(n)$. Пусть $X_1, \ldots, X_n$ — независимые в совокупности k-значные случайные величины с распределениями $\mathbf{p}^{(1)}, \ldots, \mathbf{p}^{(n)} \in \mathbf{S}^{(k)}$, а $f \in P_k(n)$ — некоторая функция. Тогда $f(X_1, \ldots, X_n)$ — также k-значная случайная величина. Её распределение $\mathbf{q} = \mathsf{P}(f(X_1, \ldots, X_n))$ может быть выражено через распределения $\mathbf{p}^{(1)}, \ldots, \mathbf{p}^{(n)}$ следующим образом:

$$q_i = \sum_{\substack{\sigma_1,\ldots,\sigma_n \in E_k: \\ f(\sigma_1,\ldots,\sigma_n)=i}} p^{(1)}_{\sigma_1} p^{(2)}_{\sigma_2} \cdots p^{(n)}_{\sigma_n}, \quad i = 1, \ldots, n. \tag{1}$$

Соотношения (1) фактически определяют функцию $\widehat{f}(\mathbf{p}^{(1)}, \ldots, \mathbf{p}^{(n)})$, отображающую $(\mathbf{S}^{(k)})^n$ в $\mathbf{S}^{(k)}$. Будем говорить, что $f(x_1, \ldots, x_n)$ *индуцирует* функцию $\widehat{f}(\mathbf{p}^{(1)}, \ldots, \mathbf{p}^{(n)})$.

Рассмотрим случайные величины, представимые как результат подстановки независимых в совокупности случайных величин с распределениями из некоторого множества начальных распределений $\mathbf{G} \subseteq \mathbf{S}^{(k)}$ в бесповторные (т. е. содержащие каждый символ переменной не более одного раза) формулы над некоторой системой функций $B \subseteq P_k$. Совокупность распределений таких случайных величин будет замкнута относительно операций из множества $\widehat{B} = \{\widehat{f} \mid f \in B\}$, т. е. будет *алгеброй распределений*. Более того, это будет наименьшая по включению алгебра, содержащая множество начальных распределений $\mathbf{G}$, фактически — замыкание $\mathbf{G}$ относительно множества операций $\widehat{B}$, далее обозначаемое $V_B(\mathbf{G})$. Помимо *выразимых* случайных величин, распределения которых принадлежат $V_B(\mathbf{G})$, можно также рассматривать случайные величины, для которых в $V_B(\mathbf{G})$ найдутся сколь угодно близкие распределения; такие случайные величины будем называть *аппроксимируемыми*. Совокупность распределений аппроксимируемых случайных величин будем обозначать через $W_B(\mathbf{G})$: это множество совпадает с топологическим замыканием $V_B(\mathbf{G})$, или, эквивалентно, состоит из $V_B(\mathbf{G})$ и всех его предельных точек. В силу непрерывности индуцированных функций множества $W_B(\mathbf{G})$ также являются алгебрами распределений.

В терминах введённого выше оператора W_B *аппроксимационную полноту* системы B определим как выполнение равенства $W_B(\{\mathbf{p}\}) = \mathbf{S}^{(k)}$ для всех $\mathbf{p} \in \mathbf{S}^{(k)}$, удовлетворяющих условию $\mu(\mathbf{p}) = E_k$. Полученный в [6] критерий аппроксимационной полноты утверждает, что для системы булевых функций $B \subseteq P_2$, не лежащей целиком в классе конъюнкций, дизъюнкций или линейных функций, аппроксимационная полнота равносильна возможности аппроксимировать распределения $\mathbf{e}^{(0)}, \mathbf{e}^{(1)} \in \mathbf{S}^{(2)}$.

Эти два распределения образуют в точности границу множества $\mathbf{S}^{(2)}$. Таким образом, одним из возможных обобщений указанного условия с P_2 на P_3 может быть рассмотрение систем, в которых заведомо аппроксимируемы распределения, лежащие на границе $\mathbf{S}^{(3)}$. Это множество распределений обозначим через $\mathbf{\Delta} = \{\mathbf{p} \in \mathbf{S}^{(3)} \mid \mu(\mathbf{p}) \neq E_3\}$.

В настоящей работе рассматриваются алгебры распределений $W_B(\mathbf{\Delta})$, т. е. фактически изучаются возможности различных систем по аппроксимации распределений из $\mathbf{S}^{(3)}$ в предположении, что распределения из $\mathbf{\Delta}$ заведомо аппроксимируемы. Описание $W_B(\mathbf{\Delta})$ в зависимости от системы функций B приближает нас к установлению общих условий аппроксимационной полноты систем функций из P_3.

2. Некоторые классы функций в $P_3(2)$

Мы ограничимся рассмотрением лишь некоторых преобразующих систем функций $B \subset P_3$, а именно, систем, содержащих функции от не более чем двух переменных. Такие системы оказываются достаточно разнообразными для порождения нетривиальных алгебр распределений в $\mathbf{S}^{(3)}$ и могут послужить фундаментом для дальнейших исследований аппроксимационной полноты систем функций из P_3.

