ИПМ им.М.В.Келдыша РАН • Электронная библиотека

Препринты ИПМ • Препринт № 34 за 2018 г.

ISSN 2071-2898 (Print)
ISSN 2071-2901 (Online)

Яшунский А. Д.

О конечных алгебрах бернуллиевских распределений

Рекомендуемая форма библиографической ссылки: Яшунский А. Д. О конечных алгебрах бернуллиевских распределений // Препринты ИПМ им. М.В.Келдыша. 2018. № 34. 19 с. doi:10.20948/prepr-2018-34
URL: http://library.keldysh.ru/preprint.asp?id=2018-34

Ордена Ленина
ИНСТИТУТ ПРИКЛАДНОЙ МАТЕМАТИКИ
имени М.В. Келдыша
Российской академии наук

А. Д. Яшунский

О конечных алгебрах бернуллиевских распределений

Москва — 2018

Яшунский А. Д.

О конечных алгебрах бернуллиевских распределений

Рассматриваются множества бернуллиевских распределений, замкнутые относительно подстановки независимых случайных величин в булевы функции из некоторого заданного множества (алгебры бернуллиевских распределений). Описаны все конечные алгебры бернуллиевских распределений.

Ключевые слова: случайная величина, распределение Бернулли, конечная алгебра

Alexey Dmitrievich Yashunsky

On finite algebras of Bernoulli distributions

We consider sets of Bernoulli distributions closed under transformations of independent random variables by Boolean functions from a given set (algebras of Bernoulli distributions). We provide a description of all finite Bernoulli distribution algebras.

Key words: random variable, Bernoulli distribution, finite algebra

Работа выполнена при поддержке гранта РНФ, проект 14-21-00025 П.

Оглавление

Введение

В математической кибернетике достаточно давно рассматривается задача преобразования дискретных случайных величин — получения случайных величин с требуемыми распределениями путем подстановки независимых случайных величин с заданными распределениями в некоторую функцию. Одна из ранних постановок задачи в таком виде содержится, например, в работе Р. Г. Бухараева [1].

При рассмотрении подобных задач естественным образом возникают вопросы выразимости одних распределений через другие. Подобные задачи весьма удобно формулировать на языке универсальных алгебр: каждой преобразующей функции соответствует некоторая операция на распределениях, тем самым задается алгебра на множестве распределений, в которой можно рассматривать подалгебры, порождаемые различными множествами. По-видимому, впервые в подобных терминах эти задачи были сформулированы в работе Ф. И. Салимова [3].

Вообще говоря, рассматривались алгебры распределений случайных величин над различными конечными множествами, однако в рамках данной работы мы ограничимся только бернуллиевскими случайными величинами, преобразования которых осуществляются булевыми функциями. Эти задачи достаточно хорошо изучены, особенно в случае, когда распределения имеют рациональные компоненты (см., например, работу Р. М. Колпакова [2]).

Помимо выразимости случайных величин рассматривается также аппроксимируемость: возможность построения случайной величины, распределение которой сколь угодно близко к требуемому. Фактически, задачи об аппроксимируемости сводятся к исследованию множества предельных точек в алгебрах распределений. Примечательно, что для достаточно простых систем булевых функций индуцируемые алгебры распределений могут быть всюду плотными в множестве распределений. Так, например, в работе Р. Л. Схиртладзе [4] показано, что любое невырожденное распределение порождает при подстановке в систему функций «конъюнкция, дизъюнкция, отрицание» всюду плотную алгебру.

Возможны и иные варианты: так, в частности, из работы автора [7] вытекает, что любое конечное множество бернуллиевских распределений при подстановке в линейные функции порождает алгебру распределений с единственной предельной точкой — равномерным распределением; существуют также системы операций, относительно которых порождаются, например, алгебры со счетным множеством предельных точек, не являющиеся при этом всюду плотными, см. [6].

Среди разнообразных конфигураций предельных точек алгебр распределений определенный интерес представляют случаи, когда в алгебре распределений предельных точек нет вовсе: конечные алгебры распределений. Относительно тривиальные примеры подобных алгебр несложно построить, однако далеко не очевидно, исчерпывают ли эти примеры все возможные конечные алгебры распределений.

В данной работе устанавливаются условия, при которых алгебра бернуллиевских распределений конечна. Они позволяют утверждать, что конечные алгебры — явление, в некотором смысле, редкое: любая конечная алгебра может быть неформально признана «вырожденной», либо в силу устройства своего основного множества, либо из-за своей сигнатуры.

Определения и вспомогательные утверждения

Пусть X — бернуллиевская случайная величина, значения которой принадлежат множеству $\{0, 1\}$. Тогда ее распределение есть двумерный вектор (p_0, p_1), где $p_0 \geqslant 0$, $p_1 \geqslant 0$, $p_0 + p_1 = 1$. Такой вектор однозначно задается любой из двух своих компонент, для определенности далее будем использовать компоненту p_1. При этом множество S таких векторов находится в естественном взаимно-однозначном соответствии с отрезком $[0; 1]$, поэтому далее, говоря о бернуллиевских распределениях, будем отождествлять их с числами из этого отрезка. Распределения 0 и 1 будем называть *вырожденными*.

Пусть B — некоторое множество булевых функций. Если $f(x_1, \ldots, x_n) \in B$ — булева функция от n переменных и $X_1, \ldots, X_n$ — независимые в совокупности бернуллиевские случайные величины со значениями в $\{0, 1\}$ и распределениями $p_1, \ldots, p_n \in S$ соответственно, то $f(X_1, \ldots, X_n)$ есть также случайная величина со значениями в $\{0, 1\}$ и для ее распределения $q \in S$ выполнено

$$q = \sum_{\substack{(\sigma_1,\ldots,\sigma_n)\in\{0,1\}^n,\\ f(\sigma_1,\ldots,\sigma_n)=1}} s(p_1, \sigma_1) \cdots s(p_n, \sigma_n), \tag{1}$$

где $s(p, 1) = p$ и $s(p, 0) = 1 - p$. Таким образом, каждая операция $f(x_1, \ldots, x_n) \in B$ индуцирует полилинейное отображение $\hat{f}(p_1, \ldots, p_n)$ из S^n в S, заданное равенством (1). Обозначим $\hat{B} = \{\hat{f} \mid f \in B\}$, тогда $\langle S, \hat{B}\rangle$ есть *алгебра бернуллиевских распределений*, индуцированная множеством булевых функций B.

Алгебра $\langle S, \hat{B}\rangle$ содержит собственные подалгебры. В данной работе изучаются конечные подалгебры алгебры $\langle S, \hat{B}\rangle$, т. е. такие подалгебры $\langle G, \hat{B}\rangle$, в которых множество G конечно. Тривиальным примером конечной подалгебры с сигнатурой $\hat{B}$ является алгебра вырожденных распределений $\langle \{0,1\}, \hat{B}\rangle$. Несложно видеть, что она изоморфна алгебре $\langle \{0,1\}, B\rangle$ из булевых констант 0 и 1 с множеством булевых операций B. Указание на существование таких подалгебр содержится (в несколько иных терминах) уже в работе Р. Г. Бухараева [1].

