Math-Net.Ru

Общероссийский математический портал

А. Д. Яшунский, О неповторных преобразованиях случайных величин над конечными полями, *Дискрет. матем.*, 2015, том 27, выпуск 3, 145–157

DOI: <https://doi.org/10.4213/dm1341>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением <http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 54.80.97.219

26 апреля 2023 г., 18:07:04

О бесповторных преобразованиях случайных величин над конечными полями

© 2015 г. А. Д. Яшунский

Рассматриваются преобразования независимых случайных величин над конечным полем бесповторными формулами. Строятся подмножества распределений случайных величин, которые сохраняются бесповторными преобразованиями. Кроме того, строится семейство распределений, которые могут быть сколь угодно точно приближены бесповторным преобразованием независимых одинаково распределенных случайных величин, распределение которых не имеет нулевых компонент.

Ключевые слова: случайная величина, конечное поле, распределение вероятностей, сохраняемое множество, приближение.

1. Введение

Преобразования случайных величин в конечной алгебраической системе рассматривались в первую очередь в контексте задачи о порождении распределений вероятностей. В общем виде ее можно сформулировать следующим образом. Пусть задано некоторое конечное множество E и набор $\mathcal{B}$ операций на нем. Пусть, кроме того, имеется некоторое конечное множество G *начальных* распределений случайных величин со значениями в E . Требуется описать множество распределений вероятностей, которые выражаются бесповторными формулами с операциями из $\mathcal{B}$ над независимыми случайными величинами с распределениями из G .

Для $E = \{0, 1\}$ и $\mathcal{B}$, состоящего из всевозможных функций алгебры логики, задача рассматривалась Р. Л. Схиртладзе. В [3] показано, что при $G = \{(\frac{1}{2}, \frac{1}{2})\}$ любое распределение с двоично-рациональными компонентами выразимо. Та же задача для произвольного множества G рассматривалась и была решена Р. М. Колпаковым, им же полученные результаты обобщены на случай $E = \{0, 1, \dots, k-1\}$ и множество $\mathcal{B}$, состоящее из всех функций k -значной логики (подробнее см. [2]).

Помимо точного выражения распределений можно также рассматривать сколь угодно точное приближение (аппроксимацию) распределений (определение аппроксимации распределений см. в разделе 8). В такой постановке Р. Л. Схиртладзе было показано [4], что при $G = \{(p, 1-p)\}$, $p \in (0, 1)$ и $\mathcal{B} = \{\&, \vee, \neg\}$ любое распределение $(\eta, 1-\eta)$ с $\eta \in (0, 1)$ аппроксимируется.

---

*Место работы: Институт прикладной математики им. М. В. Келдыша РАН,
e-mail: yashunsky@keldysh.ru

В аппроксимационной постановке можно сформулировать результаты для некоторых других конечных алгебраических систем. Если $\mathcal{B} = \{\circ\}$, где $\circ$ — групповая операция на $E = \{0, 1, \dots, k-1\}$, а $G = \{(p_0, p_1, \dots, p_{k-1})\}$, и все $p_i > 0$ (такие распределения будем называть *невырожденными*), то распределение $X_1 \circ \dots \circ X_m$ при $m \rightarrow \infty$ приближается к равномерному на E распределению (подробнее о случайных блужданиях на группах см. обзор [7]).

В работе С. Марковски и др. [6] показано, что для невырожденного начального распределения и множества $\mathcal{B} = \{\circ_1, \dots, \circ_r\}$, где $\circ_j$ — квазигрупповые операции, распределения, задаваемые формулами $((\dots((X_1 \circ_{i_1} X_2) \circ_{i_2} X_3) \dots) \circ_{i_{m-1}} X_m)$, также приближаются к равномерному на E распределению при $m \rightarrow \infty$. Автором в [5] исследованы распределения для того же множества $\mathcal{B}$ без ограничений на вид используемых бесповторных формул и для произвольного начального распределения. В частности, установлено, что для невырожденных начальных распределений единственная предельная точка выразимых распределений — равномерное распределение.

2. Постановка задачи

В данной работе рассматривается конечное поле $E = \{0, 1, \dots, k-1\}$ и множество операций $\mathcal{B} = \{\cdot, +\}$ — умножение и сложение в поле E . Считаем, что $0 \in E$ — ноль для умножения ($0 \cdot i = i \cdot 0 = 0$) и для сложения ($0 + i = i + 0 = i$).