Напомним, что переменная x_i функции $f(x_1, \ldots, x_n) \in P_3$ называется *существенной*, если найдутся такие константы $\alpha_1, \ldots, \alpha_{n-1} \in E_3$, что функция $f(\alpha_1, \ldots, \alpha_{i-1}, x, \alpha_i, \ldots, \alpha_{n-1})$ не постоянна. Через P_3^1 будем обозначать функции из P_3, имеющие не более одной существенной переменной. Как несложно проверить, имеет место равенство $W_{P_3^1}(\mathbf{\Delta}) = \mathbf{\Delta}$.

Далее будем считать, что функции, имеющие не более одной существенной переменной, заведомо входят в систему B, т. е. рассматривать системы, удовлетворяющие условиям $P_3^1 \cap P_3(2) \subseteq B \subseteq P_3(2)$.

Обозначим через $\omega(f)$ *вес* функции f — количество её различных значений. Очевидно, что для $f \in P_3$ выполнено $\omega(f) \in \{1, 2, 3\}$. При этом если $\omega(f) < 3$, то значения индуцированной функции $\widehat{f}$ лежат в множестве $\mathbf{\Delta}$. Отсюда непосредственно следует, что для систем B, удовлетворяющих условию $B \setminus P_3^1 \subseteq \{f \mid \omega(f) < 3\}$, выполнено $W_B(\mathbf{\Delta}) = \mathbf{\Delta}$. Таким образом, с точки зрения нахождения алгебр распределений $W_B(\mathbf{\Delta})$ интерес представляют только те системы, которые содержат функции веса 3.

Среди функций из $P_3(1)$ выделим функции веса 3 (или, эквивалентно, осуществляющие перестановку элементов E_3) и обозначим это множество функций через S_{E_3}. По аналогии с [9,10] введём класс *изострофий* [1)] функции $f(x_1, \ldots, x_n)$:

[1)] Понятие изострофии, вводимое обычно для n-арных квазигрупповых операций, допускает помимо перестановки переменных ещё и переход к обратной (по какой-то из переменных функции f) операции. Однако для произвольной функции f обратная

$$\mathcal{I}(f) = \{\varphi_0(f(\varphi_1(x_{\sigma_1}), \ldots, \varphi_n(x_{\sigma_n}))) \mid \varphi_0, \varphi_1, \ldots, \varphi_n \in S_{E_3},\ \{\sigma_1, \ldots, \sigma_n\} = \{1, \ldots, n\}\}.$$

В силу включения $S_{E_3} \subset P_3(1)$ преобразования трёхзначных случайных величин системой B, содержащей $P_3(1)$, можно рассматривать с точностью до изострофий входящих в B функций.

Лемма 1. *Если* $B \subseteq P_3$, $\mathbf{G} \subseteq \mathbf{S}^{(3)}$ *и* $B' = \bigcup\limits_{f \in B} \mathcal{I}(f)$, *то выполнено равенство* $W_{P_3(1) \cup B}(\mathbf{G}) = W_{P_3(1) \cup B'}(\mathbf{G})$.

В работе С. В. Яблонского [11] доказана следующая лемма о функциях, принимающих три значения.

Лемма 2 [11]**.** *Пусть функция* $f(x_1, \ldots, x_n) \in P_3 \setminus P_3^1$ *принимает все три значения* $0, 1, 2$. *Тогда найдутся подмножества* $G_i \subset E_3$, $|G_i| \leqslant 2$, $i = 1, \ldots, n$, *такие, что на наборах* $(\alpha_1, \ldots, \alpha_n)$, $\alpha_i \in G_i$, $i = 1, \ldots, n$, *функция* f *также принимает все три значения.*

Из лемм 1 и 2 вытекает, что, не ограничивая общности, можно вместо функции $f \in B$, $\omega(f) = 3$, рассматривать изострофную ей функцию, принимающую все три значения на подмножестве $\{0, 1\}^2 \subset E_3^2$. Несложно проверить, что с точностью до изострофии любая функция $f \in P_3(2)$, принимающая все три значения на множестве $\{0, 1\}^2$, имеет таблицу одного из двух следующих видов (в таблицах пустыми оставлены ячейки, значения в которых могут быть произвольными):

f	0	1	2
0	0	1	
1	0	2	
2			

,

f	0	1	2
0	0	1	
1	1	2	
2			

.

Начнём с рассмотрения функций $f \in P_3(2)$, среди изострофий которых есть функции первого типа. Обозначим класс таких функций через R.

Лемма 3. *Если* $f \in R$, *то* $W_{P_3(1) \cup \{f\}}(\mathbf{\Delta}) = \mathbf{S}^{(3)}$.

Доказательство. В силу леммы 1 вместо $W_{P_3(1) \cup \{f\}}(\mathbf{\Delta})$ можно рассматривать $W_{P_3(1) \cup \mathcal{I}(f)}(\mathbf{\Delta})$. Поскольку $f \in R$, в классе $\mathcal{I}(f)$ лежит функция g с таблицей значений вида

g	0	1	2
0	0	1	
1	0	2	
2			

.