Рассмотрим некоторые свойства операций из $\hat{B}$ и алгебр бернуллиевских распределений.

Пусть $f(x_1, \ldots, x_n) \in B$ — булева функция, обозначим ее подфункции $f(0, x_2, \ldots, x_n)$ и $f(1, x_2, \ldots, x_n)$ через f_0 и f_1 соответственно. Несложно видеть, что для $\hat{f}$ имеет место разложение, аналогичное разложению функции f по ее первой переменной:

$$\hat{f}(p_1, \ldots, p_n) = (1 - p_1)\hat{f}_0(p_2, \ldots, p_n) + p_1\hat{f}_1(p_2, \ldots, p_n).$$

В частности, если $\hat{f}_0 = \hat{f}_1$, то $\hat{f} = \hat{f}_0 = \hat{f}_1$. Как следствие, если функции f и g получаются друг из друга добавлением и изъятием несущественных переменных, то выполнено $\hat{f} = \hat{g}$. Естественно, разложение может быть продолжено по второй, третьей и т. д. переменным. Разложение функции $\hat{f}$ по всем ее переменным дает выражение, идентичное формуле (1).

Напомним, что функция $f^*(x_1, \ldots, x_n) = \overline{f(\bar{x}_1, \ldots, \bar{x}_n)}$ называется *двойственной* к булевой функции f. Как показывает лемма ниже, для каждой подалгебры распределений, существует изоморфная ей алгебра с двойственной сигнатурой.

Лемма 1. *Пусть $\langle G, \hat{B}\rangle$ — алгебра бернуллиевских распределений. Положим $G^* = \{1 - g \mid g \in G\}$ и $B^* = \{f^* \mid f \in B\}$. Тогда $\langle G^*, \hat{B}^*\rangle$ — алгебра, изоморфная $\langle G, \hat{B}\rangle$.*

Доказательство. Положим $\varphi(g) = 1 - g$ и покажем, что для любых распределений $g_1, \ldots, g_n \in G$ и любой функции $f \in B$ выполнено равенство $\varphi(\hat{f}(g_1, \ldots, g_n)) = \hat{f}^*(\varphi(g_1), \ldots, \varphi(g_n))$. Согласно выражению (1) для $\hat{f}^*$ имеем

$$\hat{f}^*(\varphi(g_1), \ldots, \varphi(g_n)) = \sum_{f^*(\sigma_1,\ldots,\sigma_n)=1} s(\varphi(g_1), \sigma_1) \cdots s(\varphi(g_n), \sigma_n) =$$

$$= \sum_{f(\bar{\sigma}_1,\ldots,\bar{\sigma}_n)=0} s(\varphi(g_1), \sigma_1) \cdots s(\varphi(g_n), \sigma_n) = \sum_{f(\sigma_1,\ldots,\sigma_n)=0} s(\varphi(g_1), \bar{\sigma}_1) \cdots s(\varphi(g_n), \bar{\sigma}_n).$$

Несложно проверить, что $s(\varphi(g), \bar{\sigma}) = s(g, \sigma)$, откуда

$$\hat{f}^*(\varphi(g_1), \ldots, \varphi(g_n)) = \sum_{f(\sigma_1,\ldots,\sigma_n)=0} s(g_1, \sigma_1) \cdots s(g_n, \sigma_n) =$$
$$= 1 - \sum_{f(\sigma_1,\ldots,\sigma_n)=1} s(g_1, \sigma_1) \cdots s(g_n, \sigma_n) = \varphi(\hat{f}(g_1, \ldots, g_n)),$$

что и требовалось доказать. Отсюда легко вытекает, что множество G^* замкнуто относительно операций из $\hat{B}^*$, так как по условию леммы множество G замкнуто относительно операций из $\hat{B}$. При этом отображение φ является искомым изоморфизмом алгебр. □

Лемма 2. *Пусть* $p_1, \ldots, p_n \notin \{0, 1\}$ *и* $\hat{f}(p_1, \ldots, p_n) = c \in \{0, 1\}$. *Тогда булева функция* $f(x_1, \ldots, x_n)$ *— постоянная, равная* c.

Доказательство. Предположим, что $f \not\equiv 0$ и при этом имеет место равенство $\hat{f}(p_1, \ldots, p_n) = 0$. Из $f \not\equiv 0$ вытекает, что представление (1) для $\hat{f}$ содержит по крайней мере одно слагаемое вида $s(p_1, \sigma_1) \cdots s(p_n, \sigma_n)$ с некоторыми $\sigma_1, \ldots, \sigma_n \in \{0, 1\}$. Легко видеть, что для $p_1, \ldots, p_n \notin \{0, 1\}$ это слагаемое строго положительно. В совокупности с неотрицательностью всех прочих слагаемых, входящих в $\hat{f}$, получаем, что $\hat{f}(p_1, \ldots, p_n) > 0$, что противоречит сделанному предположению. Таким образом, равенство $\hat{f}(p_1, \ldots, p_n) = 0$ влечет $f \equiv 0$.

Из соображений двойственности с использованием леммы 1 получаем, что равенство $\hat{f}(p_1, \ldots, p_n) = 1$ влечет $f \equiv 1$. Лемма доказана. □

Лемма 3. *Пусть* B *индуцирует некоторую конечную алгебру* $\langle G, \hat{B}\rangle$, *причем* $|G \setminus \{0, 1\}| > 1$. *Пусть* $f(x_1, \ldots, x_n) \in B$, *тогда либо функция* f *имеет не более одной существенной переменной, либо для любого* $i = 1, \ldots, n$ *и любых* $\alpha_1, \ldots, \alpha_{i-1}, \alpha_{i+1}, \ldots, \alpha_n \in G \setminus \{0, 1\}$ *имеет место равенство*

$$\hat{f}(\alpha_1, \ldots, \alpha_{i-1}, 0, \alpha_{i+1}, \ldots, \alpha_n) = \hat{f}(\alpha_1, \ldots, \alpha_{i-1}, 1, \alpha_{i+1}, \ldots, \alpha_n).$$

Доказательство. Пусть заданы, согласно условию леммы, $f \in B$, $i \in \{1, \ldots, n\}$, $\alpha_1, \ldots, \alpha_{i-1}, \alpha_{i+1}, \ldots, \alpha_n \in G \setminus \{0, 1\}$. Выберем некоторое $p_0 \in G \setminus \{0, 1\}$ и рассмотрим последовательность, заданную равенством $p_{t+1} = \hat{f}(\alpha_1, \ldots, \alpha_{i-1}, p_t, \alpha_{i+1}, \ldots, \alpha_n)$. Положим

$$A = \begin{pmatrix} 1 - \hat{f}(\ldots, \alpha_{i-1}, 0, \alpha_{i+1}, \ldots) & \hat{f}(\ldots, \alpha_{i-1}, 0, \alpha_{i+1}, \ldots) \\ 1 - \hat{f}(\ldots, \alpha_{i-1}, 1, \alpha_{i+1}, \ldots) & \hat{f}(\ldots, \alpha_{i-1}, 1, \alpha_{i+1}, \ldots) \end{pmatrix}.$$

Используя разложение для функции $\hat{f}$ по i-ой переменной, легко убедиться, что выполнено матричное равенство $(1-p_{t+1}, p_{t+1}) = (1-p_t, p_t)A$.

