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

Препринты ИПМ • Препринт № 84 за 2018 г.

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

Яшунский А.Д.

О подалгебрах вероятностных распределений над конечными кольцами

Рекомендуемая форма библиографической ссылки: Яшунский А.Д. О подалгебрах вероятностных распределений над конечными кольцами // Препринты ИПМ им. М.В.Келдыша. 2018. № 84. 14 с. doi:10.20948/prepr-2018-84
URL: http://library.keldysh.ru/preprint.asp?id=2018-84

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

А. Д. Яшунский

О подалгебрах вероятностных распределений над конечными кольцами

Москва — 2018

Яшунский А. Д.

О подалгебрах вероятностных распределений над конечными кольцами

В работе рассматриваются преобразования случайных величин над конечным кольцом операциями сложения и умножения. Для произвольных конечных колец строятся семейства подалгебр распределений — множеств распределений, замкнутых относительно взятия сумм и произведений независимых случайных величин.

Ключевые слова: случайная величина, конечное кольцо, дискретное распределение вероятностей, подалгебра

Alexey Dmitrievich Yashunsky

On subalgebras of probability distributions over finite rings

We consider the transformations of random variables over a finite ring by the addition and multiplication operations. For arbitrary finite rings we construct families of distribution subalgebras — sets of distributions that are closed under taking sums and products of independent random variables.

Key words: random variable, finite ring, discrete probability distribution, subalgebra

Работа подготовлена при поддержке программы Президиума РАН №01 «Фундаментальная математика и ее приложения» (грант PRAS-18-01).

Оглавление

Введение

В задачах о преобразованиях случайных величин дискретными функциями вопросы о выразимости случайных величин, т. е. о возможности получения случайной величины с заданным распределением, естественным образом сводятся к исследованию подалгебр распределений. В частности, Р. М. Колпаков в работе [1] описал все множества распределений с рациональными компонентами, замкнутые относительно преобразований случайных величин произвольными функциями k-значной логики.

Для более слабых систем преобразующих функций, а также для произвольных (не обязательно рациональных) распределений к настоящему моменту построены некоторые семейства подалгебр распределений, однако целиком вся решетка подалгебр распределений не описана. Данная работа обобщает результаты, полученные в [3] для подалгебр над конечными полями, на случай конечных колец.

Определение и свойства алгебр распределений

Пусть $E_k = \{0, 1, \ldots, k-1\}$, X — случайная величина со значениями в множестве E_k. Распределение случайной величины X есть вектор $\mathbf{p} = (p_0, \ldots, p_{k-1})$, компоненты которого удовлетворяют условиям $\sum p_i = 1$ и $p_i \geqslant 0, i = 0, \ldots, k-1$. Такие вектора будем называть *стохастическими*, они образуют в $\mathbb{R}^k$ симплекс, который будем обозначать $\mathbf{S}^{(k)}$. Введем специальные обозначения для некоторых векторов из $\mathbf{S}^{(k)}$: $\mathbf{e}^0 = (1, 0, \ldots, 0)$, $\mathbf{e}^1 = (0, 1, 0 \ldots, 0)$, $\ldots$, $\mathbf{e}^{k-1} = (0, \ldots, 0, 1)$.

Пусть $P_k(n) = \{f \mid f : E_k^n \to E_k\}$ — множество n-местных функций на E_k и $P_k = \bigcup\limits_{n=0}^{\infty} P_k(n)$. Пусть $B \subseteq P_k$, тогда $\langle E_k, B\rangle$ — некоторая конечная алгебра. Если $f(x_1, \ldots, x_n) \in B$ и $X_1, \ldots, X_n$ — независимые в совокупности случайные величины со значениями в E_k с распределениями $\mathbf{p}^1, \ldots, \mathbf{p}^n \in \mathbf{S}^{(k)}$ соответственно, то $f(X_1, \ldots, X_n)$ есть также случайная величина со значениями в E_k и для компонент ее распределения $\mathbf{q} = (q_0, \ldots, q_{k-1}) \in \mathbf{S}^{(k)}$ выполнено равенство

$$q_i = \sum_{\substack{(\sigma_1,\ldots,\sigma_n):\\ f(\sigma_1,\ldots,\sigma_n)=i}} p^1_{\sigma_1} \cdots p^n_{\sigma_n}.$$

Таким образом, каждая n-арная операция $f \in B$ индуцирует полилинейное отображение $\hat{f} : (\mathbf{S}^{(k)})^n \to \mathbf{S}^{(k)}$. Далее будем использовать также

обозначение $(\hat{f}(\mathbf{p}^1,\dots,\mathbf{p}^n))_i$ для i-й компоненты распределения $\mathbf{q}$. Используя это обозначение, равенства выше можно переписать в виде

$$(\hat{f}(\mathbf{p}^1,\dots,\mathbf{p}^n))_i = \sum_{\substack{(\sigma_1,\dots,\sigma_n):\\ f(\sigma_1,\dots,\sigma_n)=i}} p^1_{\sigma_1}\cdots p^n_{\sigma_n}. \tag{1}$$

Обозначим $\hat{B} = \{\hat{f} \mid f \in B\}$, тогда $\langle \mathbf{S}^{(k)}, \hat{B}\rangle$ есть *алгебра (вероятностных) распределений, индуцированная алгеброй* $\langle E_k, B\rangle$. Подалгебры этой алгебры будем также называть алгебрами распределений. Подалгебры зависят от индуцирующей системы операций B, однако есть подалгебра, возникающая при любой системе операций.

Лемма 1. $\langle\{\mathbf{e}^0,\dots,\mathbf{e}^{k-1}\}, \hat{B}\rangle$ *— подалгебра, изоморфная алгебре* $\langle E_k, B\rangle$.

