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

Препринты ИПМ • Препринт № 51 за 2014 г.

Яшунский А. Д.

О множествах распределений вероятностей, сохраняемых операциями конечного поля

Рекомендуемая форма библиографической ссылки: Яшунский А. Д. О множествах распределений вероятностей, сохраняемых операциями конечного поля // Препринты ИПМ им. М.В.Келдыша. 2014. № 51. 20 с. URL: http://library.keldysh.ru/preprint.asp?id=2014-51

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

А. Д. Яшунский

О множествах распределений вероятностей, сохраняемых операциями конечного поля

Москва — 2014

Яшунский А. Д.

О множествах распределений вероятностей, сохраняемых операциями конечного поля

Рассматриваются распределения случайных величин над конечным полем, получаемых с помощью операций поля из независимых случайных величин, имеющих заданные распределения. Строятся подмножества распределений, которые сохраняются операциями сложения и умножения в конечном поле.

Ключевые слова: случайная величина, конечное поле, выразимость, сохраняемое множество

Alexey Dmitrievich Yashunsky

On probability distribution sets preserved by finite field operations

We consider distributions of random variables over a finite field, obtained as results of field operations on independent random variables with given distributions. We construct subsets of distributions that are preserved by finite field addition and multiplication.

Key words: random variable, finite field, expressibility, preserved set

Работа выполнена при поддержке Российского фонда фундаментальных исследований (проект № 14–01–00598) и программы фундаментальных исследований ОМН РАН «Алгебраические и комбинаторные методы математической кибернетики и информационные системы нового поколения» (проект «Задачи оптимального синтеза управляющих систем»).

Оглавление

Постановка задачи

Пусть имеется конечное поле $\mathcal{F}$ из k элементов, которые для удобства будем далее обозначать $\{0, 1, 2, \ldots, k-1\}$. Для элементов $i, j \in \mathcal{F}$ определены операции сложения $i + j$ и умножения $i \cdot j$. При этом будем считать, что элемент $0 \in \mathcal{F}$ — «ноль» для операции умножения (т. е. $0 \cdot i = i \cdot 0 = 0$) и нейтральный элемент для операции сложения (т. е. $0 + i = i + 0 = i$).

Свойства прочих элементов поля $\mathcal{F}$ для дальнейших рассуждений не существенны, важно лишь, что для ненулевых $i, j \in \mathcal{F}$ выполнено $i \cdot j \neq 0$ и уравнение $i \cdot j = m$ однозначно разрешимо как относительно i, так и относительно j. Будем записывать $i = m/j$ и $j = m/i$.

Для операции сложения при любых $i, j, m \in \mathcal{F}$ уравнение $i + j = m$ разрешимо как относительно i, так и относительно j: $i = m - j$, $j = m - i$.

Будем рассматривать случайные величины со значениями в поле $\mathcal{F}$. Распределение случайной величины X будем рассматривать как вектор с k координатами $P(X) = u = (u_0, u_1, \ldots, u_{k-1})$, понимая u_i как значение вероятности $\mathcal{P}\{X = i\}$. Естественно, для всех $i \in \mathcal{F}$ имеет место $u_i \geqslant 0$, а также выполнено

$$u_0 + u_1 + u_2 + \ldots + u_{k-1} = 1.$$

Для двух независимых случайных величин X_1 и X_2 со значениями в поле $\mathcal{F}$ можно рассматривать сумму $X_1 + X_2$ и произведение $X_1 \cdot X_2$, которые также являются случайными величинами со значениями в поле $\mathcal{F}$. Пусть $P(X_1) = u$, $P(X_2) = v$. Обозначим распределения вероятностей $P(X_1 + X_2)$ и $P(X_1 \cdot X_2)$ через $u + v$ и $u \cdot v$ соответственно. Их компоненты выражаются следующим образом:

$$(u + v)_i = \sum_{j \in \mathcal{F}} u_j v_{i-j}, \tag{1}$$

$$(u \cdot v)_0 = u_0 + v_0 - u_0 v_0, \tag{2}$$

$$i \neq 0 : (u \cdot v)_i = \sum_{j \in \mathcal{F} \setminus \{0\}} u_j v_{i/j}. \tag{3}$$

Рассматривается задача о выражении различных распределений вероятностей с помощью бесповторных формул, содержащих операции над полем $\mathcal{F}$, в которые вместо переменных подставляются независимые одинаково распределённые случайные величины над $\mathcal{F}$, имеющие «начальное» распределение $p = (p_0, p_1, \ldots, p_{k-1})$.

Ранее в [3] было построено семейство распределений, которые могут быть получены с помощью бесповторных формул из произвольного начального распределения с положительными компонентами. В данной работе получены

результаты противоположного характера: построены множества распределений, сохраняемые операциями поля. Как следствие, если начальное распределение p принадлежит какому-то из построенных множеств, никакое распределение вне этого множества не может быть бесповторно выражено через независимые случайные величины с распределением p.

Естественно, в каждое из сохраняемых множеств входят распределения из построенного ранее семейства выразимых распределений.

Геометрия пространства распределений

Множество распределений на элементах поля $\mathcal{F}$ можно интерпретировать геометрически как $(k-1)$-мерный симплекс в k-мерном пространстве с координатами $(u_0, u_1, \ldots, u_k)$, заданный соотношениями:

$$u_0 \geqslant 0, u_1 \geqslant 0, \ldots, u_{k-1} \geqslant 0, u_0 + u_1 + \ldots + u_{k-1} = 1.$$

Вершинами этого симплекса являются точки с координатами $(1, 0, \ldots, 0)$, $(0, 1, 0, \ldots, 0)$,..., $(0, \ldots, 0, 1)$. Они соответствуют вырожденным распределениям, в которых вероятность некоторого элемента поля равна 1. Равномерное распределение $\left(\frac{1}{k}, \ldots, \frac{1}{k}\right)$ соответствует центру масс этого симплекса. На рис. 1 изображено множество распределений для поля из трёх элементов.

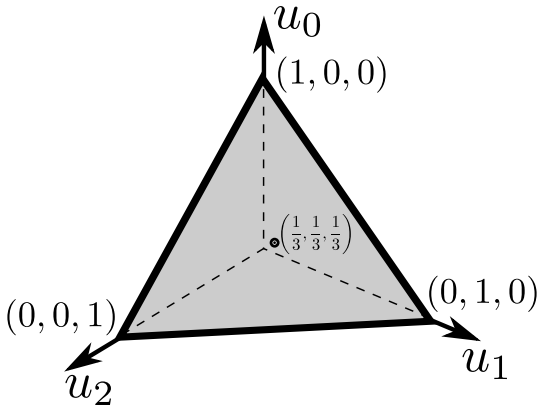

Рис. 1

Для дальнейших построений удобно описывать распределения вероятностей с помощью набора величин, выражаемых через компоненты $u_0, \ldots, u_{k-1}$. Фактически, мы рассматриваем переход к другой системе координат в k-мерном пространстве. Для точки u с набором координат $(u_0, u_1, \ldots, u_{k-1})$ положим:

$$\varepsilon(u) = 1 - u_0, \quad \delta_1(u) = u_1 - \frac{\varepsilon(u)}{k-1}, \ldots, \quad \delta_{k-1}(u) = u_{k-1} - \frac{\varepsilon(u)}{k-1}.$$

Набор величин $(\varepsilon(u), \delta_1(u), \ldots, \delta_{k-1}(u))$ представляет собой координаты точки u относительно другого набора базисных векторов; если считать, что координаты $(u_0, \ldots, u_{k-1})$ были заданы в ортонормированном базисе, то новый базис уже не будет ортонормированным (см. рис. 2 для размерности 3).