Таким образом, значения p_t представляют собой вероятности нахождения во втором из двух состояний цепи Маркова, заданной матрицей A, после t шагов. Поскольку все $p_t \in G$ и G — конечное множество, такая цепь Маркова не может быть произвольной.

Если рассматриваемая цепь периодическая с периодом 2, то имеют место равенства $\hat{f}(\dots, \alpha_{i-1}, 0, \alpha_{i+1}, \dots) = 1$ и $\hat{f}(\dots, \alpha_{i-1}, 1, \alpha_{i+1}, \dots) = 0$, которые с использованием разложения по i-ой переменной и применением леммы 2 к подфункциям от $n-1$ переменной легко влекут равенство $f = \bar{x}_i$.

Если рассматриваемая цепь представляет собой объединение двух несвязных поглощающих состояний, то матрица A единичная, что путем рассуждений, аналогичных описанным выше, влечет $f = x_i$.

В иных случаях рассматриваемая цепь Маркова является апериодической и имеет ровно один неприводимый класс возвратных состояний, что влечет наличие у матрицы A единственного вектора вида $(1-p, p)$, удовлетворяющего равенству $(1-p, p) = (1-p, p)A$, т. е. описывающего стационарное распределение цепи (подробнее о цепях Маркова см. [5]).

Поскольку множество $G \setminus \{0, 1\}$ содержит не менее двух различных распределений, которые не могут быть оба стационарными для матрицы A, получаем, что матрица A должна задавать цепь Маркова, сходящуюся для некоторых начальных распределений за конечное число шагов.

В работе [8] показано, что для сходимости цепи Маркова за конечное число шагов необходимо наличие у матрицы A нулевого собственного значения. Это равносильно тому, что определитель матрицы A равен нулю. Положим $a = \hat{f}(\dots, \alpha_{i-1}, 0, \alpha_{i+1}, \dots)$ и $b = \hat{f}(\dots, \alpha_{i-1}, 1, \alpha_{i+1}, \dots)$. Тогда $\begin{vmatrix} 1-a & a \\ 1-b & b \end{vmatrix} = 0$, откуда $a = b$, что и составляет утверждение леммы.

□

Унарные алгебры

Помимо уже упоминавшихся конечных алгебр с основным множеством, входящим в $\{0, 1\}$, простым примером конечных алгебр могут служить алгебры, индуцированные функциями, существенно зависящими менее чем от двух переменных.

Легко видеть, что если в сигнатуре $\hat{B}$ содержатся только функции, индуцированные (с точностью до несущественных переменных) функциями 0, 1, x и $\bar{x}$, то замыкание любого конечного множества распределений относительно операций из $\hat{B}$, порождает заведомо конечную

алгебру $\langle G, \hat{B}\rangle$ — *унарную*, так как функции из $\hat{B}$ также фактически являются функциями одной переменной или константами.

При этом почти очевидно, что множество G удовлетворяет следующим условиям: если $0 \in B$, то $0 \in G$; если $1 \in B$, то $1 \in G$; если $\bar{x} \in B$, то $G = \{1 - g \mid g \in G\}$. Конструирование подобных конечных алгебр не представляет ни сложности, ни особого интереса.

Неунарные алгебры

Более интересным представляется случай, когда в множестве B содержатся функции с двумя или более существенными переменными. В этом случае оказывается, что основное множество конечной алгебры может содержать самое большее три элемента. Более того, имеет место следующая теорема.

Теорема 1. *Пусть B содержит функции, существенно зависящие более чем от одной переменной, и индуцированная B алгебра $\langle G, \hat{B}\rangle$ — конечна. Тогда $|G \setminus \{0, 1\}| \leqslant 1$.*

Доказательство. Пусть $f(x_1, \ldots, x_n) \in B$ существенно зависит от более чем одной переменной. Предположим, что существуют $p, q \in G \setminus \{0, 1\}$, $p \neq q$.

Обозначим $\hat{f}(p, \ldots, p) = h$. Покажем, что для произвольного набора $\tilde{\beta} = (\beta_1, \ldots, \beta_n) \in \{0, 1, p\}^n$, имеет место равенство $\hat{f}(\beta_1, \ldots, \beta_n) = h$.

Доказательство проведем индукцией по числу b компонент в $\tilde{\beta}$, отличных от p. В случае $b = 0$ (т. е. когда все компоненты равны p) утверждение верно в силу определения h.

Пусть утверждение доказано для $b = m$, покажем, что оно верно для $b = m + 1$. Рассмотрим все наборы $\tilde{\beta}$, у которых компоненты отличные от p стоят на фиксированных $m + 1$ местах: для удобства будем считать, что это первые $m + 1$ мест, в остальных случаях доказательство проводится аналогично. Итак, $\beta_1, \ldots, \beta_{m+1} \in \{0, 1\}$, $\beta_{m+2} = \cdots = \beta_n = p$.

Рассмотрим набор $(\beta_1, \ldots, \beta_{i-1}, 0, \beta_{i+1}, \ldots, \beta_n)$, где $i \leqslant m + 1$. В силу предположения индукции имеет место равенство:

$$(1 - p)\hat{f}(\beta_1, \ldots, \beta_{i-1}, 0, \beta_{i+1}, \ldots, \beta_n) + p\hat{f}(\beta_1, \ldots, \beta_{i-1}, 1, \beta_{i+1}, \ldots, \beta_n) = \\ = \hat{f}(\beta_1, \ldots, \beta_{i-1}, p, \beta_{i+1}, \ldots, \beta_n) = h \quad (2)$$

Обозначим $\hat{f}(\underbrace{0,\dots,0}_{m+1},p,\dots,p)=h_0$. Тогда из равенств (2) вытекает, что

$$\hat{f}(1,0,\dots,0,p,\dots,p)=\hat{f}(0,1,0,\dots,0,p,\dots,p)=\dots=$$
$$=\hat{f}(0,\dots,0,1,p,\dots,p)=\frac{1}{p}(h-(1-p)h_0).$$