Определим *формулы* с операциями из $\mathcal{B}$ индуктивно. Переменные $X_1, X_2, X_3, \dots$ считаем формулами. Если Φ_1 и Φ_2 — формулы, то $(\Phi_1 \cdot \Phi_2)$ и $(\Phi_1 + \Phi_2)$ — также формулы. Формула называется *бесповторной*, если в ней все переменные различны.

Для независимых случайных величин X и Y со значениями в E , имеющих распределения u и v , сумма $X + Y$ есть случайная величина, распределение которой будем обозначать $u \oplus v$. Его компоненты получаются сверткой компонент распределений u и v (здесь и далее полагаем, что операции с элементами $i, j \in E$ выполняются в поле E):

$$(u \oplus v)_i = \sum_{j \in E} u_j v_{i-j}. \quad (1)$$

Аналогично, для произведения независимых случайных величин $X \cdot Y$ будем обозначать распределение $u \otimes v$. Тогда для его компонент выполнено:

$$(u \otimes v)_0 = u_0 + v_0 - u_0 v_0, \quad (2)$$

$$i \neq 0 : (u \otimes v)_i = \sum_{j \in E \setminus \{0\}} u_j v_{i \cdot (j^{-1})}. \quad (3)$$

Исследуется множество распределений, которые могут быть получены в качестве распределений значений бесповторной формулы при подстановке вместо ее переменных независимых случайных величин с распределениями из множества G . Для заданной бесповторной формулы распределение значений может быть найдено с помощью соотношений (1)–(3). Отсюда легко видеть, что исследуемое множество распределений есть в точности замыкание множества G относительно введенных операций $u \oplus v$ и $u \otimes v$.

3. Геометрия пространства распределений

Множество распределений на конечном множестве $E = \{0, 1, \dots, k-1\}$ — k -мерных вероятностных векторов — можно рассматривать как симплекс в k -мерном пространстве с координатами $(u_0, u_1, \dots, u_{k-1})$, заданный соотношениями $u_0 + u_1 + \dots + u_{k-1} = 1$ и $u_i \geq 0$ для всех i .

Для точки $u = (u_0, u_1, \dots, u_{k-1})$ положим:

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

Набор $(\varepsilon(u), \delta_1(u), \dots, \delta_{k-1}(u))$ представляет собой координаты точки u относительно другого набора базисных векторов и другого начала координат. Эта замена координат аффинная и невырожденная. Далее мы будем оперировать координатами $(\varepsilon(u), \delta_1(u), \dots, \delta_{k-1}(u))$, понимая, что все получаемые результаты могут быть легко перенесены в исходную систему координат. Для удобства будем считать, что $(\varepsilon, \delta_1, \dots, \delta_{k-1})$ — координаты в ортонормированном базисе, а проекции далее будем считать ортогональными.

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

$$\varepsilon \leq 1, \quad \delta_1 \geq -\frac{\varepsilon}{k-1}, \dots, \delta_{k-1} \geq -\frac{\varepsilon}{k-1}, \quad \delta_1 + \dots + \delta_{k-1} = 0.$$

Симплекс лежит в $(k-1)$ -мерной гиперплоскости D , заданной уравнением $\delta_1 + \dots + \delta_{k-1} = 0$. Вершины симплекса имеют координаты

$$(0, \dots, 0), \left(1, \frac{k-2}{k-1}, -\frac{1}{k-1}, \dots, -\frac{1}{k-1}\right), \dots, \left(1, -\frac{1}{k-1}, \dots, -\frac{1}{k-1}, \frac{k-2}{k-1}\right).$$

Для точки $(\varepsilon, \delta_1, \dots, \delta_{k-1}) \in D$ выполнено $\delta_1 + \dots + \delta_{k-1} = 0$, откуда следует, что ее радиус-вектор представляется в виде

$$\begin{aligned} (\varepsilon, \delta_1, \dots, \delta_{k-1}) &= \varepsilon(1, 0, \dots, 0) + \\ &+ \sum_{i \in E \setminus \{0\}} \delta_i \left(0, -\frac{1}{k-1}, \dots, -\frac{1}{k-1}, \underbrace{\frac{k-2}{k-1}}_{i\text{-е место}}, -\frac{1}{k-1}, \dots, -\frac{1}{k-1}\right), \end{aligned} \quad (4)$$