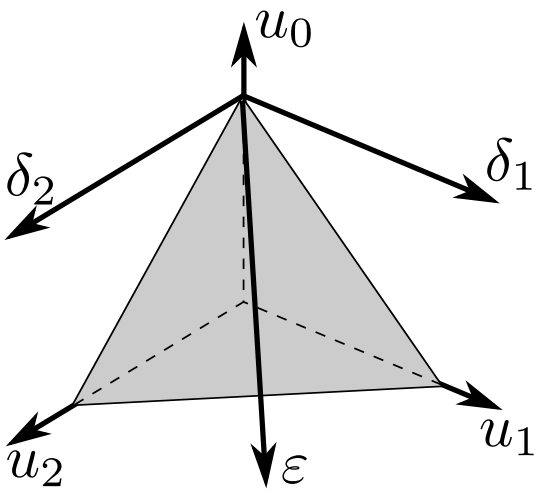

Рис. 2

Вектора нового базиса имеют в старом базисе координаты:

$$\left(-1, \frac{1}{k-1}, \ldots, \frac{1}{k-1}\right),$$
$$(0, 1, 0, \ldots, 0),$$
$$\ldots,$$
$$(0, \ldots, 0, 1),$$

т. е., за исключением первого базисного вектора, совпадают с исходными базисными векторами. Легко видеть, что эта замена координат является афинной. В дальнейшем мы будем оперировать набором координат $(\varepsilon(u), \delta_1(u), \ldots$ $\ldots, \delta_{k-1}(u))$, понимая, что все получаемые результаты могут быть легко перенесены в исходную систему координат с помощью обратного афинного преобразования.

Содержательно величины $(\varepsilon(u), \delta_1(u), \ldots, \delta_{k-1}(u))$ имеют для распределений вероятностей следующий смысл. Величина $\varepsilon(u)$ показывает, насколько отклоняется вероятность элемента $0 \in \mathcal{F}$ от значения 1, а величины $\delta_i(u)$ выражают, насколько отклоняется распределение вероятностей элементов $1, \ldots$ $\ldots, k-1 \in \mathcal{F}$ от равномерного распределения при фиксированной вероятности элемента $0 \in \mathcal{F}$, равной $1 - \varepsilon(u)$.

Для удобства будем рассматривать набор $(\varepsilon(u), \delta_1(u), \ldots, \delta_{k-1}(u))$ как координаты $(\varepsilon, \delta_1, \ldots, \delta_{k-1})$ в некотором ортнормированном базисе.

Соотношения, задающие симплекс распределений вероятностей, в новых координатах превращаются в

$$\varepsilon(u) \leqslant 1, \delta_1 \geqslant -\frac{\varepsilon}{k-1}, \ldots, \delta_{k-1} \geqslant -\frac{\varepsilon}{k-1},$$
$$\delta_1 + \ldots + \delta_{k-1} = 0.$$

Эти соотношения также задают симплекс в координатах $(\varepsilon, \delta_1, \ldots, \delta_{k-1})$. Начало координат $(0, \ldots, 0)$ является одной из вершин этого симплекса. Точка с координатами $(1, 0, \ldots, 0)$ лежит на грани симплекса; точки с координатами $(0, 1, 0, \ldots, 0)$,. . . ,$(0, \ldots, 0, 1)$ — вне симплекса. Таким образом, ось ε проходит внутри симплекса, а оси δ_1,. . . ,δ_{k-1} — вне его.

Несложно видеть, что симплекс лежит внутри $(k-1)$-мерной гиперплоскости (обозначим её D), которой ортогонален вектор с координатами $(0, 1, \ldots, 1)$. Вектор $\vec{e}_i = (0, \ldots, 0, 1, 0, \ldots, 0)$ представляется в виде суммы:

$$\vec{e}_i = \frac{1}{k-1}(0, 1, \ldots, 1) + \frac{1}{k-1}(0, -1, \ldots, -1, k-2, -1, \ldots, -1),$$

поэтому проекция вектора $\vec{e}_i$ на гиперплоскость D равна

$$\vec{e}'_i = \frac{1}{k-1}(0, -1, \ldots, -1, k-2, -1, \ldots, -1).$$

На рис. 3 изображён трёхмерный симплекс (для поля из четырёх элементов), базисный вектор $\vec{e}_0$ и проекции базисных векторов $\vec{e}'_1$, $\vec{e}'_2$, $\vec{e}'_3$.

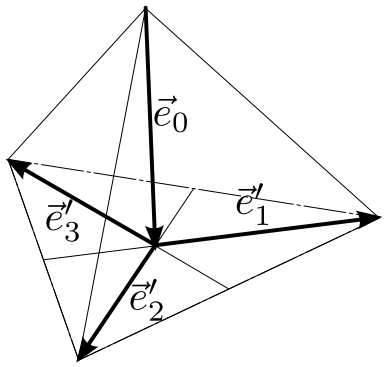

Рис. 3

Радиус-вектор $\vec{w} = (\varepsilon, \delta_1, \ldots, \delta_{k-1})$ произвольной точки пространства удовлетворяет соотношению:

$$\vec{w} = \varepsilon\vec{e}_0 + \delta_1\vec{e}_1 + \ldots + \vec{e}_{k-1}.$$

Если точка лежит в гиперплоскости D, то при проектировании в D это соотношение превращается в

$$\vec{w} = \varepsilon\vec{e}_0 + \delta_1\vec{e}'_1 + \ldots + \vec{e}'_{k-1}.$$

Умножим обе части равенства скалярно на $\vec{e}'_i$ $(i > 0)$. Учитывая соотношения $(\vec{e}'_i, \vec{e}'_i) = \frac{k-2}{k-1}$ и $(\vec{e}'_j, \vec{e}'_i) = -\frac{1}{k-1}$ при $i \neq j$, получаем:

$$\begin{aligned}(\vec{w}, \vec{e}'_i) &= \varepsilon(\vec{e}_0, \vec{e}'_i) + \delta_1(\vec{e}'_1, \vec{e}'_i) + \ldots + (\vec{e}'_{k-1}, \vec{e}'_i) = \\ &= \delta_i(\vec{e}'_i, \vec{e}'_i) + \sum_{j\neq 0,i} \delta_j(\vec{e}'_j, \vec{e}'_i) = \delta_i \frac{k-2}{k-1} + \sum_{j\neq 0,i} \delta_j \left(-\frac{1}{k-1}\right) = \\ &= \delta_i \frac{k-2}{k-1} + \delta_i \frac{1}{k-1} - \frac{1}{k-1} \sum_{j\neq 0} \delta_j = \delta_i.\end{aligned}$$