операция может быть, вообще говоря, не определена, поэтому мы исключаем эту возможность, сохраняя при этом термин *изострофия.*

Отметим, что для любых $a, b \in [0;1]$ множество $\mathbf{\Delta}$ содержит распределения $\mathbf{a} = (1-a, a, 0)$, $\mathbf{b} = (1-b, b, 0)$. Имеют место соотношения

$$W_{P_3^1 \cup \mathcal{I}(f)}(\mathbf{\Delta}) \ni \widehat{g}(\mathbf{a}, \mathbf{b}) = (1-b, (1-a)b, ab).$$

Остаётся заметить, что, выбирая $b = 1 - p_0$ и $a = \frac{p_2}{1-p_0}$ в случае $p_0 \neq 1$, можно представить любое распределение $\mathbf{p} = (p_0, p_1, p_2)$ в виде $(1-b, (1-a)b, ab)$. Это влечёт включение $W_{P_3^1 \cup \mathcal{I}(f)}(\mathbf{\Delta}) \supseteq \mathbf{S}^{(3)}$. Лемма 3 доказана.

Таким образом, множество $B \supseteq P_3^1 \cap P_3(2)$, содержащее хотя бы одну функцию из класса R, заведомо удовлетворяет равенству $W_B(\mathbf{\Delta}) = \mathbf{S}^{(3)}$, поэтому далее имеет смысл рассматривать только системы функций, не пересекающиеся с классом R. Как отмечалось ранее, все функции, принимающие три значения и не лежащие в классе R, изострофны функции f с таблицей вида

f	0	1	2
0	0	1	
1	1	2	
2			

.

Подставляя в индуцированную такой функцией f функцию $\widehat{f}$ распределения $\mathbf{a} = (1-a, a, 0) \in \mathbf{\Delta}$ и $\mathbf{b} = (1-b, b, 0) \in \mathbf{\Delta}$, получим распределение $\mathbf{p} = \widehat{f}(\mathbf{a}, \mathbf{b})$, компоненты которого удовлетворяют равенствам $p_0 = (1-a)(1-b)$ и $p_2 = ab$. Для описания множества распределений, входящих в $W_{P_3(1) \cup \{f\}}(\mathbf{\Delta})$, докажем следующее утверждение о подмножествах $\mathbb{R}^2$, заданных параметрически.

Лемма 4. *Пусть* $T = \{((1-a)(1-b), ab) \mid a, b \in [0;1]\} \subset \mathbb{R}^2$. *Тогда* $T = \{(x, y) \mid \sqrt{x} + \sqrt{y} \leqslant 1\}$.

Доказательство. Пары (x, y), принадлежащие T, задаются равенствами $x = (1-a)(1-b)$ и $y = ab$, где $a, b \in [0;1]$. Заметим, что тогда $(x, y) \in [0;1]^2$, а соотношение $y = 0$ влечёт равенство нулю одного из параметров a, b. Рассматривая эти случаи, легко получаем, что в множество T заведомо входит отрезок $\{(x, 0) \mid x \in [0;1]\}$. Далее будем рассматривать только точки $(x, y) \in T$, у которых $y \neq 0$.

Будем считать y фиксированным параметром, а $a \in [0;1]$ — переменной. Тогда из соотношения $y = ab$ вытекает, что $b = \frac{y}{a}$, причём из условия $b \in [0;1]$ следует, что переменная a для каждого фиксированного значения y может принимать только значения $a \geqslant y$. Подставляя $b = \frac{y}{a}$ в соотношение $x = (1-a)(1-b)$, получаем зависимость $x = (1-a)\left(1 - \frac{y}{a}\right)$ величины x от переменной $a \in [y;1]$. Это выражение всюду определено, поскольку $a \geqslant y > 0$.

Для величины x имеет место неравенство $x \geqslant 0$, причём $x = 0$ достигается, например, при $a = y$ и $a = 1$. Вычисляя производную x как функции от a, получаем, что x возрастает при $a \in [y; \sqrt{y}]$ и убывает при $a \in [\sqrt{y}; 1]$. Отсюда легко видеть, что $x(a)$ принимает все значения от 0 до $x(\sqrt{y}) = (1 - \sqrt{y})^2$. Итак, множество T состоит в точности из всех пар $(x, y) \in [0; 1]^2$, которые удовлетворяют неравенствам $0 \leqslant x \leqslant (1 - \sqrt{y})^2$, равносильным условию $\sqrt{x} + \sqrt{y} \leqslant 1$. Лемма 4 доказана.