т. е. раскладывается по системе векторов

$$\begin{aligned} \vec{e}_0 &= (1, 0, \dots, 0), \\ \vec{e}_1 &= \left(0, \frac{k-2}{k-1}, -\frac{1}{k-1}, \dots, -\frac{1}{k-1}\right), \dots, \vec{e}_{k-1} = \left(0, -\frac{1}{k-1}, \dots, -\frac{1}{k-1}, \frac{k-2}{k-1}\right). \end{aligned}$$

Векторы $\vec{e}_1, \dots, \vec{e}_{k-1}$ и вектор $(-\vec{e}_0)$ соединяют точку $(1, 0, \dots, 0)$ со всеми вершинами симплекса. Вектор $\vec{e}_0$ ортогонален всем $\vec{e}_i$ с $i \neq 0$, а $\sum_{i=1}^{k-1} \vec{e}_i = \vec{0}$. При $i, j \neq 0$ скалярное произведение $(\vec{e}_i, \vec{e}_j)$ с $i \neq j$ равно $-\frac{1}{k-1}$, а скалярное произведение $(\vec{e}_i, \vec{e}_i)$ равно $\frac{k-2}{k-1}$. Умножая соотношение (4) скалярно на $\vec{e}_i$, получаем, что длина проекции радиус-вектора на $\vec{e}_0$ равна ε , а длины проекций на $\vec{e}_i$ при $i \neq 0$ отличаются от δ_i лишь постоянным множителем $|\vec{e}_i|^{-1}$.

Далее будут рассматриваться множества точек, у которых координаты δ_i и ε связаны неравенствами. Приведенные выше соображения позволяют при рассмотрении этих множеств оперировать с их проекцией на плоскости векторов $\vec{e}_0, \vec{e}_i$.

4. Распределения сумм и произведений

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

$$\varepsilon(u \otimes v) = \varepsilon(u) \cdot \varepsilon(v). \quad (5)$$

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

$$\delta_i(u \otimes v) = \sum_{j \in E \setminus \{0\}} \delta_j(u) \delta_{i \cdot (j-1)}(v). \quad (6)$$

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

$$\varepsilon(u \oplus v) = \varepsilon(u) + \varepsilon(v) - \frac{k}{k-1} \varepsilon(u) \varepsilon(v) - \sum_{j \in E \setminus \{0\}} \delta_j(u) \delta_{0-j}(v), \quad (7)$$

$$\begin{aligned} \delta_i(u \oplus v) &= \left(1 - \frac{k}{k-1} \varepsilon(u)\right) \delta_i(v) + \left(1 - \frac{k}{k-1} \varepsilon(v)\right) \delta_i(u) + \\ &+ \sum_{j \in E \setminus \{0, i\}} \delta_j(u) \delta_{i-j}(v) + \frac{1}{k-1} \sum_{j \in E \setminus \{0\}} \delta_j(u) \delta_{0-j}(v). \end{aligned} \quad (8)$$

Формулы (5)–(8) можно рассматривать просто как определение двух операций в пространстве с координатами $(\varepsilon, \delta_1, \dots, \delta_{k-1})$, в том числе и вне симплекса, точки которого соответствуют распределениям вероятностей.

Далее мы будем понимать под *произведением точек* u и v (возможно, лежащих вне симплекса распределений) точку $u \otimes v$, полученную по формулам (5), (6), а под *суммой* — точку $u \oplus v$, полученную по формулам (7), (8).

5. Множества, сохраняемые умножением

Для $\varepsilon \geq 0$ определим множество H_α :

$$H_\alpha = \left\{ (\varepsilon, \delta_1, \dots, \delta_{k-1}) : \max_i |\delta_i| \leq \frac{\varepsilon^\alpha}{k-1} \right\} \cap D = \bigcap_i \left\{ |\delta_i| \leq \frac{\varepsilon^\alpha}{k-1} \right\} \cap D.$$

Также определим $H_{\alpha,b} = H_\alpha \cap \{\varepsilon \leq b\}$. Проекция множества $H_{\alpha,1}$ на плоскость векторов $\vec{e}_0, \vec{e}_i$ имеет вид, представленный на рис. 1а.