Пусть l_i — длина проекции вектора $\vec{w}$ на вектор $\vec{e}'_i$, тогда:

$$(\vec{w}, \vec{e}'_i) = l_i |\vec{e}'_i| = \frac{l_i}{|\vec{e}'_i|}(\vec{e}'_i, \vec{e}'_i) = \frac{l_i}{|\vec{e}'_i|} \frac{k-2}{k-1}.$$

Таким образом, получаем $\delta_i = \frac{k-2}{k-1} \cdot \frac{l_i}{|\vec{e}'_i|}$. Следовательно, для определения координаты δ_i произвольной точки пространства можно находить отношение длины проекции радиус-вектора этой точки на вектор $\vec{e}'_i$ к длине вектора $\vec{e}'_i$. Это соображение мы будем использовать в дальнейшем для построения подмножеств симплекса.

Множества, которые будут построены далее, представляют собой пересечения множеств, каждое из которых задано неравенствами, связывающими одну из координат δ_i с координатой ε. В силу такого устройства, при рассмотрении этих множеств удобно оперировать их проекцией на двумерную плоскость, заданную векторами $\vec{e}_0$ и $\vec{e}'_i$.

Суммы и произведения случайных величин

При переходе от распределений $u = (u_0, \ldots, u_{k-1})$ и $v = (v_0, \ldots, v_{k-1})$ к характеризующим их наборам величин $(\varepsilon(u), \delta_1(u), \ldots)$ и $(\varepsilon(v), \delta_1(v), \ldots)$, естественно, возникает необходимость преобразовать формулы (1)–(3). Поскольку $\varepsilon(u) = 1 - u_0$ и $\varepsilon(v) = 1 - v_0$, формула (2) принимает вид:

$$\varepsilon(u \cdot v) = \varepsilon(u) \cdot \varepsilon(v). \tag{4}$$

Выражая u_i через $\delta_i(u)$ и $\varepsilon(u)$, а v_i — через $\delta_i(v)$ и $\varepsilon(v)$, после необходимых преобразований получаем:

$$\delta_i(u \cdot v) = \sum_{j\in\mathcal{F}\setminus\{0\}} \delta_j(u)\delta_{i/j}(v). \tag{5}$$

Для распределения суммы вместо соотношения (1) получим два равенства:

$$\varepsilon(u+v) = \varepsilon(u) + \varepsilon(v) - \frac{k}{k-1}\varepsilon(u)\varepsilon(v) - \sum_{j\in\mathcal{F}\setminus\{0\}} \delta_j(u)\delta_{-j}(v), \tag{6}$$

$$\begin{aligned}\delta_i(u+v) = &\left(1 - \frac{k}{k-1}\varepsilon(u)\right)\delta_i(v) + \left(1 - \frac{k}{k-1}\varepsilon(v)\right)\delta_i(u) + \\ &+ \sum_{j\in\mathcal{F}\setminus\{0,i\}} \delta_j(u)\delta_{i-j}(v) + \frac{1}{k-1}\sum_{j\in\mathcal{F}\setminus\{0\}} \delta_j(u)\delta_{-j}(v).\end{aligned} \tag{7}$$

Полученные формулы (4)–(7) можно рассматривать просто как преобразования в пространстве с координатами $(\varepsilon, \delta_1, \ldots, \delta_{k-1})$, в том числе и вне симплекса, точки которого соответствуют распределениям вероятностей над полем $\mathcal{F}$.

В дальнейшем мы будем понимать под произведением точек u и v (возможно, лежащих вне симплекса распределений вероятностей) точку $u \cdot v$, полученную по формулам (4), (5), а под суммой — точку $u + v$, полученную по формулам (6), (7).

Из формулы (4) вытекает, что многократное перемножение независимых случайных величин даёт распределение, которое с ростом числа множителей приближается к распределению с $\varepsilon = 0$ (и, как следствие, $\delta_1 = \ldots = \delta_{k-1} = 0$).

Поскольку операция сложения в поле является групповой (и, следовательно, квазигрупповой), из результатов работы [2] следует, что многократное сложение независимых случайных величин с положительными компонентами распределений вероятностей даёт распределение, которое с ростом числа слагаемых приближается к равномерному распределению на элементах поля $\mathcal{F}$. Оно имеет $\varepsilon = \frac{k-1}{k}$ и $\delta_1 = \ldots = \delta_{k-1} = 0$. Величина $\frac{k-1}{k}$ будет использоваться в дальнейших построениях, обозначим её через h.

Результаты, полученные в работе [3] для распределений на конечных полях, могут быть сформулированы геометрически. Пусть $E = \{0 \leqslant \varepsilon \leqslant h, \delta_1 = \ldots = \delta_{k-1} = 0\}$ — отрезок в множестве распределений вероятностей. Для любого начального распределения π с положительными компонентами и любой точки $a \in E$ можно подобрать такую бесповторную формулу, составленную из сложений и умножений над полем $\mathcal{F}$, что при подстановке вместо её переменных независимых случайных величин с распределением π, распределение значений будет сколь угодно близко к точке a. На рис. 4 изображён отрезок E в случае поля из четырёх элементов.

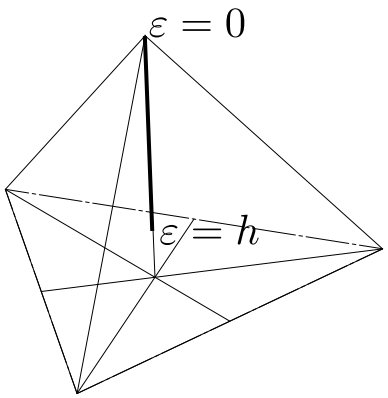

Рис. 4

Множества, сохраняемые умножением

Определим подмножество H_α в пространстве распределений:

$$H_\alpha = D \cap \left\{ (\varepsilon, \delta_1, \ldots, \delta_{k-1}) : \max_{i \neq 0} |\delta_i| \leqslant \frac{\varepsilon^\alpha}{k-1} \right\} = D \cap \left(\bigcap_{i \neq 0} \left\{ |\delta_i| \leqslant \frac{\varepsilon^\alpha}{k-1} \right\} \right).$$

Также определим $H_{\alpha,b} = H_\alpha \cap \{(\varepsilon, \delta_1, \ldots, \delta_{k-1}) : \varepsilon \leqslant b\}$. Из определения множества $H_{\alpha,1}$ легко видеть, что его проекция на двумерную плоскость векторов $\vec{e}_0$, $\vec{e}_i'$ имеет вид, представленный на рис. 5.