Таким образом, значения $\hat{f}(\beta_1,\dots,\beta_n)$ на всех наборах, у которых среди $\beta_1,\dots,\beta_{m+1}$ ровно одна единица, совпадают: обозначим это значение через h_1. Аналогично из равенств (2) вытекает, что значения $\hat{f}(\beta_1,\dots,\beta_n)$ совпадают на наборах $\tilde{\beta}$ с произвольным фиксированным количеством единиц среди $\beta_1,\dots,\beta_{m+1}$. Обозначим через h_i значение $\hat{f}(\beta_1,\dots,\beta_n)$, если среди $\beta_1,\dots,\beta_{m+1}$ ровно i единиц. Тогда равенства (2) можно переписать в виде:

$$(1-p)h_i+ph_{i+1}=h,\quad i=0,\dots,m. \tag{3}$$

Покажем, что в действительности имеет место $h_0=\dots=h_{m+1}=h$. Из леммы 3 вытекает, что для любого $j=0,\dots,m$ имеет место равенство:

$$\hat{f}(0,\underbrace{\overbrace{q,\dots,q}^{m},p,\dots,p}_{j},\dots,p)=\hat{f}(1,\underbrace{\overbrace{q,\dots,q}^{m},p,\dots,p}_{j},\dots,p). \tag{4}$$

Раскладывая функции по первым m переменным, с использованием ранее введенных обозначений h_i равенства (4) можно переписать следующим образом:

$$\sum_{l=0}^{j}\binom{j}{l}q^l(1-q)^{j-l}\sum_{s=0}^{m-j}\binom{m-j}{s}p^s(1-p)^{m-j-s}h_{l+s}=$$
$$=\sum_{l=0}^{j}\binom{j}{l}q^l(1-q)^{j-l}\sum_{s=0}^{m-j}\binom{m-j}{s}p^s(1-p)^{m-j-s}h_{l+s+1}.$$

Покажем теперь, что в сделанных выше предположениях при всех $t=0,\dots,m$ и всех $j=0,\dots,t$ имеют место аналогичные равенства

$$\sum_{l=0}^{j}\binom{j}{l}q^l(1-q)^{j-l}\sum_{s=0}^{t-j}\binom{t-j}{s}p^s(1-p)^{t-j-s}h_{l+s}=$$
$$=\sum_{l=0}^{j}\binom{j}{l}q^l(1-q)^{j-l}\sum_{s=0}^{t-j}\binom{t-j}{s}p^s(1-p)^{t-j-s}h_{l+s+1}. \tag{5}$$

Отметим, что равенства (5) представляют собой развернутую запись следующих соотношений, аналогичных равенствам (4):

$$\hat{f}(0,\overbrace{0,\dots,0}^{m-t},\underbrace{\overbrace{q,\dots,q}^{t},p,\dots,p}_{j},\dots,p)=\hat{f}(1,\overbrace{0,\dots,0}^{m-t},\underbrace{\overbrace{q,\dots,q}^{t},p,\dots,p}_{j},\dots,p).$$

Их выполнение, вообще говоря, не вытекает непосредственно из ранее доказанных утверждений.

Для $t=m$ равенства выполнены. Покажем, что если они выполнены для $t=T$, т. е.

$$\sum_{l=0}^{j}\binom{j}{l}q^l(1-q)^{j-l}\sum_{s=0}^{T-j}\binom{T-j}{s}p^s(1-p)^{T-j-s}h_{l+s}=$$
$$=\sum_{l=0}^{j}\binom{j}{l}q^l(1-q)^{j-l}\sum_{s=0}^{T-j}\binom{T-j}{s}p^s(1-p)^{T-j-s}h_{l+s+1}, \quad (6)$$

то они также выполнены для $t=T-1$.

Преобразуем сумму из левой части равенства (6):

$$\sum_{s=0}^{T-j}\binom{T-j}{s}p^s(1-p)^{T-j-s}h_{l+s}=\sum_{s=0}^{T-j}\left(\binom{T-j-1}{s}+\binom{T-j-1}{s-1}\right)p^s(1-p)^{T-j-s}h_{l+s}=$$
$$=\sum_{s=0}^{T-j}\binom{T-j-1}{s}p^s(1-p)^{T-j-s}h_{l+s}+\sum_{s=0}^{T-j}\binom{T-j-1}{s-1}p^s(1-p)^{T-j-s}h_{l+s}=$$
$$=\sum_{s=0}^{T-j-1}\binom{T-j-1}{s}p^s(1-p)^{T-j-1-s+1}h_{l+s}+$$
$$+\sum_{s=1}^{T-j}\binom{T-j-1}{s-1}p^{(s-1)+1}(1-p)^{T-j-1-(s-1)}h_{l+(s-1)+1}=$$
$$=(1-p)\sum_{s=0}^{T-j-1}\binom{T-j-1}{s}p^s(1-p)^{T-j-1-s}h_{l+s}+p\sum_{s=0}^{T-j-1}\binom{T-j-1}{s}p^s(1-p)^{T-j-1-s}h_{l+s+1}.$$

Выполняя аналогичные преобразования в правой части, равенства (6)

при $j = 0, \ldots, T-1$ можно переписать в виде:

$$(1-p)\sum_{l=0}^{j}\binom{j}{l}q^l(1-q)^{j-l}\sum_{s=0}^{T-1-j}\binom{T-1-j}{s}p^s(1-p)^{T-1-j-s}h_{l+s}+$$
$$+p\sum_{l=0}^{j}\binom{j}{l}q^l(1-q)^{j-l}\sum_{s=0}^{T-j-1}\binom{T-1-j}{s}p^s(1-p)^{T-1-j-s}h_{l+s+1}=$$
$$=(1-p)\sum_{l=0}^{j}\binom{j}{l}q^l(1-q)^{j-l}\sum_{s=0}^{T-1-j}\binom{T-1-j}{s}p^s(1-p)^{T-1-j-s}h_{l+s+1}+$$
$$+p\sum_{l=0}^{j}\binom{j}{l}q^l(1-q)^{j-l}\sum_{s=0}^{T-j-1}\binom{T-1-j}{s}p^s(1-p)^{T-1-j-s}h_{l+s+2}. \quad (7)$$

Заменим в равенстве (6) все вхождения j на $j+1$. Тогда при $j = 0, \ldots, T-1$ имеет место равенство:

$$\sum_{l=0}^{j+1}\binom{j+1}{l}q^l(1-q)^{j+1-l}\sum_{s=0}^{T-j-1}\binom{T-j-1}{s}p^s(1-p)^{T-j-1-s}h_{l+s}=$$
$$=\sum_{l=0}^{j+1}\binom{j+1}{l}q^l(1-q)^{j+1-l}\sum_{s=0}^{T-j-1}\binom{T-j-1}{s}p^s(1-p)^{T-j-1-s}h_{l+s+1}.$$

Эти равенства с использованием разложения $\binom{j+1}{l} = \binom{j}{l} + \binom{j}{l-1}$ могут быть преобразованы к следующему виду:

$$(1-q)\sum_{l=0}^{j}\binom{j}{l}q^l(1-q)^{j-l}\sum_{s=0}^{T-1-j}\binom{T-1-j}{s}p^s(1-p)^{T-1-j-s}h_{l+s}+$$
$$+q\sum_{l=0}^{j}\binom{j}{l}q^l(1-q)^{j-l}\sum_{s=0}^{T-j-1}\binom{T-1-j}{s}p^s(1-p)^{T-1-j-s}h_{l+s+1}=$$
$$=(1-q)\sum_{l=0}^{j}\binom{j}{l}q^l(1-q)^{j-l}\sum_{s=0}^{T-1-j}\binom{T-1-j}{s}p^s(1-p)^{T-1-j-s}h_{l+s+1}+$$
$$+q\sum_{l=0}^{j}\binom{j}{l}q^l(1-q)^{j-l}\sum_{s=0}^{T-j-1}\binom{T-1-j}{s}p^s(1-p)^{T-1-j-s}h_{l+s+2}. \quad (8)$$