Доказательство. Искомый изоморфизм сопоставляет значению $i \in E_k$ вектор $\mathbf{e}^i$. Доказательство леммы сводится к простой проверке с использованием соотношений (1). □

Отметим, что множество стохастических векторов $\mathbf{S}^{(k)}$ является подмножеством в $\mathbb{R}^k$, поэтому для стохастических векторов $\mathbf{p}$ и $\mathbf{q}$ определены линейные комбинации $\alpha\mathbf{p}+\beta\mathbf{q}$, где $\alpha,\beta\in\mathbb{R}$, $\alpha\mathbf{p}$ и $\beta\mathbf{q}$ понимаются как умножение вектора на число, а операция $+$ понимается как обычное сложение векторов из $\mathbb{R}^k$. Такая линейная комбинация, вообще говоря, не обязательно лежит в $\mathbf{S}^{(k)}$, однако некоторые линейные комбинации стохастических векторов также оказываются стохастическими.

Напомним, что множество $H \subseteq \mathbf{S}^{(k)}$ называется *выпуклым*, если для любого $0 \leqslant \alpha \leqslant 1$ и любых $\mathbf{p},\mathbf{q} \in H$ выполнено $\alpha\mathbf{p} + (1-\alpha)\mathbf{q} \in H$. Из определения выпуклого множества легко выводится следующее свойство.

Лемма 2. *Пусть* $H \subseteq \mathbf{S}^{(k)}$ *— выпуклое множество,* $\mathbf{h}^0,\dots,\mathbf{h}^{t-1} \in H$ *и* $\boldsymbol{\alpha} \in \mathbf{S}^{(t)}$. *Тогда* $\sum\limits_{i=0}^{t-1} \alpha_i\mathbf{h}^i \in H$.

Распределение $\sum\limits_{i=0}^{t-1} \alpha_i\mathbf{h}^i$, фигурирующее в формулировке леммы 2, называется *выпуклой комбинацией* распределений $\mathbf{h}^0,\dots,\mathbf{h}^{t-1}$. Наименьшее по включению выпуклое множество, содержащее всевозможные выпуклые комбинации векторов из заданного множества H, называется *выпуклой оболочкой* множества H и обозначается $Conv(H)$.

Заметим, что $\mathbf{S}^{(k)} = Conv(\mathbf{e}^0, \ldots, \mathbf{e}^{k-1})$ и любое распределение $\mathbf{h} \in \mathbf{S}^{(k)}$ есть выпуклая комбинация распределений $\mathbf{e}^0, \ldots, \mathbf{e}^{k-1}$:

$$\mathbf{h} = \sum_{i=0}^{k-1} h_i \mathbf{e}^i. \tag{2}$$

В силу отмечавшейся выше полилинейности индуцированных функций имеет место следующая лемма, проверяемая непосредственно по соотношениям (1).

Лемма 3. *Пусть заданы* $f(x_1, \ldots, x_n) \in P_k$, $\boldsymbol{\alpha} \in \mathbf{S}^{(t)}$, $\mathbf{h}^0, \ldots, \mathbf{h}^{t-1} \in \mathbf{S}^{(k)}$ *и* $\mathbf{g}^2, \ldots, \mathbf{g}^n \in \mathbf{S}^{(k)}$. *Тогда* $\hat{f}(\sum\limits_{i=0}^{t-1} \alpha_i \mathbf{h}^i, \mathbf{g}^2, \ldots, \mathbf{g}^n) = \sum\limits_{i=0}^{t-1} \alpha_i \hat{f}(\mathbf{h}^i, \mathbf{g}^2, \ldots, \mathbf{g}^n)$.

Из леммы 3 и определения выпуклого множества вытекает следующее утверждение.

Лемма 4. *Пусть* $H \subseteq \mathbf{S}^{(k)}$ *— выпуклое множество,* $\mathbf{h}^{ij} \in H$ *при всех* $i = 1, \ldots, n$, $j \in E_{t_i - 1}$, $f(x_1, \ldots, x_n) \in P_k$, *и для любых* $j_1, \ldots, j_n$ *имеет место* $\hat{f}(\mathbf{h}^{1j_1}, \ldots, \mathbf{h}^{nj_n}) \in H$. *Тогда для любых* $\boldsymbol{\alpha}^i \in \mathbf{S}^{(t_i)}$ *выполнено*

$$\hat{f}\left(\sum_{j=0}^{t_1-1} \alpha_j^1 \mathbf{h}^{1j}, \ldots, \sum_{j=0}^{t_n-1} \alpha_j^n \mathbf{h}^{nj}\right) \in H.$$

Терм (формула) в алгебре $\langle E_k, B \rangle$, составленный из символов переменных и символов операций из множества B, задает некоторую функцию f из P_k. Будем называть терм *бесповторным* (также используется термин *линейный*), если каждая переменная входит в него не более одного раза. Для функций, индуцированных бесповторными термами, выполнено следующее утверждение.

Лемма 5. *Пусть функция* f *задана бесповторным термом*

$$f(x_{11}, \ldots, x_{mn_m}) = g(g_1(x_{11}, \ldots, x_{1n_1}), \ldots, g_m(x_{m1}, \ldots, x_{mn_m})),$$

где $g, g_1, \ldots, g_m \in P_k$. *Тогда* $\hat{f} = \hat{g}(\widehat{g_1}(\mathbf{p}^{11}, \ldots, \mathbf{p}^{1n_1}), \ldots, \widehat{g_m}(\mathbf{p}^{m1}, \ldots, \mathbf{p}^{mn_m}))$.

Доказательство. Воспользуемся соотношениями (1). Для $i \in E_k$ выпол-

нено:

$$(\hat{f}(\mathbf{p}^{11},\dots,\mathbf{p}^{mn_m}))_i = \sum_{\substack{(\sigma_{11},\dots,\sigma_{mn_m}):\\ f(\sigma_{11},\dots,\sigma_{mn_m})=i}} p^{11}_{\sigma_{11}}\cdots p^{mn_m}_{\sigma_{mnm}} =$$

$$= \sum_{\substack{(\sigma_{11},\dots,\sigma_{mnm}):\\ g(g_1(\sigma_{11},\dots,\sigma_{1n_1}),\dots,g_m(\sigma_{m1},\dots,\sigma_{mnm}))=i}} (p^{11}_{\sigma_{11}}\cdots p^{1n_1}_{\sigma_{1n_1}})\cdots(p^{m1}_{\sigma_{m1}}\cdots p^{mn_m}_{\sigma_{mnm}}) =$$