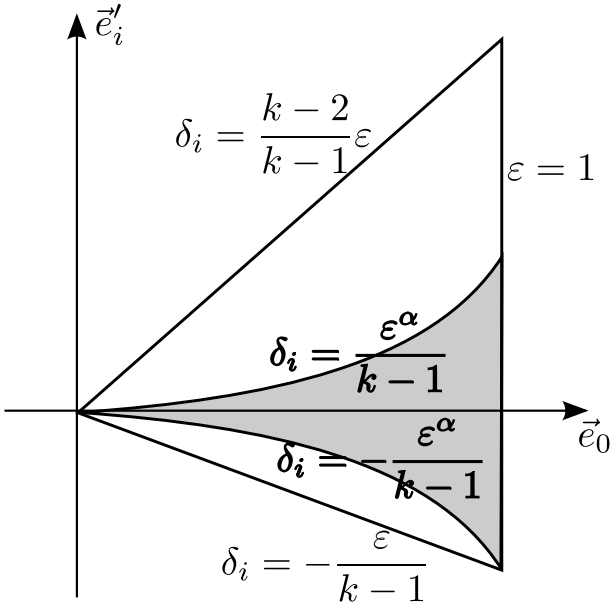

Рис. 5

Множество $H_{\alpha,1}$ для поля из четырёх элементов изображено на рис. 6. Его сечения в каждой плоскости с постоянным значением ε задаются соотношениями $\max\limits_i |\delta_i| \leqslant d$, где величина d зависит от ε. Для $k = 3$ сече-

ние — шестиугольник. Подобным образом будут устроены сечения и у других множеств, получаемых далее.

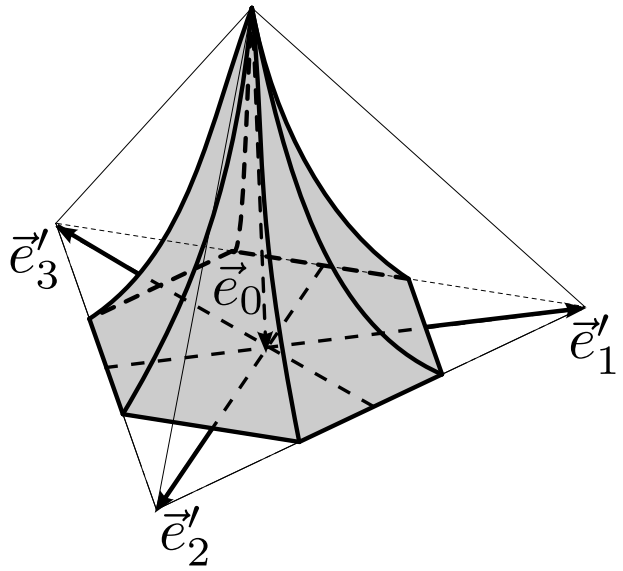

Рис. 6

Лемма 1. *Пусть* $\alpha \geqslant 1$, $b_1, b_2 \geqslant 0$, $u \in H_{\alpha,b_1}$, $v \in H_{\alpha,b_2}$. *Тогда* $u \cdot v \in H_{\alpha,b_1b_2}$.

Доказательство. Из $u \in H_{\alpha,b_1}$, $v \in H_{\alpha,b_2}$ следует, что $\varepsilon(u) \leqslant b_1$, $\varepsilon(v) \leqslant b_2$, откуда в силу (4) получаем $\varepsilon(u \cdot v) \leqslant b_1 b_2$.

Рассмотрим теперь $\delta_i(u \cdot v)$ при произвольном $i \neq 0$. Согласно (5):

$$|\delta_i(u \cdot v)| = \left|\sum_{j\neq 0} \delta_j(u)\delta_{i/j}(v)\right| \leqslant \sum_{j\neq 0} |\delta_j(u)| \cdot |\delta_{i/j}(v)| \leqslant \sum_{j\neq 0} \frac{(\varepsilon(u))^\alpha}{k-1} \cdot \frac{(\varepsilon(v))^\alpha}{k-1} =$$
$$= (k-1) \cdot \frac{(\varepsilon(u)\cdot\varepsilon(v))^\alpha}{(k-1)^2} = \frac{(\varepsilon(u\cdot v))^\alpha}{k-1}.$$

Таким образом, $u \cdot v \in H_{\alpha,b_1b_2}$. Лемма доказана.

Множества, сохраняемые сложением

Заметим, что соотношения (6) и (7) линейны как по $\varepsilon(u)$, $\delta_j(u)$ при фиксированном v, так и по $\varepsilon(v)$, $\delta_j(v)$ при фиксированном u. Отсюда легко следует, что при фиксированном распределении v выпуклое множество распределений u переходит при преобразованиях (6) и (7) в выпуклое множество (а при фиксированном u выпуклое множество распределений v переходит в выпуклое множество). Эти соображения позволяют показать, что операция сложения $u + v$ сохраняет некоторые выпуклые множества.

Пусть a, b, c — заданные положительные числа. Рассмотрим множество наборов $(\varepsilon, \delta_1, \ldots, \delta_{k-1})$ из гиперплоскости D, удовлетворяющих неравенствам:

$$|\delta_i| \leqslant a - \frac{a}{b}(\varepsilon - h), \quad |\delta_i| \leqslant a + \frac{a}{c}(\varepsilon - h), \quad i = 1, \ldots, k-1. \tag{8}$$

Обозначим это множество наборов $K_{a,b,c}$. Можно записать:

$$K_{a,b,c} = D \cap \left(\bigcap_{i \neq 0} \left\{ |\delta_i| \leqslant a - \frac{a}{b}(\varepsilon - h), |\delta_i| \leqslant a + \frac{a}{c}(\varepsilon - h) \right\} \right).$$

Легко видеть, что $K_{a,b,c}$ — выпуклое. Проекция множества $K_{a,b,c}$ на двумерную плоскость векторов $\vec{e}_0$, $\vec{e}_i'$ изображена на рис. 7.