Вычитая из равенств (7) равенства (8) после преобразований получаем

при $j = 0, \ldots, T-1$:

$$\sum_{l=0}^{j} \binom{j}{l} q^l (1-q)^{j-l} \sum_{s=0}^{T-1-j} \binom{T-1-j}{s} p^s (1-p)^{T-1-j-s} \left((q-p)h_{l+s} + (p-q)h_{l+s+1}\right) =$$
$$= \sum_{l=0}^{j} \binom{j}{l} q^l (1-q)^{j-l} \sum_{s=0}^{T-1-j} \binom{T-1-j}{s} p^s (1-p)^{T-1-j-s} \left((q-p)h_{l+s+1} + (p-q)h_{l+s+2}\right).$$

Поскольку $p \neq q$, равенства можно разделить на $q-p$, получив в результате

$$\sum_{l=0}^{j} \binom{j}{l} q^l (1-q)^{j-l} \sum_{s=0}^{T-1-j} \binom{T-1-j}{s} p^s (1-p)^{T-1-j-s} \left(h_{l+s} - h_{l+s+1}\right) =$$
$$= \sum_{l=0}^{j} \binom{j}{l} q^l (1-q)^{j-l} \sum_{s=0}^{T-1-j} \binom{T-1-j}{s} p^s (1-p)^{T-1-j-s} \left(h_{l+s+1} - h_{l+s+2}\right). \quad (9)$$

Непосредственно из равенств (3) вытекает, что для всех i выполнено $h_i - h_{i+1} = \frac{1}{p}(h_i - h)$. Подставляя эти соотношения в (9) и умножая равенство на p, получаем соотношение:

$$\sum_{l=0}^{j} \binom{j}{l} q^l (1-q)^{j-l} \sum_{s=0}^{T-1-j} \binom{T-1-j}{s} p^s (1-p)^{T-1-j-s} \left(h_{l+s} - h\right) =$$
$$= \sum_{l=0}^{j} \binom{j}{l} q^l (1-q)^{j-l} \sum_{s=0}^{T-1-j} \binom{T-1-j}{s} p^s (1-p)^{T-1-j-s} \left(h_{l+s+1} - h\right),$$

откуда легко следует, что для всех $j = 0, \ldots, T-1$ имеет место равенство:

$$\sum_{l=0}^{j} \binom{j}{l} q^l (1-q)^{j-l} \sum_{s=0}^{T-1-j} \binom{T-1-j}{s} p^s (1-p)^{T-1-j-s} h_{l+s} =$$
$$= \sum_{l=0}^{j} \binom{j}{l} q^l (1-q)^{j-l} \sum_{s=0}^{T-1-j} \binom{T-1-j}{s} p^s (1-p)^{T-1-j-s} h_{l+s+1}.$$

Таким образом, из выполнения равенств (5) при $t = T$ вытекает их выполнение для $t = T-1$, а значит они выполнены при всех $t = 0, \ldots, m$.

В частности, при $t = 0$ и $j = 0$ получаем

$$\sum_{l=0}^{0} \binom{0}{l} q^l (1-q)^{0-l} \sum_{s=0}^{0} \binom{0}{s} p^s (1-p)^{0-s} h_{l+s} = \\ = \sum_{l=0}^{0} \binom{0}{l} q^l (1-q)^{0-l} \sum_{s=0}^{0} \binom{0}{s} p^s (1-p)^{0-s} h_{l+s+1},$$

что в действительности представляет собой равенство $h_0 = h_1$. С учетом соотношений (3), это равенство влечет $h_0 = h_1 = h$. Применяя соотношения (3) многократно, получаем $h_0 = \cdots = h_{m+1} = h$.

Таким образом показано, что $\hat{f}(\beta_1, \ldots, \beta_n) = h$ для всех наборов $\tilde{\beta}$ содержащих ровно $m+1$ компоненту, отличную от p. По индукции получаем, что $\hat{f}(\beta_1, \ldots, \beta_n) = h$ для всех наборов $\tilde{\beta} \in \{0, 1, p\}^n$, в частности, для наборов $\tilde{\beta} \in \{0, 1\}^n$. Но для таких наборов значение $\hat{f}(\beta_1, \ldots, \beta_n) \in \{0, 1\}$, откуда вытекает, что $h \in \{0, 1\}$. Тогда в силу леммы 2, получаем, что функция f — константа, а это противоречит тому, что она существенно зависит от более чем одной переменной. Полученное противоречие показывает, что предположение о существовании $p, q \in G \setminus \{0, 1\}$, $p \neq q$ неверно. Теорема доказана. □

Помимо случая, когда $G \cap \{0, 1\} \neq \varnothing$, который будет рассмотрен далее, возможны также алгебры, в которых множество G состоит из единственного элемента $p \notin \{0, 1\}$. Для каждой функции $f \in B$ такое число p должно являться решением уравнения $\hat{f}(p, \ldots, p) = p$, которое очевидно, алгебраическое, поэтому число p — алгебраическое.

Достаточно просто построить разнообразные примеры алгебр из единственного элемента. Рассмотрим булевы функции трех переменных x_1, x_2, x_3, заданные таблицей ниже.

x_1	x_2	x_3	μ	λ	φ	ψ
0	0	0	0	0	0	0
0	0	1	0	1	1	1
0	1	0	0	1	1	1
0	1	1	1	0	0	1
1	0	0	0	1	0	0
1	0	1	1	0	0	0
1	1	0	1	0	1	0
1	1	1	1	1	0	0

Заметим, что $\hat{\mu}(p, p, p) = 3p^2(1-p) + p^3$, $\hat{\lambda}(p, p, p) = 3p(1-p)^2 + p^3$ и $\hat{\varphi}(p, p, p) = \hat{\psi}(p, p, p) = 2p(1-p)^2 + p^2(1-p)$. Отсюда легко получить,

что $\langle \frac{1}{2}, \hat{\mu} \rangle$, $\langle \frac{1}{2}, \hat{\lambda} \rangle$, $\langle \frac{1}{2}, \{\hat{\mu}, \hat{\lambda}\} \rangle$, а также $\langle \frac{3-\sqrt{5}}{2}, \hat{\varphi} \rangle$, $\langle \frac{3-\sqrt{5}}{2}, \hat{\psi} \rangle$ и $\langle \frac{3-\sqrt{5}}{2}, \{\hat{\varphi}, \hat{\psi}\} \rangle$ — конечные алгебры.