$$= \sum_{\substack{(\tau_1,\dots,\tau_m):\\ g(\tau_1,\dots,\tau_m)=i}} \sum_{\substack{(\sigma_{11},\dots,\sigma_{1n_1}):\\ g_1(\sigma_{11},\dots,\sigma_{1n_1})=\tau_1}} \cdots \sum_{\substack{(\sigma_{m1},\dots,\sigma_{mn_m}):\\ g_m(\sigma_{m1},\dots,\sigma_{mn_m})=\tau_m}} (p^{11}_{\sigma_{11}}\cdots p^{1n_1}_{\sigma_{1n_1}})\cdots(p^{m1}_{\sigma_{m1}}\cdots p^{mn_m}_{\sigma_{mnm}}) =$$

$$= \sum_{\substack{(\tau_1,\dots,\tau_m):\\ g(\tau_1,\dots,\tau_m)=i}} \left(\sum_{\substack{(\sigma_{11},\dots,\sigma_{1n_1}):\\ g_1(\sigma_{11},\dots,\sigma_{1n_1})=\tau_1}} p^{11}_{\sigma_{11}}\cdots p^{1n_1}_{\sigma_{1n_1}} \right) \cdots \left(\sum_{\substack{(\sigma_{m1},\dots,\sigma_{mn_m}):\\ g_m(\sigma_{m1},\dots,\sigma_{mn_m})=\tau_m}} p^{m1}_{\sigma_{m1}}\cdots p^{mn_m}_{\sigma_{mnm}} \right).$$

Каждая из сумм в скобках является правой частью равенства (1) для соответствующей функции g_j, с учетом чего приходим к равенству:

$$(\hat{f}(\mathbf{p}^{11},\dots,\mathbf{p}^{mn_m}))_i = \sum_{\substack{(\tau_1,\dots,\tau_m):\\ g(\tau_1,\dots,\tau_m)=i}} (\widehat{g_1}(\mathbf{p}^{11},\dots,\mathbf{p}^{1n_1}))_{\tau_1}\cdots(\widehat{g_m}(\mathbf{p}^{m1},\dots,\mathbf{p}^{mn_m}))_{\tau_m}.$$

Применяя равенство (1) к правой части полученного соотношения, выводим соотношение

$$(\hat{f}(\mathbf{p}^{11},\dots,\mathbf{p}^{mn_m}))_i = (\widehat{g}(\widehat{g_1}(\mathbf{p}^{11},\dots,\mathbf{p}^{1n_1}),\dots,\widehat{g_m}(\mathbf{p}^{m1},\dots,\mathbf{p}^{mn_m})))_i,$$

которое и составляет утверждение леммы. □

Таким образом, отображение, индуцированное бесповторным термом в алгебре $\langle E_k, B\rangle$, задается в алгебре $\langle \mathbf{S}^{(k)}, \hat{B}\rangle$ термом, который получается в результате формальной замены в исходном терме всех символов функций на индуцированные, а переменных — на переменные распределения. Терм, получающийся в результате такой замены в терме φ, будем обозначать $\hat{\varphi}$. Отметим, что, хотя формальная замена возможна в произвольном терме алгебры $\langle E_k, B\rangle$, терм $\hat{\varphi}$ действительно будет задавать функцию $\hat{f}$, индуцированную функцией f, задаваемой термом φ, только в случае бесповторного терма φ.

Свойства бесповторных термов позволяют доказать следующее утверждение.

Лемма 6. *Пусть φ, ψ — бесповторные термы в алгебре $\langle E_k, B\rangle$ и выполнено тождество $\varphi = \psi$. Тогда в алгебре $\langle \mathbf{S}^{(k)}, \hat{B}\rangle$ выполнено тождество $\hat{\varphi} = \hat{\psi}$.*

Доказательство. Пусть термы φ, ψ содержат переменные из множества $x_1, \ldots, x_n$. Пусть $X_1, \ldots, X_n$ — независимые в совокупности случайные величины с заданными произвольными распределениями.

Поскольку выполнено тождество $\varphi = \psi$, случайные величины, получающиеся при подстановке $X_1, \ldots, X_n$ вместо переменных в термах φ и ψ, совпадают. В частности, их распределения совпадают, откуда получаем, что значения термов $\hat{\varphi}$ и $\hat{\psi}$ совпадают на распределениях случайных величин $X_1, \ldots, X_n$. В силу произвольности этих распределений, имеет место тождество $\hat{\varphi} = \hat{\psi}$. Лемма доказана. □

Алгебры распределений над кольцами

Напомним, что конечная алгебра $\langle E_k; +, \times\rangle$ с бинарными операциями $+$ и $\times$ называется *кольцом*, если $\langle E_k, +\rangle$ — абелева группа, и имеет место дистрибутивность операции $\times$ относительно операции $+$ (см. [2]). Иначе говоря, в кольце выполнены следующие тождества:

$$\begin{aligned} x + y &= y + x, \\ x + (y + z) &= (x + y) + z, \\ x \times (y + z) &= (x \times y) + (x \times z), \\ (x + y) \times z &= (x \times z) + (y \times z). \end{aligned}$$

Будем считать, что $0 \in E_k$ — нейтральный элемент группы $\langle E_k, +\rangle$. Тогда еще одно тождество записывается как $0 + x = x$. Отметим, что тождества $0 \times x = x \times 0 = 0$ также имеют место и являются непосредственными следствиями дистрибутивности и тождества $0 + x = x$.

Наконец, кольцо называется *ассоциативным*, если дополнительно выполняется тождество

$$x \times (y \times z) = (x \times y) \times z.$$

Далее везде рассматривается ассоциативное кольцо $\langle E_k; +, \times\rangle$. Пусть $\langle \mathbf{S}^{(k)}; \oplus, \otimes\rangle$ — индуцированная этим кольцом алгебра распределений[1].