Из леммы 4 и ранее рассмотренного результата подстановки распределений $\mathbf{a}$ и $\mathbf{b}$ в индуцированную функцию $\widehat{f}$ вытекает, что $W_{P_3^1 \cup \{f\}}(\mathbf{\Delta})$ содержит множество распределений, обозначаемое далее $\mathbf{T}$ и определяемое следующим образом:

$$\mathbf{T} = \{(p_0, p_1, p_2) \mid \sqrt{p_i} + \sqrt{p_j} \leqslant 1,\ i \neq j\}.$$

Симплекс $\mathbf{S}^{(3)}$ как подмножество $\mathbb{R}^3$ представляет собой равносторонний треугольник в плоскости, заданной уравнением $p_0 + p_1 + p_2 = 1$. Множество $\mathbf{T} \subseteq \mathbf{S}^{(3)}$, определённое соотношениями выше, изображено внутри треугольника $\mathbf{S}^{(3)}$ на рис. 1 (каждое распределение $\mathbf{p} = (p_0, p_1, p_2)$ по сути представляет собой барицентрические координаты точек внутри этого треугольника).

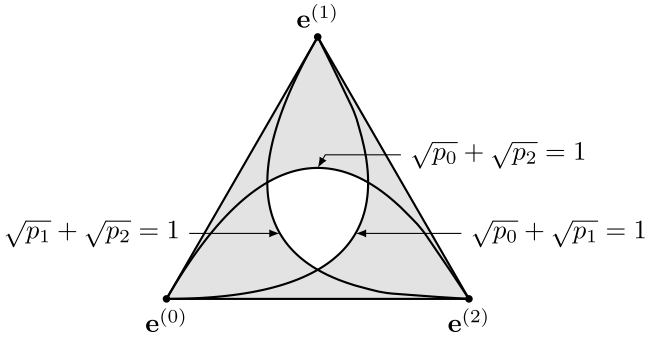

Рис. 1. Подмножество $\mathbf{T}$ (закрашено серым) в симплексе $\mathbf{S}^{(3)}$

Множество распределений $\mathbf{T}$ заведомо входит в $W_B(\mathbf{\Delta})$ для всех рассматриваемых систем B, содержащих функции веса 3 от двух переменных. Для дальнейшего анализа замыкания $W_B(\mathbf{\Delta})$ опишем с точностью до изострофии все функции из $P_3(2)$ веса 3, не входящие в класс R. Это удобно осуществлять путём постепенного заполнения таблицы функции f, исключая при этом те заполнения, которые заведомо попадают в класс R. Для сокращения записи будем выписывать в каждой таблице лишь девять ячеек со значениями функций. Несложно проверить,

что функция $f \in P_3(2) \setminus R$ с точностью до изострофии может иметь на $\{0,1\} \times \{0,1,2\}$ только одну из следующих таблиц значений:

$$\text{(a)}\ \begin{array}{|ccc|}\hline 0 & 1 & 0 \\ 1 & 2 & 1 \\ \hline \end{array}, \quad \text{(b)}\ \begin{array}{|ccc|}\hline 0 & 1 & 1 \\ 1 & 2 & 1 \\ \hline \end{array}, \quad \text{(c)}\ \begin{array}{|ccc|}\hline 0 & 1 & 1 \\ 1 & 2 & 2 \\ \hline \end{array}, \quad \text{(d)}\ \begin{array}{|ccc|}\hline 0 & 1 & 2 \\ 1 & 2 & 0 \\ \hline \end{array}. \qquad (2)$$

Функции, среди изострофий которых есть функция с таблицей вида (d), выделим в отдельный класс и обозначим его Q.

Лемма 5. *Если $f(x,y) \in Q$, то $W_{P_3(1)\cup\{f\}}(\mathbf{\Delta}) = \mathbf{S}^{(3)}$.*

Доказательство. Как и в лемме 3, в силу леммы 1 достаточно доказать, что $W_{P_3(1)\cup\mathcal{I}(f)}(\mathbf{\Delta}) = \mathbf{S}^{(3)}$. Тогда, не ограничивая общности, можно предполагать, что функция f, принадлежащая по условию классу Q, имеет таблицу вида

$$\begin{array}{|ccc|}\hline 0 & 1 & 2 \\ 1 & 2 & 0 \\ \hline \end{array}.$$

Обозначим через $\mathbf{h}$ распределение $\left(\frac{1}{2}, \frac{1}{2}, 0\right) \in \mathbf{\Delta}$. Для функции f указанного вида и любого распределения $\mathbf{p} \in \mathbf{S}^{(3)}$ выполнено равенство

$$\widehat{f}(\mathbf{h},\mathbf{p}) = \left(\frac{1}{2}(p_0+p_2), \frac{1}{2}(p_1+p_0), \frac{1}{2}(p_2+p_1)\right) = \frac{1}{2}(p_0,p_1,p_2) + \frac{1}{2}(p_2,p_0,p_1),$$

где в последнем выражении умножение на $\frac{1}{2}$ и сложение понимаются как операции с векторами из $\mathbb{R}^3$. Таким образом, фактически распределение $\widehat{f}(\mathbf{h},\mathbf{p})$ — средняя точка между распределениями (p_0,p_1,p_2) и (p_2,p_0,p_1). Как несложно заметить, второе распределение получается из первого поворотом вокруг центра треугольника $\mathbf{S}^{(3)}$ на треть полного оборота.