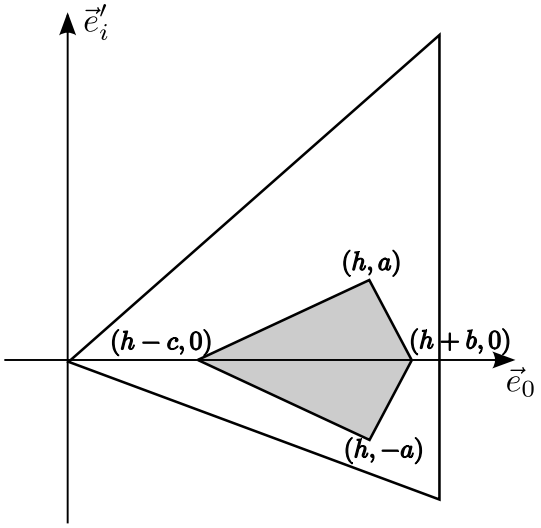

Рис. 7

Множество $K_{a,b,c}$ можно рассматривать как решение системы

$$\begin{cases} \frac{a}{b}\varepsilon + \delta_1 \leqslant a + \frac{a}{b}h \\ \frac{a}{b}\varepsilon - \delta_1 \leqslant a + \frac{a}{b}h \\ -\frac{a}{c}\varepsilon + \delta_1 \leqslant a - \frac{a}{c}h \\ -\frac{a}{c}\varepsilon - \delta_1 \leqslant a - \frac{a}{c}h \\ \ldots \\ \delta_1 + \ldots + \delta_{k-1} \leqslant 0 \\ -\delta_1 - \ldots - \delta_{k-1} \leqslant 0 \end{cases}, \tag{9}$$

состоящей из $4(k-1)+2$ неравенств.

Множество решений системы образует выпуклый многогранник, являющийся выпуклой оболочкой своих вершин (крайних точек), см. [1]. Вершины являются решениями системы уравнений, полученной из системы (9) заменой нестрогих неравенств либо на строгие неравенства, либо на равенства, так, что система, составленная только из равенств, имеет ранг в точности k.

Несложно видеть, что последние два неравенства обязательно обращаются в равенства. Для произвольного i рассмотрим четыре неравенства, связывающие δ_i и ε. Среди возможных вариантов обращения неравенств в равенства ровно четыре являются совместными, они дают вершины множества, изображённого на рис. 7:

1. $\varepsilon = h - c$, $\delta_i = 0$;
2. $\varepsilon = h$, $\delta_i = a$;
3. $\varepsilon = h$, $\delta_i = -a$;
4. $\varepsilon = h + b$, $\delta_i = 0$.

Выбор $\varepsilon = h - c$ или $\varepsilon = h + b$ обращает в равенства по два неравенства в каждой четвёрке неравенств, связывающих одно из δ_j и ε, причём получающиеся равенства линейно зависимы, а следовательно, добавляют к рангу системы 1, а не 2. Из этих равенств вытекает, что $\delta_j = 0$. Суммарный ранг системы из равенств будет равен $2 + 1 \cdot (k - 2) = k$.

Выбор $\varepsilon = h$ приводит к тому, что из четвёрки неравенств, связывающих одно из δ_j и ε, два превращаются в $\delta_j \leqslant a$, а другие два — в $\delta_j \geqslant -a$. Следовательно, в равенство могут обращаться какие-то два неравенства из четырёх, причём каждая пара таких равенств добавляет к рангу системы 1. Вообще говоря, возможно, что ни одно из четырёх неравенств, содержащих δ_j и ε, не обращается в равенство.

Помимо δ_i, мы можем выбрать $k - 3$ независимых равенств, задающих значения для δ_j. Для задания последнего незаданного δ_j добавим в систему равенство $\delta_1 + \ldots + \delta_{k-1} = 0$. Оно, очевидно, является независимым и позволяет получить недостающее значение δ_j. В итоге, ранг системы равенств будет равен $2 + 1 \cdot (k - 3) + 1 = k$.

Таким образом, заключаем, что вершинами выпуклого множества $K_{a,b,c}$ являются:

1. точка $(h - c, 0, \ldots, 0)$;
2. точка $(h + b, 0, \ldots, 0)$;
3. точки вида $(h, d_1, \ldots, d_{k-1})$, где $d_1 + \ldots + d_{k-1} = 0$ и все d_i, за исключением, быть может, одного, принадлежат множеству $\{a, -a\}$ (а если есть $d_i \neq \pm a$, то оно равно нулю).

Все эти точки, естественно, лежат в гиперплоскости D, но, вообще говоря, не обязательно лежат внутри симплекса, соответствующего распределениям вероятностей.

Покажем, что при определённых соотношениях между параметрами a, b, c множество $K_{a,b,c}$ сохраняется преобразованиями (6) и (7).

Лемма 2. *Пусть* $0 < a \leqslant \frac{1}{k}$, $k(k-1)a^2 \leqslant b \leqslant c \leqslant h$. *Пусть* $u, v \in K_{a,b,c}$. *Тогда* $u + v \in K_{a,b,c}$.

Доказательство. В силу выпуклости множества $K_{a,b,c}$ и билинейности отображения $u + v$, достаточно проверить, что для любой пары вершин u, v множества $K_{a,b,c}$, $u + v \in K_{a,b,c}$. Рассмотрим всевозможные пары.

Пусть сначала $u = (h + x, 0, \ldots, 0)$, $v = (h + y, 0, \ldots, 0)$. Тогда из (6), (7) получаем:

$$\begin{aligned} \varepsilon(u+v) &= (h+x) + (h+y) - \frac{1}{h}(h+x)(h+y) = h - \frac{xy}{h}, \\ \delta_i(u+v) &= 0. \end{aligned} \tag{10}$$

Используя эти соотношения, находим $\varepsilon(u + v)$ для следующих комбинаций вершин:

1. $u = (h - c, 0, \ldots, 0)$, $v = (h - c, 0, \ldots, 0)$: $\varepsilon(u + v) = h - \frac{c^2}{h}$.
2. $u = (h - c, 0, \ldots, 0)$, $v = (h + b, 0, \ldots, 0)$: $\varepsilon(u + v) = h + \frac{bc}{h}$.
3. $u = (h + b, 0, \ldots, 0)$, $v = (h + b, 0, \ldots, 0)$: $\varepsilon(u + v) = h - \frac{b^2}{h}$.

В силу выполненных по условию леммы неравенств $b \leqslant c \leqslant h$ имеет место $\frac{bc}{h} \leqslant b$, $\frac{c^2}{h} \leqslant c$ и $\frac{b^2}{h} \leqslant c$. Отсюда вытекает, что во всех рассмотренных комбинациях $u + v \in K_{a,b,c}$.

Пусть теперь $u = (h + x, 0, \ldots, 0)$, $v = (h, d_1, \ldots, d_{k-1})$. Тогда из (6), (7) получаем:

$$\begin{aligned} \varepsilon(u+v) &= (h+x) + h - \frac{1}{h}(h+x)h = h, \\ \delta_i(u+v) &= \left(1 - \frac{1}{h}(h+x)\right) d_i = -\frac{x}{h} d_i. \end{aligned} \tag{11}$$

Как в случае $u = (h - c, 0, \ldots, 0)$, так и в случае $u = (h + b, 0, \ldots, 0)$, в силу неравенств $b \leqslant c \leqslant h$ выполнено:

$$|\delta_i(u+v)| \leqslant |d_i| \leqslant a,$$

откуда легко следует, что $u + v \in K_{a,b,c}$.