[1]На распределениях из $\mathbf{S}^{(k)}$ таким образом определена операция $\oplus$, индуцированная операцией $+$ конечного кольца, определенной на множестве E_k. Вместе с тем, для выпуклых комбинаций распределений мы продолжим использовать запись $\sum \alpha_i \mathbf{h}^i$, в которой, фактически, фигурирует операция суммирования векторов из $\mathbb{R}^k$. Мы предполагаем, что везде из контекста понятно, о какой операции суммирования идет речь.

Тогда в силу леммы 6 некоторые из тождеств кольца переносятся на алгебру распределений. В частности, операции $\oplus$ и $\otimes$ — ассоциативны, а операция $\oplus$ — еще и коммутативна. Иначе говоря, для любых распределений $\mathbf{g}, \mathbf{h}, \mathbf{j} \in \mathbf{S}^{(k)}$ выполнено:

$$\begin{aligned} \mathbf{h} \oplus \mathbf{g} &= \mathbf{g} \oplus \mathbf{h}, \\ \mathbf{g} \oplus (\mathbf{h} \oplus \mathbf{j}) &= (\mathbf{g} \oplus \mathbf{h}) \oplus \mathbf{j}, \\ \mathbf{g} \otimes (\mathbf{h} \otimes \mathbf{j}) &= (\mathbf{g} \otimes \mathbf{h}) \otimes \mathbf{j}. \end{aligned}$$

Аналогично для любого распределения $\mathbf{g}$ имеет место $\mathbf{e}^0 \oplus \mathbf{g} = \mathbf{g} \oplus \mathbf{e}^0 = \mathbf{g}$. Дистрибутивность операции $\otimes$ относительно $\oplus$, вообще говоря, не имеет места, так как правая часть тождеств для дистрибутивности не является бесповторной. Более того, можно явно продемонстрировать, что в алгебре распределений соответствующие тождества *не* выполняются. Однако имеет место более слабый вариант дистрибутивности, а именно — дистрибутивность относительно умножения на распределения $\mathbf{e}^0, \ldots, \mathbf{e}^{k-1}$. Покажем это.

Пусть $i \in E_k$, определим одноместную функцию $\mu_i(x) = i \times x$. Легко видеть, что при этом $\widehat{\mu}_i(\mathbf{g}) = \mathbf{e}^i \otimes \mathbf{g}$. В силу дистрибутивности умножения имеет место тождество $\mu_i(x+y) = \mu_i(x) + \mu_i(y)$, которое по лемме 6 влечет тождество

$$\widehat{\mu}_i(\mathbf{h} \oplus \mathbf{g}) = \widehat{\mu}_i(\mathbf{h}) \oplus \widehat{\mu}_i(\mathbf{g}). \tag{3}$$

Пусть задано множество $M \subseteq E_k$, содержащее m элементов, и конечное множество распределений $\mathbf{g}^1, \ldots, \mathbf{g}^t \in \mathbf{S}^{(k)}$. Введем следующие множества распределений:

$$K_{ij} = \{\mathbf{e}^j \otimes (\mathbf{g}^i \oplus \mathbf{e}^s) \mid s \in E_k\} \cup \{\mathbf{e}^0\},\ i = 1, \ldots, t, j \in M, \tag{4}$$

$$K_i = \{\mathbf{h}^{ij_1} \oplus \cdots \oplus \mathbf{h}^{i\,j_m} \mid \{j_1, \ldots, j_m\} = M, \mathbf{h}^{ij_r} \in K_{ij_r}\},\ i = 1, \ldots, t, \tag{5}$$

$$K = \{\mathbf{j}^1 \oplus \cdots \oplus \mathbf{j}^t \mid \mathbf{j}^1 \in K_1, \ldots, \mathbf{j}^t \in K_t\}. \tag{6}$$

Далее будем обозначать множество $Conv(K)$, построенное по заданному множеству M и распределениям $\mathbf{g}^1, \ldots, \mathbf{g}^t$ согласно (4)–(6), через $A(\mathbf{g}^1, \ldots, \mathbf{g}^t; M)$.

Лемма 7. *Пусть* $H = A(\mathbf{g}^1, \ldots, \mathbf{g}^t; M)$*, тогда для любых* $\mathbf{a}, \mathbf{b} \in H$ *выполнено* $\mathbf{a} \oplus \mathbf{b} \in H$.

Доказательство. В силу леммы 4 достаточно доказать утверждение для $\mathbf{a}, \mathbf{b} \in K$, где K — множество, определяемое соотношениями (4)–(6).

Рассмотрим $\mathbf{a} \oplus \mathbf{b}$. Поскольку $\mathbf{a}, \mathbf{b} \in K$, их можно представить в виде:

$$\begin{aligned} \mathbf{a} &= (\mathbf{a}^{1j_1} \oplus \cdots \oplus \mathbf{a}^{1\,j_m}) \oplus \cdots \oplus (\mathbf{a}^{tj_1} \oplus \cdots \oplus \mathbf{a}^{t\,j_m}), \\ \mathbf{b} &= (\mathbf{b}^{1j_1} \oplus \cdots \oplus \mathbf{b}^{1\,j_m}) \oplus \cdots \oplus (\mathbf{b}^{tj_1} \oplus \cdots \oplus \mathbf{b}^{t\,j_m}), \end{aligned}$$

где $\mathbf{a}^{ij}, \mathbf{b}^{ij} \in K_{ij}$ для $i = 1, \ldots, t$, $j \in M$.

Заметим, что $\mathbf{e}^0 \in K_{ij}$ при всех i и j, поэтому для некоторых пар i, j возможно, что $\{\mathbf{a}^{ij}, \mathbf{b}^{ij}\} \ni \mathbf{e}^0$. Поскольку $\mathbf{a}^{ij} \oplus \mathbf{e}^0 = \mathbf{a}^{ij}$ и $\mathbf{e}^0 \oplus \mathbf{b}^{ij} = \mathbf{b}^{ij}$, сумма $\mathbf{a}^{ij} \oplus \mathbf{b}^{ij}$ также лежит в множестве $\{\mathbf{a}^{ij}, \mathbf{b}^{ij}\}$.