Алгебры с вырожденными распределениями

Как отмечалось ранее, для любого набора булевых функций B конечной алгеброй является $\langle \{0,1\}, \hat{B} \rangle$. В случае же наличия в конечной алгебре как вырожденных, так и невырожденных распределений, оказывается, что имеются весьма жесткие ограничения на индуцирующее множество булевых функций.

Напомним, что булева функция $f(x_1, \ldots, x_n)$ *линейна*, если она представляется в виде $x_{i_1} + \cdots + x_{i_m} + c \pmod 2$, где $c \in \{0,1\}$. Множество линейных булевых функций обозначим через L.

Теорема 2. *Пусть B содержит функции, существенно зависящие более чем от одной переменной, и индуцированная им алгебра $\langle G, \hat{B} \rangle$ — конечна. Если $G \not\subseteq \{0,1\}$ и $|G| > 1$, то $G \subseteq \{0, \frac{1}{2}, 1\}$ и $B \subseteq L$.*

Доказательство. Рассмотрим каждую функцию $f \in B$, существенно зависящую от более чем одной переменной. Для каждой такой функции $\langle G, \hat{f} \rangle$ — конечная алгебра бернуллиевских распределений.

В силу теоремы 1 имеет место включение $G \subseteq \{0,1,p\}$, где $p \notin \{0,1\}$. За исключением $G = \{0,1\}$ имеются три варианта, при которых $|G| > 1$. Два из них ($G = \{0,p\}$ и $G = \{1,p\}$) являются двойственными, третий ($G = \{0,1,p\}$) требует отдельного рассмотрения.

Пусть сначала $G = \{0,p\}$. Тогда значения $\hat{f}$ на наборах $\tilde{\beta} \in \{0,p\}^n$ также лежат в множестве $\{0,p\}$. Для набора $\tilde{\beta} \in \{0,p\}^n$ обозначим через $\tilde{\beta}^{\uparrow}$ набор из множества $\{0,1\}^n$, получающийся из набора $\tilde{\beta}$ заменой всех элементов p на единицы. Для набора $\tilde{\sigma} \in \{0,1\}^n$ через $|\tilde{\sigma}|$ будем обозначать число единиц в наборе $\tilde{\sigma}$. С использованием разложения $\hat{f}$ по переменным несложно убедиться в том, что для всех $\tilde{\beta} \in \{0,p\}^n$ выполняются равенства:

$$\hat{f}(\tilde{\beta}) = \sum_{\substack{\tilde{\sigma} \in \{0,1\}^n, \\ \tilde{\sigma} \leqslant \tilde{\beta}^{\uparrow}}} f(\tilde{\sigma}) p^{|\tilde{\sigma}|} (1-p)^{|\tilde{\beta}^{\uparrow}| - |\tilde{\sigma}|}, \tag{10}$$

где неравенство $\tilde{\sigma} \leqslant \tilde{\beta}^{\uparrow}$ понимается в смысле обычного частичного порядка на множестве $\{0,1\}^n$.

Равенства (10) можно рассматривать как систему уравнений относительно 2^n неизвестных $f(\tilde{\beta}^{\uparrow})$, $\tilde{\beta}^{\uparrow} \in \{0,1\}^n$. Расположив неизвестные

по возрастанию величины $|\tilde{\beta}^{\uparrow}|$, получим систему линейных уравнений с нижнетреугольной матрицей, у которой на диагонали стоят величины $p^{|\tilde{\beta}^{\uparrow}|}$. При $p \neq 0$ такая система имеет единственное решение для каждого набора $\hat{f}(\tilde{\beta})$, $\tilde{\beta} \in \{0, p\}^n$. Отметим, что этому решению соответствует некоторая булева функция f только в том случае, если все его компоненты равны 0 или 1. В остальных случаях соответствующей булевой функции не существует.

Введем на множестве наборов $\{0, p\}^n$ частичный порядок, положив $0 \preccurlyeq p$ и считая, что $(\alpha_1 \ldots, \alpha_n) \preccurlyeq (\beta_1, \ldots, \beta_n)$, если для всех $i = 1, \ldots, n$ выполнено $\alpha_i \preccurlyeq \beta_i$.

Покажем, что функция $\hat{f}$ на множестве наборов $\{0, p\}^n$ является монотонно возрастающей относительно введенного частичного порядка. Пусть для некоторого $\tilde{\beta} \in \{0, p\}^n$ имеет место равенство $\hat{f}(\tilde{\beta}) = 0$. Тогда из (10) получаем, что

$$0 = \sum_{\substack{\tilde{\sigma} \in \{0,1\}^n, \\ \tilde{\sigma} \leqslant \tilde{\beta}^{\uparrow}}} f(\tilde{\sigma}) p^{|\tilde{\sigma}|} (1-p)^{|\tilde{\beta}^{\uparrow}| - |\tilde{\sigma}|}. \tag{11}$$

Поскольку $p \notin \{0, 1\}$, это влечет для всех $\tilde{\sigma} \leqslant \tilde{\beta}^{\uparrow}$ равенство $f(\tilde{\sigma}) = 0$, откуда легко вытекает, что $\hat{f}(\tilde{\alpha}) = 0$ для всех $\tilde{\alpha} \preccurlyeq \tilde{\beta}$.

Если $\hat{f}(\tilde{\beta}) = p$, то для всех таких $\tilde{\alpha}$, что $\tilde{\alpha} \succcurlyeq \tilde{\beta}$ имеет место равенство $\hat{f}(\tilde{\alpha}) = p$, так как в противном случае, по ранее доказанному получалось бы, что $\hat{f}(\tilde{\beta}) = 0$. Таким образом, монотонное возрастание $\hat{f}$ на $\{0, p\}^n$ доказано.

Легко видеть, что $\hat{f}(0, \ldots, 0) = f(0, \ldots, 0) = 0$, так как $f(0, \ldots, 0) \in \in \{0, 1\}$, а $\hat{f}(0, \ldots, 0) \in \{0, p\}$. Если $\hat{f}(p, \ldots, p) = 0$, то $f \equiv 0$, что противоречит ее существенной зависимости от более чем одной переменной. Следовательно, $\hat{f}(p, \ldots, p) = p$.

Среди наборов $\tilde{\gamma} \in \{0, p\}^n$ выберем такие, что $\hat{f}(\tilde{\gamma}) = p$ и при этом для любого $\tilde{\alpha} \in \{0, p\}^n$, $\tilde{\alpha} \preccurlyeq \tilde{\gamma}$, $\tilde{\alpha} \neq \tilde{\gamma}$, выполнено $\hat{f}(\tilde{\alpha}) = 0$. Такие наборы $\tilde{\gamma}$ будем называть *нижними*.

Покажем, что нижние наборы не могут содержать более одного элемента p. Действительно, пусть некоторый нижний набор $\tilde{\gamma}$ содержит k элементов, равных p, $k \geqslant 2$. Тогда из (10) с учетом равенств $f(\tilde{\sigma}) = 0$ для всех $\tilde{\sigma} < \tilde{\gamma}^{\uparrow}$ получаем $p = \hat{f}(\tilde{\gamma}) = p^k f(\tilde{\gamma}^{\uparrow})$.