Наконец, рассмотрим $u = (h, d'_1, \ldots, d'_{k-1})$ и $v = (h, d''_1, \ldots, d''_{k-1})$. Тогда из (6), (7) получаем:

$$\varepsilon(u+v) = h + h - \frac{1}{h}h^2 - \sum_{j\neq 0} d'_j d''_{-j} = h - \sum_{j\neq 0} d'_j d''_{-j},$$

$$\delta_i(u+v) = \sum_{j\neq 0,i} d'_j d''_{i-j} + \frac{1}{k-1}\sum_{j\neq 0} d'_j d''_{-j}.$$

Из полученных соотношений следуют оценки $|\varepsilon(u+v) - h| \leqslant (k-1)a^2$ и

$$|\delta_i(u+v)| \leqslant (k-2)a^2 + \frac{1}{k-1}(k-1)a^2 = (k-1)a^2.$$

Таким образом, точка $u+v$ лежит внутри выпуклого множества, заданного неравенствами:

$$h - (k-1)a^2 \leqslant \varepsilon \leqslant h + (k-1)a^2,$$
$$-(k-1)a^2 \leqslant \delta_i \leqslant (k-1)a^2, \quad i = 1, \ldots, k-1.$$

Проекция этого множества на двумерную плоскость векторов $\vec{e}_0$, $\vec{e}'_i$ имеет вид, представленный на рис. 8.

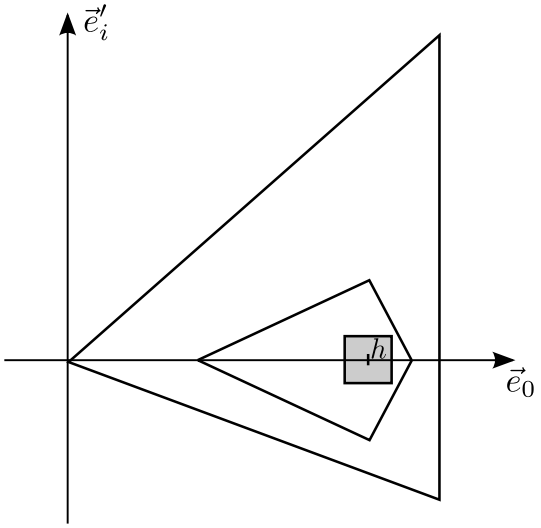

Рис. 8

Покажем, что всё это множество целиком лежит внутри $K_{a,b,c}$. Для этого достаточно показать, что его вершины лежат внутри $K_{a,b,c}$, т. е. удовлетворяют неравенствам (8).

В рассматриваемых точках вершин $\varepsilon = h \pm (k-1)a^2$, а следовательно, $\varepsilon - h = \pm(k-1)a^2$. Кроме того, в указанных точках $|\delta_i| = (k-1)a^2$. Следовательно, требуется показать, что выполнены неравенства:

$$(k-1)a^2 \leqslant a \pm \frac{a}{b}(k-1)a^2, \quad (k-1)a^2 \leqslant a \pm \frac{a}{c}(k-1)a^2.$$

В силу положительности a, b, c, неравенства

$$(k-1)a^2 \leqslant a + \frac{a}{c}(k-1)a^2 \text{ и } (k-1)a^2 \leqslant a + \frac{a}{b}(k-1)a^2$$

следуют из

$$(k-1)a^2 \leqslant a - \frac{a}{c}(k-1)a^2 \text{ и } (k-1)a^2 \leqslant a - \frac{a}{b}(k-1)a^2.$$

По условию леммы, $b, c \geqslant k(k-1)a^2$, откуда $\frac{a}{b}(k-1)a^2 \leqslant \frac{a}{k}$ и $\frac{a}{c}(k-1)a^2 \leqslant \frac{a}{k}$. Тогда

$$a - \frac{a}{b}(k-1)a^2 \geqslant a - \frac{a}{k} = \frac{a}{k}(k-1),$$
$$a - \frac{a}{c}(k-1)a^2 \geqslant a - \frac{a}{k} = \frac{a}{k}(k-1).$$

Вместе с неравенством $a \leqslant \frac{1}{k}$, выполненным по условию леммы, это даёт необходимые неравенства. Лемма доказана.

Лемма 3. *Пусть* $K_1 = K_{a,k(k-1)a^2,c}$, $K_2 = K_{a',k(k-1)a'^2,c'}$, *где* $0 < a, a' \leqslant \frac{1}{k}$, $k(k-1)a^2 \leqslant c \leqslant h$, $k(k-1)a'^2 \leqslant c' \leqslant h$. *Тогда для любых* $u, v \in K_1 \cup K_2$ *выполнено* $u + v \in K_1 \cup K_2$.

Доказательство. Без ограничения общности можно считать, что $a \geqslant a'$. Если при этом $c' \leqslant c$, то $K_2 \subseteq K_1$, $K_1 \cup K_2 = K_1$, и утверждение леммы вытекает из леммы 2. Далее предполагаем, что $c' > c$. Проекции множеств K_1 и K_2 на двумерную плоскость векторов $\vec{e}_0$, $\vec{e}'_i$ в этом случае изображены на рис. 9.

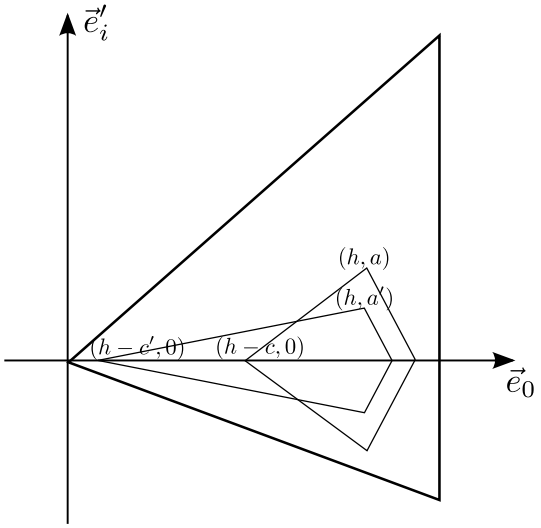

Рис. 9

Пусть $u, v \in K_1 \cup K_2$. Если при этом $u, v \in K_1$ (соответственно, $u, v \in K_2$), то по лемме 2 имеет место $u + v \in K_1$ (соответственно, $u + v \in K_2$), откуда

вытекает утверждение леммы. Таким образом, остаётся рассмотреть случаи, когда $u \in K_1$, $v \in K_2$.

Покажем, что при произвольном фиксированном $u \in K_1$ и всевозможных $v \in K_2$ сумма $u + v$ лежит в K_1. В силу выпуклости множеств K_1 и K_2 для этого достаточно показать, что всевозможные комбинации, где u — вершина множества K_1, а v — вершина множества K_2, дают $u + v \in K_1$.