Множество $H_{\alpha,1}$ для поля из четырех элементов изображено на рис. 1б. Его сечения в каждой плоскости с фиксированным значением ε — правильные шестиугольники, заданные соотношениями $\max_i |\delta_i| \leq d$, где d зависит от ε .

Лемма 1. Пусть $\alpha \geq 1$, $b_1, b_2 \geq 0$, $u \in H_{\alpha,b_1}$, $v \in H_{\alpha,b_2}$. Тогда $u \otimes v \in H_{\alpha,b_1 b_2}$.

Доказательство. Из $u \in H_{\alpha,b_1}$, $v \in H_{\alpha,b_2}$ следует, что $\varepsilon(u) \leq b_1$, $\varepsilon(v) \leq b_2$, откуда в силу (5) получаем $\varepsilon(u \otimes v) \leq b_1 b_2$.

Рис. 1.

Рассмотрим теперь $\delta_i(u \otimes v)$ при произвольном i . Согласно (6):

$$\begin{aligned}
 |\delta_i(u \otimes v)| &= \left| \sum_{j \in E \setminus \{0\}} \delta_j(u) \delta_{i \cdot (j-1)}(v) \right| \leq \sum_{j \in E \setminus \{0\}} |\delta_j(u)| \cdot |\delta_{i \cdot (j-1)}(v)| \leq \\
 &\leq \sum_{j \in E \setminus \{0\}} \frac{\varepsilon(u)^\alpha}{k-1} \cdot \frac{\varepsilon(v)^\alpha}{k-1} = (k-1) \cdot \frac{(\varepsilon(u) \cdot \varepsilon(v))^\alpha}{(k-1)^2} = \frac{\varepsilon(u \otimes v)^\alpha}{k-1}.
 \end{aligned}$$

Таким образом, $u \otimes v \in H_{\alpha, b_1 b_2}$. Лемма доказана.

6. Множества, сохраняемые сложением

Обозначим $h = \frac{k-1}{k}$. Пусть a, b, c — некоторые положительные числа. Определим множество $K_{a,b,c}$:

$$K_{a,b,c} = \bigcap_i \left\{ |\delta_i| \leq a - \frac{a}{b}(\varepsilon - h), |\delta_i| \leq a + \frac{a}{c}(\varepsilon - h) \right\} \cap D.$$

Проекция множества $K_{a,b,c}$ на плоскость векторов $\vec{e}_0, \vec{e}_i$ изображена на рис. 2.

Легко видеть, что $K_{a,b,c}$ — выпуклое множество. Его можно рассматривать как решение системы

$$\left\{ \begin{array}{l} \frac{a}{b}\varepsilon + \delta_1 \leq a + \frac{a}{b}h, \\ \frac{a}{b}\varepsilon - \delta_1 \leq a + \frac{a}{b}h, \\ -\frac{a}{c}\varepsilon + \delta_1 \leq a - \frac{a}{c}h, \\ -\frac{a}{c}\varepsilon - \delta_1 \leq a - \frac{a}{c}h, \\ \dots \\ \delta_1 + \dots + \delta_{k-1} \leq 0, \\ -\delta_1 - \dots - \delta_{k-1} \leq 0, \end{array} \right. \quad (9)$$

Рис. 2.

состоящей из $4(k-1) + 2$ неравенств.

Множество решений системы — выпуклый многогранник, являющийся выпуклой оболочкой своих вершин, см. [1]. Каждая вершина — решение системы уравнений, полученной из (9) заменой нестрогих неравенств либо на строгие неравенства, либо на равенства, так, что система, составленная только из равенств, имеет в точности ранг k (размерность пространства).

Рассматривая различные варианты обращения неравенств системы (9) в равенства, устанавливаем, что вершинами множества $K_{a,b,c}$ являются:

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

Все эти точки, естественно, лежат в гиперплоскости D , но, вообще говоря, не обязательно лежат внутри симплекса, соответствующего распределениям вероятностей. Множество $K_{a,b,c}$ представляет собой объединение двух конусов с разными вершинами $(h-c, 0, \dots, 0)$ и $(h+b, 0, \dots, 0)$, но с общим основанием, лежащим в гиперплоскости $\{\varepsilon = h\}$ и являющимся сечением $(k-1)$ -мерного куба $\{-a \leq \delta_i \leq a\}$ гиперплоскостью D .