Если при всех i и j выполнено $\mathbf{a}^{ij} \oplus \mathbf{b}^{ij} = \mathbf{c}^{ij} \in \{\mathbf{a}^{ij}, \mathbf{b}^{ij}\} \subseteq K_{ij}$, то

$$\mathbf{a} \oplus \mathbf{b} = (\mathbf{c}^{1 j_1} \oplus \cdots \oplus \mathbf{c}^{1 j_m}) \oplus \cdots \oplus (\mathbf{c}^{t j_1} \oplus \cdots \oplus \mathbf{c}^{t j_m}),$$

и $\mathbf{a} \oplus \mathbf{b} \in K$ по определению множества K.

Пусть r — количество пар $\{\mathbf{a}^{ij}, \mathbf{b}^{ij}\} \not\ni \mathbf{e}^0$. Покажем индукцией по r, что $\mathbf{a} \oplus \mathbf{b} \in Conv(K)$. Для $r = 0$ выше показано, что $\mathbf{a} \oplus \mathbf{b} \in K \subseteq Conv(K)$. Пусть утверждение доказано для $r = R$, докажем его для $r = R + 1$.

Представим $\mathbf{a}$ и $\mathbf{b}$ в виде $\mathbf{a}' \oplus \mathbf{a}^{ij}$ и $\mathbf{b}' \oplus \mathbf{b}^{ij}$ соответственно, где $\{\mathbf{a}^{ij}, \mathbf{b}^{ij}\} \not\ni \mathbf{e}^0$. По определению имеем, что $\mathbf{b}^{ij} = \mathbf{e}^j \otimes (\mathbf{g}^i \oplus \mathbf{e}^s)$ для некоторого $s \in E_k$. Положим $\mathbf{c} = \mathbf{g}^i \oplus \mathbf{e}^s$, тогда с учетом соотношения (2), используя обозначение μ_j, можно записать $\mathbf{b}^{ij} = \widehat{\mu_j}\left(\sum\limits_{l=0}^{k-1} c_l \mathbf{e}^l\right)$. При этом также выполнено $\mathbf{a}^{ij} = \widehat{\mu_j}(\mathbf{g}^i \oplus \mathbf{e}^r)$ для некоторого $r \in E_k$.

Принимая во внимание (3), преобразуем сумму:

$$\mathbf{a}^{ij} \oplus \mathbf{b}^{ij} = \widehat{\mu_j}(\mathbf{g}^i \oplus \mathbf{e}^r) \oplus \widehat{\mu_j}\left(\sum_{l=0}^{k-1} c_l \mathbf{e}^l\right) = \widehat{\mu_j}\left((\mathbf{g}^i \oplus \mathbf{e}^r) \oplus \sum_{l=0}^{k-1} c_l \mathbf{e}^l\right).$$

Затем, дважды используя лемму 3, получаем:

$$\mathbf{a}^{ij} \oplus \mathbf{b}^{ij} = \widehat{\mu_j}\left((\mathbf{g}^i \oplus \mathbf{e}^r) \oplus \sum_{l=0}^{k-1} c_l \mathbf{e}^l\right) = \widehat{\mu_j}\left(\sum_{l=0}^{k-1} c_l (\mathbf{g}^i \oplus \mathbf{e}^r \oplus \mathbf{e}^l)\right) = \\ = \sum_{l=0}^{k-1} c_l \widehat{\mu_j}(\mathbf{g}^i \oplus \mathbf{e}^r \oplus \mathbf{e}^l).$$

В результате сумма $\mathbf{a} \oplus \mathbf{b}$, также с использованием леммы 3, может быть переписана в виде:

$$\mathbf{a} \oplus \mathbf{b} = \mathbf{a}' \oplus \mathbf{a}^{ij} \oplus \mathbf{b}' \oplus \mathbf{b}^{ij} = \mathbf{a}' \oplus \mathbf{b}' \oplus \sum_{l=0}^{k-1} c_l \widehat{\mu_j}(\mathbf{g}^i \oplus \mathbf{e}^m \oplus \mathbf{e}^l) = \\ = \sum_{l=0}^{k-1} c_l (\mathbf{a}' \oplus \mathbf{b}' \oplus \widehat{\mu_j}(\mathbf{g}^i \oplus \mathbf{e}^m \oplus \mathbf{e}^l)).$$

Обозначим $\mathbf{d}^{ijl} = \widehat{\mu_j}(\mathbf{g}^i \oplus \mathbf{e}^m \oplus \mathbf{e}^l) = \mathbf{e}^j \otimes (\mathbf{g}^i \oplus (\mathbf{e}^m \oplus \mathbf{e}^l))$. Тогда в силу леммы 1, $\mathbf{d}^{ijl} \in K_{ij}$. Заметим, что в «суммах», обозначенных $\mathbf{a}'$ и $\mathbf{b}'$,

нет «слагаемых» из множества K_{ij}, поэтому к каждому выражению $\mathbf{a}' \oplus \mathbf{b}' \oplus \mathbf{d}^{ijl}$ применимо предположение индукции. Тогда при всех l выполнено $\mathbf{a}' \oplus \mathbf{b}' \oplus \mathbf{d}^{ijl} \in Conv(K)$, а следовательно, в силу леммы 2 имеет место соотношение $\mathbf{a} \oplus \mathbf{b} = \sum\limits_{l=0}^{k-1} c_l(\mathbf{a}' \oplus \mathbf{b}' \oplus \mathbf{d}^{ijl}) \in Conv(K)$.

Шаг индукции доказан; таким образом, для любых $\mathbf{a}, \mathbf{b} \in H$ выполнено $\mathbf{a} \oplus \mathbf{b} \in Conv(K) = H$. □

Доказываемая далее теорема 2 обобщает ранее полученные автором результаты о подалгебрах распределений, индуцированных конечными полями, на случай алгебр, индуцированных конечными кольцами. Одна из теорем из работы [3] в используемых нами обозначениях может быть записана следующим образом.