В силу соотношений $a \geqslant a'$ и $c < c'$ между параметрами множеств K_1 и K_2, все вершины множества K_2 за исключением $(h - c', 0, \ldots, 0)$, лежат внутри K_1, поэтому для них $u + v \in K_1$ в силу леммы 2. Покажем, что для $v = (h - c', 0, \ldots, 0)$ также выполнено $u + v \in K_1$ для всех вершин u множества K_1.

Из соотношений (10) и неравенства $c' \leqslant h$ следует, что для вершин $u = (h - c, 0, \ldots, 0)$ и $u = (h + k(k-1)a^2, 0, \ldots, 0)$ выполняется $u + v \in K_1$.

Для $u = (h, d_1, \ldots, d_{k-1})$ из соотношений (11) и неравенства $c' \leqslant h$, вытекает что $u + v \in K_1$. Таким образом, лемма доказана.

Теоремы сохранения

Теорема 1. *Пусть* $0 < a \leqslant \frac{1}{k}$. *Тогда для любых* $u, v \in K_{a,k(k-1)a^2,h} \cap \{\varepsilon \leqslant 1\}$ *выполнено* $u \cdot v, u + v \in K_{a,k(k-1)a^2,h} \cap \{\varepsilon \leqslant 1\}$.

Доказательство. По лемме 2 в условиях теоремы $u + v \in K_{a,k(k-1)a^2,h}$, поэтому достаточно доказать, что $u \cdot v \in K_{a,k(k-1)a^2,h}$.

Пусть заданы $u, v \in K_{a,k(k-1)a^2,h}$ и пусть, без ограничения общности, выполнено $\varepsilon(u) \leqslant \varepsilon(v)$. Положим:

$$d = \max_i \{|\delta_i| : (\varepsilon(u), \delta_1, \ldots, \delta_{k-1}) \in K_{a,k(k-1)a^2,h}\}.$$

В силу $a \leqslant \frac{1}{k}$ можно выбрать α такое, что $d = \frac{(\varepsilon(u))^\alpha}{k-1}$, а именно $\alpha = \frac{\ln(k-1)d}{\ln \varepsilon(u)} \geqslant 1$ (см. рис. 10).

В силу выбора d и α получаем, что $H_{\alpha,\varepsilon(u)} \subset K_{a,k(k-1)a^2,h}$. Кроме того, $u \in H_{\alpha,\varepsilon(u)}$, $v \in H_{\alpha_0,\varepsilon(v)}$. Тогда по лемме 1 и в силу $\varepsilon(u), \varepsilon(v) \leqslant 1$ имеем:

$$u \cdot v \in H_{\alpha,\varepsilon(u)\varepsilon(v)} \subseteq H_{\alpha,\varepsilon(u)} \subset K_{a,k(k-1)a^2,h}.$$

Неравенства $\varepsilon(u \cdot v) \leqslant 1$ и $\varepsilon(u + v) \leqslant 1$ легко выводятся из условий теоремы. Теорема доказана.

Теорема 2. *Для любого* $k \geqslant 3$ *найдётся такое* $\alpha_0(k)$, *что при всех* $\alpha \geqslant \alpha_0(k)$ *множества*

$$I_\alpha = (H_{\alpha,h} \cup K_{a,k(k-1)a^2,k(k-1)a^2}) \cap \{\varepsilon \leqslant 1\},$$

где $a = \frac{h^\alpha}{k-1}$, *сохраняются сложением и умножением, т. е. для любых* $u, v \in I_\alpha$ *выполнено* $u \cdot v, u + v \in I_\alpha$.

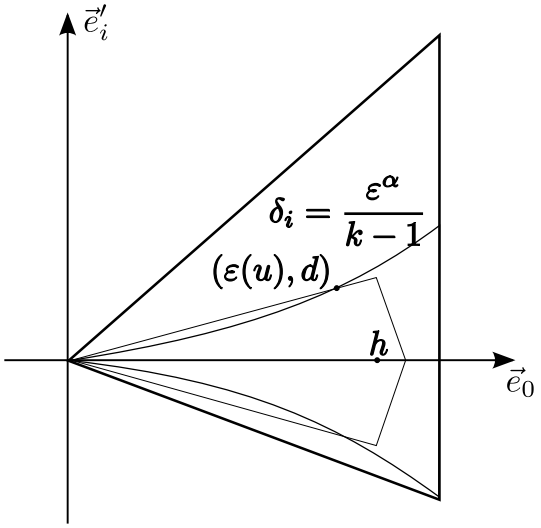

Рис. 10

Доказательство. Рассмотрим взаимное расположение множества H_α и множества $K_{a,k(k-1)a^2,k(k-1)a^2}$ при $a = \frac{h^\alpha}{k-1}$. Покажем, что для достаточно больших значений α имеет место

$$K_{a,k(k-1)a^2,k(k-1)a^2} \subset H_\alpha.$$

Рассмотрим проекции указанных множеств на двумерную плоскость, заданную векторами $\vec{e}_0$, $\vec{e}'_i$ (см. рис. 11). Легко видеть, что точка с $\varepsilon = h$ и $\delta_i = \frac{h^\alpha}{k-1}$ лежит на границе обоих множеств.

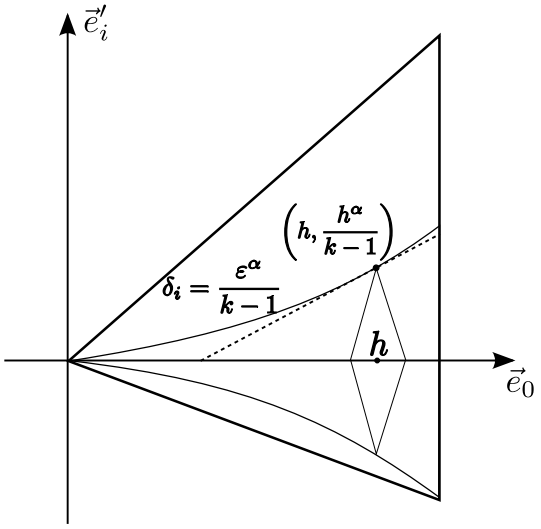

Рис. 11

Точки из множества $K_{a,k(k-1)a^2,k(k-1)a^2}$ удовлетворяют неравенству

$$|\delta_i| \leqslant a + \frac{a}{k(k-1)a^2}(\varepsilon - h).$$

Далее будем рассматривать только точки с $\delta_i \geqslant 0$ (для $\delta_i \leqslant 0$ — аналогично).

Точки множества H_α удовлетворяют неравенству $\delta_i \leqslant \frac{\varepsilon^\alpha}{k-1}$. Рассмотрим касательную к графику функции $\frac{\varepsilon^\alpha}{k-1}$ в точке $\varepsilon = h$. Функция выпукла вниз, поэтому точки, лежащие ниже касательной, лежат заведомо ниже функции.