При $k \geqslant 2$ это влечет $p \in \{0, 1\}$, что противоречит определению значения p выше. Итак, $k = 1$, а кроме того, для нижнего набора $\tilde{\gamma}$ выполнено $f(\tilde{\gamma}^{\uparrow}) = 1$. Пусть для определенности имеется ровно m нижних наборов, и в них компонента p стоит на одном и первых m мест — этого всегда можно добиться, переставляя переменные функции f.

Покажем, что для каждого значения m единственная с точностью до перестановки переменных функция f, у которой $\hat{f}$ монотонно возрастает на $\{0,p\}^n$ и имеет ровно m нижних наборов, является линейной, а для функций, существенно зависящих от двух и более переменных, дополнительно выполняется равенство $p=\frac{1}{2}$.

Рассмотрим функцию $e(x_1,\ldots,x_n)=x_1$, для нее выполнено $\hat{e}(\tilde{\beta})=\beta_1$. Из этого равенства вытекает, что функция $\hat{e}$ — монотонно возрастающая на $\{0,p\}^n$ и имеет ровно один нижний набор $(p,0,\ldots,0)$. В силу единственности решения системы (10), у функции f, существенно зависящей от двух или более переменных, функция $\hat{f}$ не может иметь менее двух нижних наборов. Пусть далее $m\geqslant 2$. Рассмотрим $\hat{f}(p,p,0,\ldots,0)$:

$$p=\hat{f}(p,p,0,\ldots,0)=p^2f(1,1,0,\ldots,0)+p(1-p)f(1,0,0,\ldots,0)+\\+p(1-p)f(0,1,0,\ldots,0)+(1-p)^2f(0,\ldots,0).$$

С учетом ранее найденных значений функции f на наборах с одной единицей получаем равенство $p=p^2f(1,1,0,\ldots,0)+2p(1-p)$, которое вместе с условиями $p\notin\{0,1\}$ и $f(1,1,0,\ldots,0)\in\{0,1\}$, влечет $p=\frac{1}{2}$.

Рассмотрим функцию $g(x_1,\ldots,x_n)=x_1+\cdots+x_m \pmod 2$ и значения функции $\hat{g}$ на наборах $\tilde{\beta}\in\{0,\frac{1}{2}\}^n$. Если $\beta_1=\cdots=\beta_m=0$, то для всех $\tilde{\alpha}\in\{0,\frac{1}{2}\}^n$, $\tilde{\alpha}\preccurlyeq\tilde{\beta}$ имеет место равенство $g(\tilde{\alpha}^{\uparrow})=0$, что влечет $\hat{g}(\tilde{\beta})=0$.

Пусть среди $\beta_1,\ldots,\beta_m$ ровно t элементов равны 0, $t<m$. Тогда $\hat{g}(\tilde{\beta})$ в точности равно $\hat{g}'\left(\frac{1}{2},\ldots,\frac{1}{2}\right)$, где $g'(y_1,\ldots,y_{m-t})=y_1+\cdots+y_{m-t} \pmod 2$. Несложно видеть, что

$$\hat{g}'\left(\tfrac{1}{2},\ldots,\tfrac{1}{2}\right)=\sum_{s \bmod 2=1}\binom{m-t}{s}\left(\tfrac{1}{2}\right)^s\left(\tfrac{1}{2}\right)^{m-t-s}=\tfrac{1}{2^{m-t}}\sum_{s \bmod 2=1}\binom{m-t}{s}=\tfrac{2^{m-t-1}}{2^{m-t}}=\tfrac{1}{2}.$$

Отсюда легко следует, что функция $\hat{g}$ монотонно возрастает на $\{0,\frac{1}{2}\}^n$ и имеет в точности m нижних наборов. В силу единственности решения системы (10) получаем, что с точностью до переименования переменных выполнено $f(x_1,\ldots,x_n)=x_1+\cdots+x_m \pmod 2$. Итак, в случае $G=\{0,p\}$ доказано, что $f\in L$ и $p=\frac{1}{2}$.

Пусть теперь $G=\{1,p\}$. Тогда рассмотрим множество $G^*=\{0,1-p\}$ и функцию f^*, двойственную функции f. В силу леммы 1 получаем, что $\langle G^*,f^*\rangle$ — также конечная алгебра. По доказанному выше $f^*\in L$ и $1-p=\frac{1}{2}$, откуда следует, что $f\in L$ и $p=\frac{1}{2}$.

Наконец перейдем к случаю $G=\{0,1,p\}$. Пусть $f\in B$, тогда $\langle G,\hat{f}\rangle$ — конечная алгебра. Рассмотрим значения функции $\hat{f}$ на наборах $\tilde{\beta}\in\{0,p\}^n$. Равенства (10) сохраняются, однако $\hat{f}(\tilde{\beta})$ может принимать значения из множества $\{0,1,p\}$. Если для какого-то набора $\tilde{\beta}$ выполнено

$\hat{f}(\tilde{\beta}) = c \in \{0,1\}$, то из равенств (10) вытекает, что подфункция f' функции f, определенная на всех таких наборах $\tilde{\sigma}$, что $\tilde{\sigma} \leqslant \tilde{\beta}^{\uparrow}$, удовлетворяет равенству $\hat{f}'(p,\ldots,p) = c \in \{0,1\}$. Из леммы 2 вытекает, что тогда $f' \equiv c$ и, в частности, $f'(0,\ldots,0) = c$. В силу определения f' также имеет место $f(0,\ldots,0) = c$.

Поскольку из равенства $\hat{f}(\tilde{\beta}) = c \in \{0,1\}$ для произвольного набора $\tilde{\beta}$ вытекает, что $f(0,\ldots,0) = c = \hat{f}(\tilde{\beta})$, получаем, что значения $\hat{f}(\tilde{\beta})$ для всех $\tilde{\beta} \in \{0,p\}^n$ лежат в множестве $\{f(0,\ldots,0),p\}$, т. е. либо в множестве $\{0,p\}$, либо в множестве $\{1,p\}$. В первом случае утверждение теоремы вытекает из ранее доказанного. Пусть далее $\hat{f}(\tilde{\beta}) \in \{1,p\}$ при $\tilde{\beta} \in \{0,p\}^n$.

Рассмотрим теперь для той же функции f значения $\hat{f}$ на множестве $\{1,p\}^n$. Если для какого-то набора $\tilde{\omega} \in \{1,p\}^n$ выполнено $\hat{f}(\tilde{\omega}) = c \in \{0,1\}$, то из равенств (10) и леммы 2 аналогично описанному выше вытекает, что $f(1,\ldots,1) = c$. Таким образом, все значения $\hat{f}$ лежат либо в $\{1,p\}$, либо в $\{0,p\}$. В первом случае утверждение теоремы вытекает из ранее доказанного. Далее считаем, что $\hat{f}(\tilde{\omega}) \in \{0,p\}$ при $\tilde{\omega} \in \{1,p\}^n$.