Теорема 1 [3]. *Пусть $\langle E_k; +, \times\rangle$ — конечное поле, $0 \in E_k$ — его нулевой элемент, а $\mathcal{A} = \langle \mathbf{S}^{(k)}; \oplus, \otimes\rangle$ — индуцированная им алгебра распределений. Пусть задано $\mathbf{g} \in \mathbf{S}^{(k)}$. Положим $K = \{\mathbf{e}^i \otimes (\mathbf{g} \oplus \mathbf{e}^j) \mid i \in E_k \setminus \{0\}, j \in E_k\} \cup \cup \{\mathbf{e}^0\}$, тогда $\langle Conv(K); \oplus, \otimes\rangle$ — подалгебра в алгебре $\mathcal{A}$.*

Несложно видеть, что фигурирующее в теореме 1 множество K является подмножеством в множестве K, определяемом соотношениями (4)–(6) с $M = E_k \setminus \{0\}$ (т. е. для кольца описание подалгебры устроено сложнее). Перейдем к формулировке теоремы.

Теорема 2. *Пусть $\langle E_k; +, \times\rangle$ — ассоциативное кольцо, $0 \in E_k$ — его нулевой элемент, а $\mathcal{A} = \langle \mathbf{S}^{(k)}; \oplus, \otimes\rangle$ — индуцированная им алгебра распределений. Пусть $\mathbf{g}^1, \ldots, \mathbf{g}^t \in \mathbf{S}^{(k)}$, тогда $\langle A(\mathbf{g}^1, \ldots, \mathbf{g}^t; E_k \setminus \{0\}); \oplus, \otimes\rangle$ — подалгебра в алгебре $\mathcal{A}$.*

Доказательство. Покажем, что для любых $\mathbf{a}, \mathbf{b} \in A(\mathbf{g}^1, \ldots, \mathbf{g}^t; E_k \setminus \{0\})$ выполнено $\mathbf{a} \oplus \mathbf{b}, \mathbf{a} \otimes \mathbf{b} \in A(\mathbf{g}^1, \ldots, \mathbf{g}^t; E_k \setminus \{0\})$.

Соотношение $\mathbf{a} \oplus \mathbf{b} \in A(\mathbf{g}^1, \ldots, \mathbf{g}^t; E_k \setminus \{0\})$ выполнено в силу леммы 7.

Напомним, что $A(\mathbf{g}^1, \ldots, \mathbf{g}^t; E_k \setminus \{0\}) = Conv(K)$, где K — множество, определяемое соотношениями (4)–(6) с $M = E_k \setminus \{0\}$. Тогда по лемме 4 достаточно доказать соотношение $\mathbf{a} \otimes \mathbf{b} \in Conv(K)$ для $\mathbf{a}, \mathbf{b} \in K$.

Согласно (2), имеет место $\mathbf{a} = \sum\limits_{l=0}^{k-1} a_l \mathbf{e}^l$, поэтому, в силу леммы 4 для доказательства включения $\mathbf{a} \otimes \mathbf{b} \in Conv(K)$ достаточно показать, что при всех $l \in E_k$ имеет место $\mathbf{e}^l \otimes \mathbf{b} \in Conv(K)$.

Поскольку $\mathbf{b} \in K$, выполнено $\mathbf{b} = (\mathbf{b}^{11} \oplus \cdots \oplus \mathbf{b}^{1\,k-1}) \oplus \cdots \oplus (\mathbf{b}^{t1} \oplus \ldots \oplus \oplus \mathbf{b}^{t\,k-1})$, где $\mathbf{b}^{ij} \in K_{ij}$. Тогда, используя (3), получаем:

$$\mathbf{e}^l \otimes \mathbf{b} = \widehat{\mu}_l(\mathbf{b}) = \widehat{\mu}_l((\mathbf{b}^{11} \oplus \cdots \oplus \mathbf{b}^{1\,k-1}) \oplus \cdots \oplus (\mathbf{b}^{t1} \oplus \cdots \oplus \mathbf{b}^{t\,k-1})) =$$
$$= (\widehat{\mu}_l(\mathbf{b}^{11}) \oplus \cdots \oplus \widehat{\mu}_l(\mathbf{b}^{1\,k-1})) \oplus \cdots \oplus (\widehat{\mu}_l(\mathbf{b}^{t1}) \oplus \cdots \oplus \widehat{\mu}_l(\mathbf{b}^{t\,k-1})).$$

Кроме того, имеет место $\widehat{\mu}_l(\mathbf{b}^{ij}) = \mathbf{e}^l \otimes (\mathbf{e}^j \otimes (\mathbf{g}^i \oplus \mathbf{e}^r)) = (\mathbf{e}^l \otimes \mathbf{e}^j) \otimes (\mathbf{g}^i \oplus \mathbf{e}^r)$. В силу леммы 1 выполнено $\mathbf{e}^l \otimes \mathbf{e}^j \in \{\mathbf{e}^0, \ldots, \mathbf{e}^{k-1}\}$. Если $\mathbf{e}^l \otimes \mathbf{e}^j = \mathbf{e}^0$, то $\widehat{\mu}_l(\mathbf{b}^{ij}) = \mathbf{e}^0$. В остальных случаях имеет место включение $\widehat{\mu}_l(\mathbf{b}^{ij}) \in K_{il \times j}$, где $l \times j \in E_k \setminus \{0\}$. В итоге получаем, что $\widehat{\mu}_l(\mathbf{b}^{ij}) \in K_i \subseteq K$. Таким образом $\mathbf{e}^l \otimes \mathbf{b}$ есть результат применения операции $\oplus$ к элементам из множества $K \subset Conv(K)$, по ранее доказанному он лежит в $Conv(K)$. Следовательно, $\mathbf{e}^l \otimes \mathbf{b} \in Conv(K)$, что влечет $\mathbf{a} \otimes \mathbf{b} \in Conv(K)$. Теорема доказана. □

Для ассоциативных колец с единицей можно несколько уменьшить количество распределений, от которых берется выпуклая оболочка при построении подалгебры. Соответствующее утверждение представлено в следующей теореме.