Определим для каждого $i \in E_3$ последовательность распределений, положив $\mathbf{g}^{(i,1)} = \mathbf{e}^{(i)}$ и далее $\mathbf{g}^{(i,n+1)} = \widehat{f}(\mathbf{h}, \mathbf{g}^{(i,n)})$ для $n \in \mathbb{N}$. В силу принадлежности $\mathbf{h} \in \mathbf{\Delta}$ и $\mathbf{e}^{(i)} \in \mathbf{\Delta}$ для всех $i \in E_3$ распределения $\mathbf{g}^{(i,n)}$ лежат в $W_{P_3(1)\cup\{f\}}(\mathbf{\Delta})$ для всех $i \in E_3$ и $n \in \mathbb{N}$.

С учётом геометрической интерпретации, описанной выше, индукцией по n легко проверить, что для каждого фиксированного n распределения $\mathbf{g}^{(0,n)}, \mathbf{g}^{(1,n)}, \mathbf{g}^{(2,n)}$ получаются друг из друга циклическим сдвигом координат (т. е. поворотом вокруг центра $\mathbf{S}^{(3)}$) (рис. 2).

Обозначим [2)]

$$\mathbf{\Delta}_{i,n} = \{t_0\mathbf{g}^{(i,n)} + t_1\mathbf{g}^{(i,n+1)} + t_2\mathbf{g}^{((i-1) \bmod 3, n+1)} \mid \mathbf{t} \in \mathbf{S}^{(3)}\}.$$

Тогда $\mathbf{\Delta}_{i,n}$ — выпуклая оболочка распределений $\mathbf{g}^{(i,n)}, \mathbf{g}^{(i,n+1)}, \mathbf{g}^{(i-1,n+1)}$, т. е. треугольник с вершинами в указанных распределениях.

[2)] Здесь, как и выше, мы умножаем распределения на числа и складываем как наборы из $\mathbb{R}^3$.

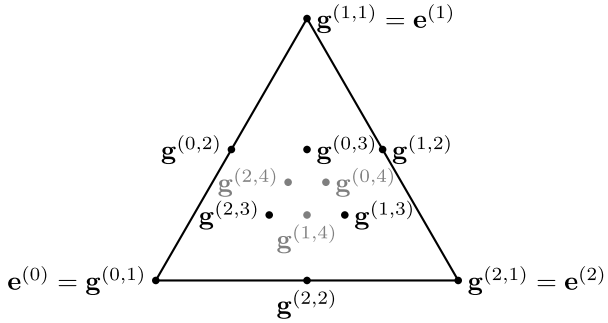

Рис. 2. Распределения $\mathbf{g}^{(i,n)}$, $i \in E_3$, $n = 1, 2, 3, 4$

Докажем индукцией по n, что для любых $i \in E_3$ и $n \in \mathbb{N}$ выполнено вложение $\mathbf{\Delta}_{i,n} \subseteq W_{P_3(1)\cup\{f\}}(\mathbf{\Delta})$. Для доказательства основания индукции покажем, что $\mathbf{\Delta}_{i,1} \subseteq \mathbf{T} \subseteq W_{P_3(1)\cup\{f\}}(\mathbf{\Delta})$. Будем доказывать это для $i = 1$, остальные случаи рассматриваются аналогично. Из определения распределений $\mathbf{g}^{(i,n)}$ имеем

$$\begin{aligned}\mathbf{\Delta}_{1,1} &= \{t_0\mathbf{g}^{(1,1)} + t_1\mathbf{g}^{(1,2)} + t_2\mathbf{g}^{(0,2)} \mid \mathbf{t} \in \mathbf{S}^{(3)}\} = \\ &= \left\{t_0(0,1,0) + t_1\left(0,\frac{1}{2},\frac{1}{2}\right) + t_2\left(\frac{1}{2},\frac{1}{2},0\right) \mid \mathbf{t} \in \mathbf{S}^{(3)}\right\} = \\ &= \left\{\left(\frac{1}{2}t_2, \frac{1}{2} + \frac{1}{2}t_0, \frac{1}{2}t_1\right) \mid \mathbf{t} \in \mathbf{S}^{(3)}\right\} = \left\{\mathbf{p} \in \mathbf{S}^{(3)} \mid p_0 + p_2 \leqslant \frac{1}{2}\right\},\end{aligned}$$

где последнее равенство вытекает из $p_1 = \frac{1}{2} + \frac{1}{2}t_0 \geqslant \frac{1}{2}$. Далее из неравенства $p_0 + p_2 \leqslant \frac{1}{2}$ получаем оценку $\sqrt{p_0} + \sqrt{p_2} \leqslant \sqrt{\frac{1}{2} - p_2} + \sqrt{p_2}$. Значение выражения $\sqrt{\frac{1}{2} - p_2} + \sqrt{p_2}$ при $p_2 \in \left[0; \frac{1}{2}\right]$ максимально, если $p_2 = \frac{1}{4}$, таким образом выполнено $\sqrt{p_0} + \sqrt{p_2} \leqslant \sqrt{\frac{1}{2} - p_2} + \sqrt{p_2} \leqslant 2\sqrt{\frac{1}{4}} = 1$. Отсюда следует, что множество $\left\{\mathbf{p} \in \mathbf{S}^{(3)} \mid p_0 + p_2 \leqslant \frac{1}{2}\right\}$ лежит в $\mathbf{T}$, это обеспечивает основание индукции.