На множестве $\{0,p\}^n$ воспользуемся ранее введенным частичным порядком, используя при этом для значений функции $\hat{f}$ упорядочение[1] $1 \preccurlyeq p$. На множестве $\{1,p\}^n$ введем частичный порядок, используя для компонент наборов из $\{1,p\}^n$ упорядочение $p \preccurlyeq 1$, а для значений функции $\hat{f}$ на множестве $\{1,p\}^n$ — упорядочение $p \preccurlyeq 0$. При таких определениях функция $\hat{f}$ оказывается монотонно возрастающей на каждом из множеств $\{0,p\}^n$, $\{1,p\}^n$.

Будем называть набор $\tilde{\gamma} \in \{0,p\}^n$ *нижним*, если $\hat{f}(\tilde{\gamma}) = p$ и для любых $\tilde{\alpha} \in \{0,p\}^n$, $\tilde{\alpha} \preccurlyeq \tilde{\gamma}$, $\tilde{\alpha} \neq \tilde{\gamma}$ выполнено $\hat{f}(\tilde{\alpha}) = 1$.

Будем называть набор $\tilde{\zeta} \in \{1,p\}^n$ *верхним*, если $\hat{f}(\tilde{\zeta}) = p$ и для любых $\tilde{\chi} \in \{1,p\}^n$, $\tilde{\chi} \succcurlyeq \tilde{\zeta}$, $\tilde{\chi} \neq \tilde{\zeta}$ выполнено $\hat{f}(\tilde{\chi}) = 0$.

Для наборов $\tilde{\omega} \in \{1,p\}^n$ будем обозначать через $\tilde{\omega}^{\downarrow}$ набор из $\{0,1\}^n$, получающийся из $\tilde{\omega}$ заменой всех компонент p на нули.

Пусть $\tilde{\gamma} \in \{0,p\}^n$ — нижний набор и $\tilde{\zeta} \in \{1,p\}^n$ — верхний набор для функции $\hat{f}$ на соответствующих множествах. Тогда для этих наборов равенства (10) имеют вид:

$$p = \hat{f}(\tilde{\gamma}) = p^{|\tilde{\gamma}^{\uparrow}|} f(\tilde{\gamma}^{\uparrow}) + 1 - p^{|\tilde{\gamma}^{\uparrow}|}$$
$$p = \hat{f}(\tilde{\zeta}) = (1-p)^{n-|\tilde{\zeta}^{\downarrow}|} f(\tilde{\zeta}^{\downarrow})$$

[1]Для всех вводимых частичных порядков используем один и тот же символ $\preccurlyeq$, предполагая, что, поскольку они вводятся на разных множествах, в каждом случае понятно, о каком именно порядке идет речь.

Если $f(\tilde{\gamma}^{\uparrow}) = 1$, то из первого равенства следует, что $p = 1$. Аналогично, второе равенство превращается в $p = 0$ в случае $f(\tilde{\zeta}^{\downarrow}) = 0$. Поскольку $p \notin \{0, 1\}$, получаем, что должны выполняться равенства $p = 1 - p^{|\tilde{\gamma}^{\uparrow}|}$ и $p = (1-p)^{n-|\tilde{\zeta}^{\downarrow}|}$. Объединяя их, получаем условие $1 - p^{|\tilde{\gamma}^{\uparrow}|} = (1-p)^{n-|\tilde{\zeta}^{\downarrow}|}$.

Легко видеть, что $1 - p^{|\tilde{\gamma}^{\uparrow}|} \geqslant 1 - p \geqslant (1-p)^{n-|\tilde{\zeta}^{\downarrow}|}$. При этом для $p \notin \{0, 1\}$ равенства возможны только в случае $|\tilde{\gamma}^{\uparrow}| = 1$ (а также $|\tilde{\zeta}^{\downarrow}| = n - 1$, но для дальнейших рассуждений это несущественно).

Таким образом показано, что нижние наборы в $\{0, p\}^n$ обязательно содержат ровно одну компоненту, равную p. Равенство $p = 1 - p^{|\tilde{\gamma}^{\uparrow}|}$ при этом превращается в $p = 1 - p$, что естественно влечет $p = \frac{1}{2}$.

Аналогично ранее доказанному можно показать, что функция $\hat{g}$, индуцированная функцией $g(x_1, \ldots, x_n) = x_1 + \cdots + x_m + 1 \pmod 2$, монотонно возрастает на наборах из $\{0, \frac{1}{2}\}^n$, равна 1 на наборе $(0, \ldots, 0)$ и имеет в точности m нижних наборов $\tilde{\gamma}$ (с одной компонентой $\frac{1}{2}$ и остальными нулями), для которых $\hat{g}(\tilde{\gamma}) = \frac{1}{2}$. В силу единственности решения системы (10), получаем, что функция f с точностью до перестановки переменных совпадает с функцией g, а следовательно $f \in L$. Теорема доказана. □

Описание конечных алгебр распределений

Объединение доказанных выше утверждений позволяет сформулировать следующую теорему.

Теорема 3. *Пусть $\langle G, \hat{B} \rangle$ — конечная алгебра бернуллиевских случайных величин, индуцированная множеством булевых функций B. Тогда имеет место по крайней мере одно из следующих утверждений:*

1. $G \subseteq \{0, 1\}$;
2. *B не содержит функций, существенно зависящих от двух или более переменных;*
3. $G = \{p\}$, $p \notin \{0, 1\}$ — *алгебраическое число;*
4. $G \subseteq \{0, 1, \frac{1}{2}\}$, $B \subseteq L$.

Автор выражает глубокую признательность профессору О. М. Касим-Заде за внимание к данной работе.

Список литературы

[1] Бухараев Р. Г. Об управляемых генераторах случайных величин // Вероятностные методы и кибернетика. II, Сборник работ НИИММ им. Н. Г. Чеботарева при Казанском университете, Учен. зап. Казан. ун-та., 123, № 6, ред. Р. Г. Бухараев, Изд-во Казанского ун-та, Казань, 1963. С. 68–87.

[2] Колпаков Р. М. Критерий порождения множеств рациональных вероятностей в классе булевых функций // Дискретный анализ и исследование операций. 1999. Т. 6, № 2. С. 41–61.

[3] Салимов Ф. И. Об одной системе образующих для алгебр над случайными величинами // Изв. вузов. Матем., 1981, № 5. С. 78–82.

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

[5] Феллер В. Введение в теорию вероятностей и ее приложения. Мир, Москва, 1984.

[6] Яшунский А. Д. О вероятностях значений случайных булевых выражений: дис.. . . канд.физ.-мат. наук. МГУ имени М. В. Ломоносова. Москва, 2006.

[7] Яшунский А. Д. О преобразованиях распределений вероятностей бесповторными квазигрупповыми формулами // Дискретная математика. 2013. Т. 25, № 2. С. 149–159.

[8] Lindqvist B. Ergodic Markov chains with finite convergence time // Stochastic Processes and their Applications. 1981. V. 11. Pp. 91–99.