Теорема 3. *Пусть $\langle E_k; +, \times\rangle$ — ассоциативное кольцо, $1 \in E_k$ — единица кольца, $0 \in E_k$ — его нулевой элемент, U — группа обратимых элементов, а $\mathcal{A} = \langle \mathbf{S}^{(k)}; \oplus, \otimes\rangle$ — индуцированная им алгебра распределений. Обозначим через Z множество $E_k \setminus (U \cup \{0\})$. Пусть $\mathbf{g}^1, \ldots, \mathbf{g}^t \in \mathbf{S}^{(k)}$, положим:*

$$I = \{\mathbf{e}^j \otimes (\mathbf{g}^i \oplus \mathbf{e}^s) \mid j \in U, s \in E_k, i = 1, \ldots, t\}.$$

Тогда $\langle Conv(I \cup A(\mathbf{g}^1, \ldots, \mathbf{g}^t; Z)); \oplus, \otimes\rangle$ — подалгебра в алгебре $\mathcal{A}$.

Доказательство. Пусть $A(\mathbf{g}^1, \ldots, \mathbf{g}^t; Z) = Conv(K)$, где множество K определяется по $\mathbf{g}^1, \ldots, \mathbf{g}^t$ и Z согласно уравнениям (4)–(6). Заметим, что $Conv(I \cup Conv(K)) = Conv(I \cup K)$. По лемме 4 для доказательства теоремы достаточно показать, что для любых $\mathbf{a}, \mathbf{b} \in I \cup K$ выполнено $\mathbf{a} \oplus \mathbf{b}, \mathbf{a} \otimes \mathbf{b} \in Conv(I \cup K)$.

Если $\mathbf{a}, \mathbf{b} \in K$, то принадлежность $\mathbf{a} \oplus \mathbf{b} \in Conv(K)$ вытекает из леммы 7. Пусть теперь хотя бы одно из распределений $\mathbf{a}, \mathbf{b}$ лежит в множестве I. Без ограничения общности можно считать, что $\mathbf{b} \in I$. Покажем, что для любого $r \in E_k$ имеет место $\mathbf{e}^r \oplus \mathbf{b} \in I$. Тогда по лемме 4 получим, что для любого $\mathbf{a}$ выполнено $\mathbf{a} \oplus \mathbf{b} \in Conv(I) \subseteq Conv(I \cup K)$.

Рассмотрим $\mathbf{e}^r \oplus \mathbf{b}$. Поскольку $\mathbf{b} \in I$, найдутся такие $j, s \in E_k$ и такой номер i, что $\mathbf{b} = \mathbf{e}^j \otimes (\mathbf{g}^i \oplus \mathbf{e}^s)$. Тогда

$$\mathbf{e}^r \oplus \mathbf{b} = \mathbf{e}^r \oplus (\mathbf{e}^j \otimes (\mathbf{g}^i \oplus \mathbf{e}^s)) = \widehat{\mu}_j(\mathbf{e}^{j^{-1}r}) \oplus \widehat{\mu}_j(\mathbf{g}^i \oplus \mathbf{e}^s) = \widehat{\mu}_j(\mathbf{e}^{j^{-1}r} \oplus \mathbf{g}^i \oplus \mathbf{e}^s) =$$
$$= \mathbf{e}^j \otimes (\mathbf{e}^{j^{-1}r} \oplus \mathbf{g}^i \oplus \mathbf{e}^s) = \mathbf{e}^j \otimes (\mathbf{g}^i \oplus \mathbf{e}^{j^{-1}r+s}).$$

Отсюда в силу определения множества I получаем, что $\mathbf{e}^r \oplus \mathbf{b} \in I$. Итак, принадлежность $\mathbf{a} \oplus \mathbf{b} \in Conv(I \cup K)$ доказана.

Рассмотрим теперь $\mathbf{a} \otimes \mathbf{b}$. В силу леммы 4 достаточно доказать включение $\mathbf{a} \otimes \mathbf{b} \in Conv(I \cup K)$ для $\mathbf{a}, \mathbf{b} \in I \cup K$. Покажем, что для

любого элемента $r \in E_k$ выполнено $\mathbf{e}^r \otimes \mathbf{b} \in Conv(I \cup K)$. Тогда по лемме 4 получим, что $\mathbf{a} \otimes \mathbf{b} \in Conv(I \cup K)$ для любого распределения $\mathbf{a}$. Заметим, что любое $\mathbf{b} \in I \cup K$ представляется в виде $\mathbf{b} = \bigoplus\limits_{w=1}^{W} \mathbf{e}^{j_w} \otimes (\mathbf{g}^{i_w} \oplus \mathbf{e}^{s_w})$ для некоторого конечного W. Тогда

$$\mathbf{e}^r \otimes \mathbf{b} = \widehat{\mu}_r \left(\bigoplus_{w=1}^{W} \mathbf{e}^{j_w} \otimes (\mathbf{g}^{i_w} \oplus \mathbf{e}^{s_w}) \right) = \bigoplus_{w=1}^{W} \widehat{\mu}_r (\mathbf{e}^{j_w} \otimes (\mathbf{g}^{i_w} \oplus \mathbf{e}^{s_w})) =$$

$$= \bigoplus_{w=1}^{W} \mathbf{e}^{r \times j_w} \otimes (\mathbf{g}^{i_w} \oplus \mathbf{e}^{s_w}).$$

В последнем выражении осуществляется «суммирование» элементов, принадлежащих множеству $I \cup K$. По ранее доказанному, результат лежит в $Conv(I \cup K)$, откуда следует, что $\mathbf{e}^r \otimes \mathbf{b} \in Conv(I \cup K)$. Теорема доказана. □

Покажем, что если распределения $\mathbf{g}^1, \ldots, \mathbf{g}^t$ не содержат нулевых компонент, то фигурирующие в теоремах 2 и 3 подалгебры являются заведомо собственными, т. е. отличными от $\mathbf{S}^{(k)}$.

Сформулируем несколько вспомогательных утверждений.

Лемма 8. *Пусть* $\mathbf{h}^0, \ldots, \mathbf{h}^{t-1} \in \mathbf{S}^{(k)}$, $\boldsymbol{\alpha} \in \mathbf{S}^{(t)}$ *и* $\mathbf{e}^r = \sum\limits_{i=0}^{t-1} \alpha_i \mathbf{h}^i$. *Тогда существует такое* j, *что* $\alpha_j = 1$ *и* $\mathbf{h}^j = \mathbf{e}^r$.