Шаг индукции вытекает из полилинейности отображения $\widehat{f}$, которая непосредственно следует из (1). По предположению индукции выполнено $\mathbf{\Delta}_{i,n} \subseteq W_{P_3(1)\cup\{f\}}(\mathbf{\Delta})$, откуда

$$\begin{aligned}W_{P_3(1)\cup\{f\}}(\mathbf{\Delta}) &\supseteq \{\widehat{f}(\mathbf{h}, \mathbf{p}) \mid \mathbf{p} \in \mathbf{\Delta}_{i,n}\} = \\ &= \{\widehat{f}(\mathbf{h}, t_0\mathbf{g}^{(i,n)} + t_1\mathbf{g}^{(i,n+1)} + t_2\mathbf{g}^{((i-1) \bmod 3, n+1)}) \mid \mathbf{t} \in \mathbf{S}^{(3)}\} = \\ &= \{t_0\widehat{f}(\mathbf{h}, \mathbf{g}^{(i,n)}) + t_1\widehat{f}(\mathbf{h}, \mathbf{g}^{(i,n+1)}) + t_2\widehat{f}(\mathbf{h}, \mathbf{g}^{((i-1) \bmod 3, n+1)}) \mid \mathbf{t} \in \mathbf{S}^{(3)}\} = \\ &= \{t_0\mathbf{g}^{(i,n+1)} + t_1\mathbf{g}^{(i,n+2)} + t_2\mathbf{g}^{((i-1) \bmod 3, n+2)} \mid \mathbf{t} \in \mathbf{S}^{(3)}\} = \mathbf{\Delta}_{i,n+1}.\end{aligned}$$

Остаётся заметить, что

$$\bigcup_{n=1}^{N}\bigcup_{i=0}^{2}\mathbf{\Delta}_{i,n}=\mathbf{S}^{(3)}\setminus\left\{\sum_{i=0}^{2}t_i\mathbf{g}^{(i,N+1)}\mid\mathbf{t}\in\mathbf{S}^{(3)}\right\},$$

т. е. все распределения, которые не входят в какое-то из множеств $\mathbf{\Delta}_{i,n}$ с $n\leqslant N$, лежат в треугольнике $\left\{\sum\limits_{i=0}^{2}t_i\mathbf{g}^{(i,N+1)}\mid\mathbf{t}\in\mathbf{S}^{(3)}\right\}$. Поскольку его размеры стремятся к нулю с ростом N, топологическое замыкание множества $\bigcup\limits_{n=1}^{\infty}\bigcup\limits_{i\in E_3}\mathbf{\Delta}_{i,n}\subseteq W_{P_3(1)\cup\{f\}}(\mathbf{\Delta})$ совпадает с $\mathbf{S}^{(3)}$, что и требовалось доказать.

3. Основные результаты

Дальнейший анализ возможных заполнений таблиц функций из $P_3(2)$, приведённых в (2), позволяет полностью охарактеризовать алгебру распределений $W_{P_3^1\cup\{f\}}(\mathbf{\Delta})$.

Теорема 1. *Пусть $f\in P_3(2)\setminus P_3^1$ — произвольная функция. Тогда*

$$W_{P_3^1\cup\{f\}}(\mathbf{\Delta})=\begin{cases}\mathbf{\Delta}, & \text{если } \omega(f)<3,\\ \mathbf{S}^{(3)}, & \text{если } f\in Q\cup R,\\ \mathbf{T} & \text{иначе.}\end{cases}$$

Доказательство. Случаи функции f веса менее 3 или принадлежащей одному из классов Q, R рассмотрены выше (леммы 3 и 5). Остаётся показать, что никакое заполнение таблиц из (2) не приводит к функции f, у которой замыкание $W_{P_3^1\cup\{f\}}(\mathbf{\Delta})$ отлично от $\mathbf{T}$. В предположении непринадлежности функции f классам Q и R с точностью до изострофии возможные варианты заполнения таблиц (a), (b), (c) из (2) перечислены ниже:

$$f_1\colon\begin{array}{|ccc|}\hline 0&1&0\\1&2&1\\0&1&0\\\hline\end{array},\quad f_2\colon\begin{array}{|ccc|}\hline 0&1&0\\1&2&1\\0&1&1\\\hline\end{array},\quad f_3\colon\begin{array}{|ccc|}\hline 0&1&0\\1&2&1\\1&1&1\\\hline\end{array},$$

$$f_4\colon\begin{array}{|ccc|}\hline 0&1&1\\1&2&1\\1&1&1\\\hline\end{array},\quad f_5\colon\begin{array}{|ccc|}\hline 0&1&1\\1&2&1\\1&1&2\\\hline\end{array},\quad f_6\colon\begin{array}{|ccc|}\hline 0&1&1\\1&2&2\\0&1&1\\\hline\end{array}.$$