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

Доказательство. Поскольку системы координат $(\varepsilon, \delta_1, \dots, \delta_{k-1})$ и $(u_0, u_1, \dots, u_{k-1})$ связаны невырожденным аффинным преобразованием, множество $K_{a,b,c}$ является выпуклым многогранником и в системе координат $(u_0, u_1, \dots, u_{k-1})$, где в силу (1) операция $u \oplus v$ билинейна. Следовательно, выполнение условия $u \oplus v \in K_{a,b,c}$ достаточно проверить только для всевозможных пар вершин u, v множества $K_{a,b,c}$.

Пусть сначала $u = (h + x, 0, \dots, 0)$, $v = (h + y, 0, \dots, 0)$. Тогда из (7), (8) следует, что

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

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

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

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

Пусть теперь $u = (h + x, 0, \dots, 0)$, $v = (h, d_1, \dots, d_{k-1})$. Тогда из (7), (8) следует, что

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

Как в случае $u = (h - c, 0, \dots, 0)$, так и в случае $u = (h + b, 0, \dots, 0)$, в силу неравенств $b \leq c \leq h$ выполнено $|\delta_i(u \oplus v)| \leq |d_i| \leq a$, откуда легко следует, что $u \oplus v \in K_{a,b,c}$.

Наконец, пусть $u = (h, d'_1, \dots, d'_{k-1})$, $v = (h, d''_1, \dots, d''_{k-1})$. Тогда в силу (7), (8)

$$\begin{aligned}\varepsilon(u \oplus v) &= h + h - \frac{1}{h}h^2 - \sum_{j \in E \setminus \{0\}} d'_j d''_{0-j} = h - \sum_{j \in E \setminus \{0\}} d'_j d''_{0-j}, \\ \delta_i(u \oplus v) &= \sum_{j \in E \setminus \{0, i\}} d'_j d''_{i-j} + \frac{1}{k-1} \sum_{j \in E \setminus \{0\}} d'_j d''_{0-j}.\end{aligned}$$

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

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

Таким образом, точка $u \oplus v$ лежит внутри выпуклого множества K' , заданного неравенствами

$$\begin{aligned}h - (k-1)a^2 &\leq \varepsilon \leq h + (k-1)a^2, \\ -(k-1)a^2 &\leq \delta_i \leq (k-1)a^2, \quad i = 1, \dots, k-1.\end{aligned}$$

Покажем, что K' целиком лежит внутри $K_{a,b,c}$. Для этого достаточно показать, что вершины K' лежат внутри $K_{a,b,c}$, т.е. удовлетворяют неравенствам (9).

Для вершин множества K' выполнено $\varepsilon = h \pm (k-1)a^2$, а следовательно, $\varepsilon - h = \pm(k-1)a^2$. Кроме того, для них имеет место $|\delta_i| = (k-1)a^2$. Таким образом, требуется показать, что выполнены неравенства

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

В силу положительности a, b, c , неравенства $(k-1)a^2 \leq a + \frac{a}{c}(k-1)a^2$ и $(k-1)a^2 \leq a + \frac{a}{b}(k-1)a^2$ следуют из $(k-1)a^2 \leq a - \frac{a}{c}(k-1)a^2$ и $(k-1)a^2 \leq a - \frac{a}{b}(k-1)a^2$.

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

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

Вместе с неравенством $a \leq \frac{1}{k}$, выполненным по условию леммы, это дает необходимые соотношения. Лемма доказана.

Сложение точек сохраняет также некоторые невыпуклые множества.

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

Доказательство. Без ограничения общности можно считать, что $a \geq a'$. Если при этом $c' \leq c$, то $K_2 \subseteq K_1$, $K_1 \cup K_2 = K_1$, и утверждение леммы вытекает из леммы 2. Далее предполагаем, что $c' > c$. Проекция множеств K_1 и K_2 на двумерную плоскость векторов $\vec{e}_0, \vec{e}_i$ в этом случае изображены на рис. 3.

Рис. 3.

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 $u \oplus v \in K_1$ (соответственно, $u \oplus v \in K_2$), откуда вытекает утверждение леммы. Остается рассмотреть случай $u \in K_1, v \in K_2$.

Покажем, что при произвольном фиксированном $u \in K_1$ и всевозможных $v \in K_2$ сумма $u \oplus v \in K_1$. 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 $u \oplus v \in K_1$.

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

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

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

7. Теоремы сохранения

Из утверждений лемм 1 и 2 может быть выведена следующая теорема.