Касательная пересекается с прямой $a + \frac{a}{k(k-1)a^2}(\varepsilon - h)$ в точке $\varepsilon = h$. Если тангенс угла наклона касательной меньше, чем тангенс угла наклона прямой, то все точки множества $K_{a,k(k-1)a^2,k(k-1)a^2}$ с $\varepsilon \leqslant h$ лежат ниже касательной, а следовательно — в множестве H_α. При этом точки множества $K_{a,k(k-1)a^2,k(k-1)a^2}$ с $\varepsilon \geqslant h$ заведомо лежат в множестве H_α.

Запишем условие для тангенсов угла наклона в виде неравенства:

$$\frac{\alpha h^{\alpha-1}}{k-1} \leqslant \frac{a}{k(k-1)a^2}.$$

Поскольку $a = \frac{h^\alpha}{k-1}$, оно эквивалентно $\alpha h^{2(\alpha-1)} \leqslant 1$. Так как имеет место $\lim\limits_{\alpha\to\infty} \alpha h^{2(\alpha-1)} = 0$, то найдётся такое α_0 (зависящее от h и, следовательно, от k), что для всех $\alpha \geqslant \alpha_0$ неравенство выполнено. Для указанных значений α имеет место включение $K_{a,k(k-1)a^2,k(k-1)a^2} \subset H_\alpha$.

Пусть теперь $u, v \in I_\alpha$, где $\alpha \geqslant \alpha_0$.

Если $\varepsilon(u) \leqslant h$ или $\varepsilon(v) \leqslant h$, то $u \cdot v \in H_{\alpha,h} \subset I_\alpha$. Если же $\varepsilon(u), \varepsilon(v) > h$, то найдётся такое $\alpha' \geqslant \alpha$, что

$$u, v \in H_{\alpha',\max\{\varepsilon(u),\varepsilon(v)\}} \subset I_\alpha.$$

Отсюда $u \cdot v \in H_{\alpha',\max\{\varepsilon(u),\varepsilon(v)\}} \subset I_\alpha$.

Покажем теперь, что $u + v \in I_\alpha$. Если $u \in K_{a,k(k-1)a^2,k(k-1)a^2}$, положим $K_1 = K_{a,k(k-1)a^2,k(k-1)a^2}$. В противном случае выберем в качестве K_1 такое множество $K_{a',k(k-1)a'^2,c}$, что:

1. $\frac{a'}{c} = \frac{\alpha(\varepsilon(u))^\alpha}{k-1}$,
2. $\max\limits_i\{\delta_i : (\varepsilon(u), \delta_1, \ldots, \delta_{k-1}) \in K_1\} = \frac{(\varepsilon(u))^\alpha}{k-1}$,

т. е., которое касается границы множества H_α в точке $\varepsilon = \varepsilon(u)$. Легко видеть, что $u \in K_1 \subset I_\alpha$. Аналогично выберем K_2 по v. Тогда $u, v \in K_1 \cup K_2$, и по лемме 3 получаем, что $u + v \in K_1 \cup K_2 \subset I_\alpha$.

Теорема доказана.

Теоремы 1 и 2 позволяют построить последовательность вложенных подмножеств симплекса распределений, каждое из которых сохраняется сложением и умножением. В проекции на плоскость, заданную векторами $\vec{e}_0$, $\vec{e}'_i$, эти множества изображены на рис. 12.

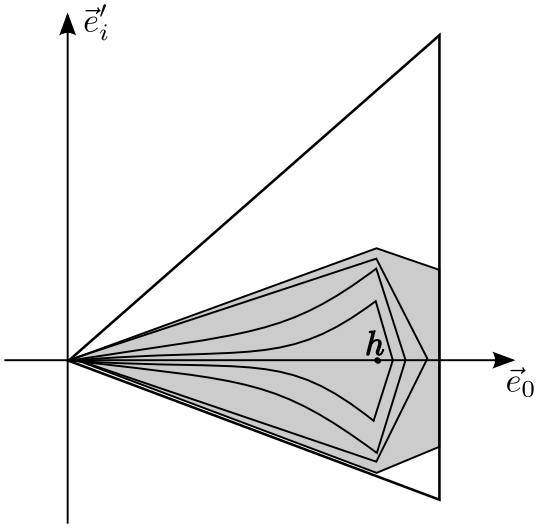

Рис. 12

Дополнительные замечания

Помимо операций сложения и умножения в поле $\mathcal{F}$ можно также рассматривать обратные им операции вычитания и деления. С точки зрения преобразования распределений это равносильно рассмотрению унарных операций взятия противоположного и обратного элементов.

Для конечного поля операция взятия противоположного элемента является, фактически, некоторой перестановкой на множестве элементов поля, причём эта перестановка оставляет элемент $0 \in \mathcal{F}$ на месте. Легко видеть, что все построенные выше сохраняемые сложением и умножением множества сохраняются также всеми перестановками, которые оставляют на месте 0, а значит, сохраняются и унарной операцией взятия противоположного элемента.

Взятие обратного элемента x^{-1} не определено для $0 \in \mathcal{F}$, однако, если доопределить $0^{-1} = 0$, то x^{-1} также будет задавать перестановку элементов поля, оставляющую ноль на месте, а значит, будет сохранять построенные выше множества.

Отметим, кроме того, что от структуры $\mathcal{F}$ в построениях выше требовались далеко не все свойства поля. Все конструкции остаются в силе, если вместо $\mathcal{F}$ рассматривать множество, на котором задана квазигрупповая операция «сложения» с нейтральным элементом $0 \in \mathcal{F}$, а также операция «умножения», квазигрупповая на $\mathcal{F} \setminus \{0\}$ и удовлетворяющая $0 \cdot x = x \cdot 0 = 0$ для всех $x \in \mathcal{F}$. Такие структуры могут, в частности, содержать произвольное число элементов k (а не только степень простого числа, как в случае поля). По аналогии с квазигруппами, Р. В. Гончаров в частной беседе предложил называть эти структуры «квазиполями».

Построенные в теоремах 1 и 2 множества покрывают далеко не весь сим-

плекс распределений вероятностей. Только в частном случае $k = 3$ для любой точки симплекса среди построенных множество найдётся множество, содержащее эту точку. Уже для $k = 4$ можно явно указать точки симплекса, не попадающие ни в одно из построенных множеств. Более того, с ростом k доля объёма построенных сохраняемых множеств в объёме симплекса стремится к нулю.

Автор выражает благодарность О. М. Касим-Заде за внимание к работе и плодотворные обсуждения.

Список литературы

[1] Ашманов С. А. Линейное программирование. — М.: Наука, 1981. — 340 с.

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

[3] Яшунский А. Д. Об одном семействе распределений вероятностей, порождаемом бесповторными формулами над конечными полями // Материалы IX молодежной научной школы по дискретной математике и ее приложениям (Москва, 16–21 сентября 2013 г.). — М.: ИПМ им. М. В. Келдыша, 2013. — С. 127–130.