Пусть $\mathbf{p},\mathbf{q}\in\mathbf{S}^{(3)}$ — произвольные распределения. Положим $\mathbf{r}^{(i)}=\widehat{f_i}(\mathbf{p},\mathbf{q})$ и покажем, что для всех $i=1,\ldots,6$ имеет место включение $\mathbf{r}^{(i)}\in\mathbf{T}$.

При $i = 1, 2, 3, 4$ выполнены соотношения

$$\sqrt{r_0^{(i)}} + \sqrt{r_2^{(i)}} \leqslant \sqrt{(p_0 + p_2)(q_0 + q_2)} + \sqrt{p_1 q_1} = \\ = \sqrt{(1 - p_1)(1 - q_1)} + \sqrt{p_1 q_1} \leqslant 1,$$

где последнее неравенство вытекает из леммы 4. Аналогично оценим:

$$\sqrt{r_0^{(5)}} + \sqrt{r_2^{(5)}} \leqslant \sqrt{p_0 q_0} + \sqrt{(1 - p_0)(1 - q_0)} \leqslant 1,$$
$$\sqrt{r_0^{(6)}} + \sqrt{r_2^{(6)}} = \sqrt{(1 - p_1) q_0} + \sqrt{p_1 (1 - q_0)} \leqslant 1.$$

Эти неравенства и определение множества $\mathbf{T}$ обеспечивают принадлежность $\mathbf{r}^{(i)} \in \mathbf{T}$ для всех $i = 1, \ldots, 6$. Таким образом, любые значения функций $\widehat{f_i}$ принадлежат $\mathbf{T}$, а следовательно, $W_{P_3^1 \cup \{f_i\}}(\mathbf{\Delta}) \subseteq \mathbf{T}$. Теорема 1 доказана.

Утверждение теоремы 1 легко может быть распространено на системы, содержащие несколько функций из $P_3(2) \setminus P_3^1$.

Следствие 1. *Пусть B — система функций, удовлетворяющая соотношениям $P_3^1 \cap P_3(2) \subseteq B \subseteq P_3(2)$. Тогда*

$$W_B(\mathbf{\Delta}) = \begin{cases} \mathbf{\Delta}, & \text{если } B \setminus P_3^1 \subseteq \{f \mid \omega(f) < 3\}, \\ \mathbf{S}^{(3)}, & \text{если } B \cap (Q \cup R) \neq \varnothing, \\ \mathbf{T} & \text{иначе.} \end{cases}$$

Заключение

Доказанные в следствии 1 свойства алгебр распределений $W_B(\mathbf{\Delta})$ показывают, что возможность приближения случайных величин с распределениями из $\mathbf{\Delta}$, являясь, очевидно, необходимым условием аппроксимационной полноты, не будет достаточным. Как и в булевом случае, возникает класс функций (в данном случае — $P_3(2) \setminus (Q \cup R)$), любое подмножество которого аппроксимационно неполно. Есть основания полагать, что свойства, определяющие классы Q и R, сохранят свою важность и для проверки аппроксимационной полноты систем функций с бóльшим числом переменных.

Автор посвящает настоящую статью профессору О. М. Касим-Заде, своему учителю, который всегда с большим вниманием и интересом следил за исследованиями автора.

ЛИТЕРАТУРА

1. **Бухараев Р. Г.** Об управляемых генераторах случайных величин // Вероятностные методы и кибернетика. II. Учён. зап. Казан. ун-та. Т. 123, кн. 6. Казань: Изд-во Казан. ун-та, 1963. С. 68–87.
2. **Wilhelm D., Bruck J., Qian L.** Probabilistic switching circuits in DNA // Proc. Nat. Acad. Sci. USA. 2018. Vol. 115, No. 5. P. 903–908.
3. **Markovski S.** Design of crypto primitives based on quasigroups // Quasigroups Related Syst. 2015. Vol. 23, No 1. P. 41–90.
4. **Колпаков Р. М.** Замкнутые классы конечных распределений рациональных вероятностей // Дискрет. анализ и исслед. операций. Сер. 1. 2004. Т. 11, № 3. С. 16–31.
5. **Схиртладзе Р. Л.** О методе построения булевой величины с заданным распределением вероятностей // Дискрет. анализ. Вып. 7. Новосибирск: Наука, 1966. С. 71–80.
6. **Яшунский А. Д.** О преобразованиях вероятности бесповторными булевыми формулами // Синтез и сложность управляющих систем. Мат. XVI Междунар. шк.-семин. (Санкт-Петербург, Россия, 26–30 июня 2006 г.). М.: Мех.-мат. фак. МГУ, 2006. С. 150–155.
7. **Zhou H., Loh P.-L., Bruck J.** The synthesis and analysis of stochastic switching circuits. Ithaca, NY: Cornell Univ., 2012. (Cornell Univ. Libr. e-Print Archive; arXiv:1209.0715).
8. **Яшунский А. Д.** Алгебры вероятностных распределений на конечных множествах // Тр. МИАН. 2018. Т. 301. С. 320–335.
9. **Белоусов В. Д.** Основы теории квазигрупп и луп. М.: Наука, 1967.
10. **Белоусов В. Д.** Неассоциативные бинарные системы // Алгебра. Топология. Геометрия. 1965. Итоги науки. Сер. Мат. М.: ВИНИТИ, 1967. С. 63–81.
11. **Яблонский С. В.** Функциональные построения в k-значной логике // Сборник статей по математической логике и её приложениям к некоторым вопросам кибернетики. Тр. МИАН СССР. Т. 51. М.: Изд-во АН СССР, 1958. С. 5–142.