Теорема 1. Пусть $0 < a \leq \frac{1}{k}$. Тогда $u \otimes v, u \oplus v \in K_{a, k(k-1)a^2, h} \cap \{\varepsilon \leq 1\}$ для любых $u, v \in K_{a, k(k-1)a^2, h} \cap \{\varepsilon \leq 1\}$.

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

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

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

Положим $\alpha = \frac{\ln[(k-1)d]}{\ln \varepsilon(u)}$. Тогда $d = \frac{\varepsilon(u)^\alpha}{k-1}$, и $\alpha \geq 1$, так как $a \leq \frac{1}{k}$.

В силу выбора d и α получаем, что $H_{\alpha, \varepsilon(u)} \subset K_{a, k(k-1)a^2, h}$. Кроме того, $u \in H_{\alpha, \varepsilon(u)}$, а из $\varepsilon(u) \leq \varepsilon(v)$ и $v \in K_{a, k(k-1)a^2, h}$ вытекает, что $v \in H_{\alpha, \varepsilon(v)}$. Тогда по лемме 1 и с учетом условий $\varepsilon(u), \varepsilon(v) \leq 1$ имеем:

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

Неравенства $\varepsilon(u \otimes v) \leq 1$ и $\varepsilon(u \oplus v) \leq 1$ легко выводятся из леммы 1 и соотношения (7). Теорема доказана.

Использование леммы 3 позволяет установить существование сохраняемых множеств более сложной формы:

Теорема 2. Для любого $k \geq 3$ найдется такое $\alpha_0(k)$, что при всех $\alpha \geq \alpha_0(k)$ множества $I_\alpha = (H_{\alpha, h} \cup K_{a, k(k-1)a^2, k(k-1)a^2}) \cap \{\varepsilon \leq 1\}$, где $a = \frac{h^\alpha}{k-1}$, сохраняются сложением и умножением, т. е. для любых $u, v \in I_\alpha$ выполнено $u \otimes v, u \oplus v \in I_\alpha$.

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 включение

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

Рассмотрим проекции указанных множеств на двумерную плоскость, заданную векторами $\vec{e}_0, \vec{e}_i$ (см. рис. 4). Легко видеть, что точка с $\varepsilon = h$ и $\delta_i = \frac{h^\alpha}{k-1}$ лежит на границе обоих множеств.

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

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

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

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

Рис. 4.

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 этой прямой, то все точки множества $K_{a,k(k-1)a^2,k(k-1)a^2}$ с $\varepsilon \leq h$ 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 $\varepsilon \geq h$ заведомо лежат в множестве H_α .

Запишем условие для тангенсов угла наклона в виде неравенства:

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

Поскольку $a = \frac{h^\alpha}{k-1}$, оно эквивалентно неравенству $\alpha h^{2(\alpha-1)} \leq 1$. Так как имеет место $\lim_{\alpha \rightarrow \infty} \alpha h^{2(\alpha-1)} = 0$, то найдется такое α_0 (зависящее от h и, следовательно, от k), что для всех $\alpha \geq \alpha_0$ 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 $\alpha \geq \alpha_0$.

Если $\varepsilon(u) \leq h$ или $\varepsilon(v) \leq h$, то $u \otimes v \in H_{\alpha,h} \subset I_\alpha$. Если же $\varepsilon(u), \varepsilon(v) > h$, то найдется такое $\alpha' \geq \alpha$, что $u, v \in H_{\alpha', \max\{\varepsilon(u), \varepsilon(v)\}} \subset I_\alpha$. Следовательно, $u \otimes v \in H_{\alpha', \max\{\varepsilon(u), \varepsilon(v)\}} \subset I_\alpha$.

Покажем теперь, что $u \oplus v \in I_\alpha$. Если $u \in K_{a,k(k-1)a^2,k(k-1)a^2}$, то 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) $\frac{a'}{c} = \frac{\alpha \varepsilon(u)^{\alpha-1}}{k-1}$,
- (2) $\max_i \{\delta_i : (\varepsilon(u), \delta_1, \dots, \delta_{k-1}) \in K_1\} = \frac{\varepsilon(u)^\alpha}{k-1}$,

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

Общая картина сохраняемых множеств, описываемых теоремами 1 и 2, изображена на рис. 5 в проекции на плоскость векторов $\vec{e}_0, \vec{e}_i$.