Множество $N(\mathbf{p}) = \{i \in E_k \mid p_i > 0\}$ называется *носителем распределения* $\mathbf{p}$. Легко проверяется следующее утверждение.

Лемма 9. $|N(\mathbf{p} \oplus \mathbf{q})| \geqslant \max\{|N(\mathbf{p})|, |N(\mathbf{q})|\}$.

Также для операций $\oplus$ и $\otimes$, индуцированных операциями кольца, имеет место следующая лемма.

Лемма 10. *Пусть* $j, m \in E_k \setminus \{0\}$, $s \in E_k$, $\mathbf{g} \in \mathbf{S}^{(k)}$, $N(\mathbf{g}) = E_k$. *Тогда* $\mathbf{e}^j \otimes (\mathbf{g}^i \oplus \mathbf{e}^s) \neq \mathbf{e}^m$.

Доказательство. Предположим, что найдутся такие j, m, s, что выполнено $\mathbf{e}^j \otimes (\mathbf{g}^i \oplus \mathbf{e}^s) = \mathbf{e}^m$. Поскольку предполагается, что $N(\mathbf{g}) = E_k$, по лемме 9 получаем, что $N(\mathbf{g} \oplus \mathbf{e}^s) = E_k$, и тогда из соотношения $\mathbf{e}^j \otimes (\mathbf{g}^i \oplus \mathbf{e}^s) = \mathbf{e}^m$ следует, что в кольце выполняется тождество $j \times x = m$ для любого элемента $x \in E_k$. Полагая $x = 0$, получаем, что $m = j \times 0 = 0$, что противоречит условию леммы $m \neq 0$. Лемма доказана. □

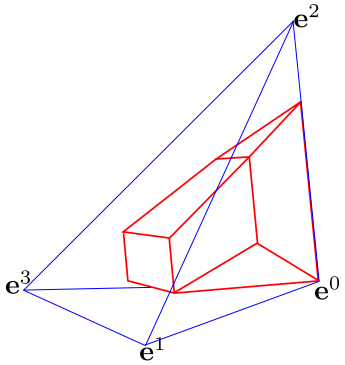
Из леммы 10 вытекает, что множество I из формулировки теоремы 3 и множества K_{ij}, определяемые соотношениями (4)–(6), не содержат распределений $\mathbf{e}^1, \ldots, \mathbf{e}^{k-1}$, если для всех $i = 1, \ldots, t$ выполнено $N(\mathbf{g}^i) = E_k$. Из леммы 9 следует, что эти распределения отсутствуют также в множествах K_i и K. Как следствие, по лемме 8 получаем, что распределения $\mathbf{e}^1, \ldots, \mathbf{e}^{k-1}$ лежат вне подалгебр, описываемых теоремами 2 и 3.

Приведем теперь пример подалгебры, построенной согласно теореме 3. В качестве кольца рассмотрим $\mathbb{Z}_4$ с операциями сложения и умножения $\pmod 4$. Это коммутативное ассоциативное кольцо с единицей, в котором элементы $1, 3 \in \mathbb{Z}_4$ образуют группу обратимых элементов.

Будем строить подалгебру, содержащую одно заданное распределение $\mathbf{g}$. Множество I из теоремы 3 имеет вид:

$$I = \{\mathbf{e}^1 \otimes (\mathbf{g} \oplus \mathbf{e}^0), \mathbf{e}^1 \otimes (\mathbf{g} \oplus \mathbf{e}^1), \mathbf{e}^1 \otimes (\mathbf{g} \oplus \mathbf{e}^2), \mathbf{e}^1 \otimes (\mathbf{g} \oplus \mathbf{e}^3),$$
$$\mathbf{e}^3 \otimes (\mathbf{g} \oplus \mathbf{e}^0), \mathbf{e}^3 \otimes (\mathbf{g} \oplus \mathbf{e}^1), \mathbf{e}^3 \otimes (\mathbf{g} \oplus \mathbf{e}^2), \mathbf{e}^3 \otimes (\mathbf{g} \oplus \mathbf{e}^3), \mathbf{e}^0\}.$$

Множество Z из теоремы 3 равно $E_4 \setminus \{0, 1, 3\} = \{2\}$.



Выпуклая подалгебра распределений над $\mathbb{Z}_4$

Построим такое множество K, что $A(\mathbf{g}; Z) = Conv(K)$. Согласно соотношениям (4)–(6), имеем: $K = K_1 = K_{12} = \{\mathbf{e}^2 \otimes (\mathbf{g} \oplus \mathbf{e}^s) \mid s \in E_4\} \cup \{\mathbf{e}^0\}$. С учетом свойств умножения в $\mathbb{Z}_4$ можно показать, что в действительности некоторые из перечисленных выше элементов множества K совпадают. Оно может быть переписано в виде $K = \{\mathbf{e}^2 \otimes \mathbf{g}, \mathbf{e}^2 \otimes (\mathbf{g} \oplus \mathbf{e}^1), \mathbf{e}^0\}$.

Для распределения $\mathbf{g} = (\frac{1}{2}, \frac{1}{4}, \frac{3}{16}, \frac{1}{16})$ выпуклая подалгебра $Conv(I \cup K)$ изображена на рисунке в проекции на подпространство $p_0 = 0$. Симплекс стохастических векторов нарисован синим, выпуклая подалгебра — красным. Отметим, что все три распределения из множества K лежат на отрезке, соединяющем распределения $\mathbf{e}^0$ и $\mathbf{e}^2$.

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

Список литературы

[1] Колпаков Р. М. Замкнутые классы конечных распределений рациональных вероятностей // Дискретный анализ и исследование операций. Серия 1. 2004. Т. 11, №3. С. 16–31.

[2] Мальцев А. И. Алгебраические системы. М.: Наука, 1970. 392 с.

[3] Яшунский А. Д. Выпуклые многогранники распределений, сохраняемые операциями конечного поля // Вестник МГУ. Математика. Механика. 2017. №4. С. 54–58.