Яшунский Алексей Дмитриевич

Статья поступила
24 февраля 2021 г.
После доработки —
24 февраля 2021 г.
Принята к публикации
18 марта 2021 г.

DISKRETNYI ANALIZ I ISSLEDOVANIE OPERATSII
/DISCRETE ANALYSIS AND OPERATIONS RESEARCH/
July–September 2021. Vol. 28, No. 3. P. 90–103

UDC 519.716+519.214.7 DOI 10.33048/daio.2021.28.707

ON THREE-VALUED RANDOM VARIABLE TRANSFORMATIONS BY BIVARIATE FUNCTIONS

A. D. Yashunsky

Keldysh Institute of Applied Mathematics RAS,
4 Miusskaya Square, 125047 Moscow, Russia
E-mail: yashunsky@keldysh.ru

Abstract. We consider transformations of three-valued random variables by three-valued logic functions. For arbitrary systems of bivariate functions that contain all functions with inessential variables we describe the classes of random variable distributions approximated by substituting independent random variables that omit at least one of three values for arguments of the said operations. Illustr. 2, bibliogr. 11.

Keywords: three-valued logic, random variable, distribution, approximation.

REFERENCES

1. **R. G. Bukharaev,** On controlled generators of random numbers, in *Probabilistic Methods and Cybernetics. II* (Uch. Zap. Kazan. Gos. Univ., Vol. 123, B. 6) (Izd. Kazan. Univ., Kazan, 1963), pp. 68–87 [Russian].
2. **D. Wilhelm, J. Bruck,** and **L. Qian,** Probabilistic switching circuits in DNA, *Proc. Nat. Acad. Sci. USA* **115** (5), 903–908 (2018).
3. **S. Markovski,** Design of crypto primitives based on quasigroups, *Quasigr. Relat. Syst.* **23** (1), 41–90 (2015).
4. **R. M. Kolpakov,** Closed classes of finite distributions of rational probabilities, *Diskretn. Anal. Issled. Oper., Ser. 1,* **11** (3), 16–31 (2004) [Russian].
5. **R. L. Skhirtladze,** On a method for constructing a Boolean value with a given probability distribution, in *Discrete Analysis*, Vol. 7 (Nauka, Novosibirsk, 1966), pp. 71–80 [Russian].
6. **A. D. Yashunsky,** On probability transformations by read-once Boolean formulas, in *Proc. XVI Int. School and Seminar "Synthesis and Complexity of Control Systems", St. Petersburg, Russia, June 26–30, 2006* (Mekh.-Mat. Fak. MGU, Moscow, 2006), pp. 150–155 [Russian].

This research is supported by the Russian Science Foundation (Project 19–71–30004).

English version: Journal of Applied and Industrial Mathematics **15** (3) (2021).

7. **H. Zhou, P.-L. Loh,** and **J. Bruck,** The synthesis and analysis of stochastic switching circuits (Cornell Univ., Ithaca, NY, 2012) (Cornell Univ. Libr. e-Print Archive; arXiv:1209.0715).
8. **A. D. Yashunsky,** Algebras of probability distributions on finite sets, *Tr. Mat. Inst. Steklov.* **301**, 320–335 (2018) [Russian] [*Proc. Steklov Inst. Math.* **301**, 305–319 (2018)].
9. **V. D. Belousov,** *Fundamentals of the Theory of Quasigroups and Loops* (Moscow, Nauka, 1967) [Russian].
10. **V. D. Belousov,** Nonassociative binary systems, in *Itogi Nauki., Ser. Mat. Algebra Topol. Geom., 1965* (VINITI, Moscow, 1967), pp. 63–81 [Russian].
11. **S. V. Yablonskii,** Functional constructions in a k-valued logic, *Trudy Mat. Inst. Steklov.*, **51**, 5–142 (1958) [Russian].

Aleksey D. Yashunsky

Received February 24, 2021
Revised February 24, 2021
Accepted March 18, 2021