Рис. 5.

8. Аппроксимируемые распределения

Будем говорить, что распределение u *приближает* распределение v с *точностью* $\Delta > 0$, если¹ $|\varepsilon(u) - \varepsilon(v)| < \Delta$ и $\max_i |\delta_i(u) - \delta_i(v)| < \Delta$. Распределения, которые могут быть приближены с любой наперед заданной точностью $\Delta > 0$ бесповторными комбинациями независимых случайных величин с распределениями из G , будем называть *аппроксимируемыми*.

Пусть $p \in G$ — невырожденное распределение. Покажем, что в этом случае все распределения с $\varepsilon \in [0, h]$ и $\delta_1 = \dots = \delta_{k-1} = 0$ аппроксимируемы. Пусть задана точность аппроксимации $\Delta > 0$.

Рассмотрим произведение $X_1 \cdot X_2 \cdots X_m$ независимых случайных величин с распределением p . Очевидно, что распределение $p^{(m)}$ произведения $m + 1$ случайных величин удовлетворяет $p^{(0)} = p$, $p^{(m+1)} = p^{(m)} \otimes p$.

Несложно видеть, что $p^{(m)}$ сходится к распределению $(1, 0, \dots, 0)$. Заметим также, что условное распределение произведения $X_1 \cdots X_m$ при условии $X_1 \cdots X_m \neq 0$ в точности совпадает с распределением произведения независимых случайных величин над группой поля по умножению, имеющих невырожденное распределение $(p_1/(1 - p_0), \dots, p_{k-1}/(1 - p_0))$. В [5] показано, что такие распределения сходятся к равномерному. Отсюда непосредственно вытекает, что $\delta_i(p^{(m)})/\varepsilon(p^{(m)}) \rightarrow 0$ при $m \rightarrow \infty$. Следовательно, найдется такое $\alpha > 1$, что $p^{(m)} \in H_{\alpha, 1}$ при всех достаточно больших m .

Отсюда легко вывести, что для любого a , $0 < a \leq \frac{1}{k}$, найдется такой номер m_0 , что $p^{(m)} \in K_{a, k(k-1)a^2, h}$ при $m \geq m_0$. Выберем $a = \min\{\Delta, \frac{1}{k}\}$ и соответствующее m_0 . Поскольку $p^{(m)}$ сходится к $(1, 0, \dots, 0)$ при $m \rightarrow \infty$, имеет место $\varepsilon(p^{(m)}) \rightarrow 0$, а следовательно, найдется такое $m_1 \geq m_0$, что $\varepsilon(p^{(m_1)}) < \Delta$. Тогда $p^{(m_1)}$ приближает с точностью Δ распределение с $\varepsilon = 0$, $\delta_1 = \dots = \delta_k = 0$.

¹Это эквивалентно $\max_i |u_i - v_i| < \Delta'$ для подходящего $\Delta' > 0$.

Положим $q = p^{(m_1)}$. Отметим, что $q \in H_{\alpha,1}$. Определим последовательность $q^{(0)} = q$, $q^{(n+1)} = q^{(n)} \oplus q$. В силу выбора q , по лемме 2 при всех n выполнено $q^{(n)} \in K_{a,k(k-1)a^2,h}$. Следовательно, $|\delta_i(q^{(n)})| < \Delta$ для всех i .

Согласно (1) имеем $q_0^{(n+1)} = q_0^{(n)} q_0 + \sum_{j \in E \setminus \{0\}} q_j^{(n)} q_{0-j}$, откуда

$$\varepsilon(q^{(n+1)}) = \varepsilon(q^{(n)}) + \varepsilon(q) - \varepsilon(q^{(n)})\varepsilon(q) - \sum_{j \in E \setminus \{0\}} q_j^{(n)} q_{0-j}.$$

Тогда, с одной стороны,

$$\varepsilon(q^{(n+1)}) - \varepsilon(q^{(n)}) \leq \varepsilon(q)(1 - \varepsilon(q^{(n)})) \leq \varepsilon(q) \leq \Delta,$$

а с другой, в силу $q \in H_{\alpha,1}$,

$$\begin{aligned} \varepsilon(q^{(n+1)}) - \varepsilon(q^{(n)}) &\geq \varepsilon(q)(1 - \varepsilon(q^{(n)})) - \max_{j \in E \setminus \{0\}} q_j \sum_{j \in E \setminus \{0\}} q_j^{(n)} \geq \\ &\geq \varepsilon(q)(1 - \varepsilon(q^{(n)})) - \frac{\varepsilon(q) + \varepsilon(q)^\alpha}{k-1} \varepsilon(q^{(n)}) = \varepsilon(q) \left(1 - \varepsilon(q^{(n)}) \left(1 + \frac{1 + \varepsilon(q)^{\alpha-1}}{k-1} \right) \right). \end{aligned}$$

Если $\varepsilon(q^{(n)}) \leq h - \frac{\varepsilon(q)^{\alpha-1}}{k-1}$, то

$$\varepsilon(q^{(n+1)}) - \varepsilon(q^{(n)}) \geq \varepsilon(q) \left(1 - \left(\frac{k-1}{k} - \frac{\varepsilon(q)^{\alpha-1}}{k-1} \right) \left(\frac{k}{k-1} + \frac{\varepsilon(q)^{\alpha-1}}{k-1} \right) \right) > 0.$$

Таким образом, последовательность $\varepsilon(q^{(n)})$ возрастает и образует Δ -сеть на отрезке $[0, h - \frac{\Delta^{\alpha-1}}{k-1}]$. Отсюда, из $q^{(n)} \in K_{a,k(k-1)a^2,h}$ и $a \leq \Delta$ вытекает аппроксимируемость всех распределений с $\varepsilon \in [0, h]$ и $\delta_1 = \dots = \delta_{k-1} = 0$.

Итак, аппроксимированы распределения из отрезка, соединяющего распределение с $\varepsilon = 0$ и равномерное распределение ($\varepsilon = h$, $\delta_1 = \dots = \delta_{k-1} = 0$). Из этого факта и билинейности суммы распределений легко вывести, что вместе с любым аппроксимируемым распределением аппроксимируется и отрезок, соединяющий его с равномерным распределением.

9. Возможные обобщения

Помимо операций сложения и умножения в поле E 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, оставляющей на месте элемент $0 \in E$. Все построенные выше множества, сохраняемые сложением и умножением, сохраняются также перестановками, оставляющими на месте 0. Следовательно, они сохраняются операцией взятия противоположного элемента.

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

В проведенных построениях от операций сложения и умножения требовались далеко не все свойства, имеющиеся в поле. Конструкции остаются в силе, если на множестве E задать квазигрупповую операцию «сложения» с нейтральным элементом $0 \in E$, а также операцию «умножения», квазигрупповую на $E \setminus \{0\}$ и удовлетворяющую условию $0 \cdot x = x \cdot 0 = 0$ для всех $x \in E$. Такие структуры могут, в частности, содержать произвольное число элементов (а не только степень простого числа, как в случае поля).

Автор выражает благодарность О.М.Касим-Заде за внимание к работе и плодотворные обсуждения. Работа выполнена при поддержке РФФИ (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»).

Список литературы

1. Ашманов С. А., *Линейное программирование*, Наука, Москва, 1981, 340 с.
2. Колпаков Р. М., “Дискретные преобразования вероятностных распределений”, *Современные проблемы математики и механики Т. III Математика. Вып. 3. Дискретная математика*, ред. О. М. Касим-Заде, Изд-во МГУ, Москва, 2009, 35–50.
3. Схиртладзе Р. Л., “О синтезе p -схемы из контактов со случайными дискретными состояниями”, *Сообщ. АН ГрССР*, **26**:2 (1961), 181–186.
4. Схиртладзе Р. Л., “О методе построения булевой величины с заданным распределением вероятностей”, *Дискретный анализ*, 1966, № 7, 71–80.
5. Яшунский А. Д., “О преобразованиях распределений вероятностей бесповторными квазигрупповыми формулами”, *Дискретная математика*, **25**:2 (2013), 149–159.
6. Markovski S., Gligoroski D., Bakeva V., “Quasigroup String Processing: Part 1”, *Contributions, Sec. Math. Tech. Sci., MANU*, **XX**:1-2 (1999), 13–28.
7. Saloff-Coste L., “Random walks on finite groups”, *Probability on discrete structures. Encyclopaedia Math. Sci.*, 110., ред. Н. Kesten, Springer, Berlin, 2004, 263–346.

Статья поступила 27.02.2015.