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

Препринты ИПМ • Препринт № 11 за 2016 г.

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

Яшунский А.Д.

О выпуклых многогранниках распределений, сохраняемых операциями конечного поля

Рекомендуемая форма библиографической ссылки: Яшунский А.Д. О выпуклых многогранниках распределений, сохраняемых операциями конечного поля // Препринты ИПМ им. М.В.Келдыша. 2016. № 11. 10 с. doi:10.20948/prepr-2016-11
URL: http://library.keldysh.ru/preprint.asp?id=2016-11

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

А. Д. Яшунский

О выпуклых многогранниках распределений, сохраняемых операциями конечного поля

Москва — 2016

Яшунский А. Д.

О выпуклых многогранниках распределений, сохраняемых операциями конечного поля

Строятся семейства многогранников в пространстве вероятностных распределений над конечным полем, обладающих свойством сохранения: при сложении или умножении независимых случайных величин, имеющих распределение из построенного множества, распределение результата также лежит в этом множестве.

Ключевые слова: случайная величина, конечное поле, сохраняемое множество, выпуклый многогранник

Alexey Dmitrievich Yashunsky

On convex polytopes of distributions preserved by finite field operations

We construct families of polytopes in the space of probability distributions over a finite field, which are preserved, i.e. when adding or multiplying independent random variables with distributions from the constructed set, one obtains a result whose distribution belongs to the set as well.

Key words: random variable, finite field, preserved set, convex polytope

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»).

Рассмотрим преобразования случайных величин над конечным множеством E путем применения к ним операций из заданного множества операций $\mathcal{B}$. При рассмотрении таких преобразований, в частности, возникает вопрос о построении множества распределений вероятностей K, обладающего следующим свойством: для любого набора $X_1, \ldots, X_n$ независимых в совокупности случайных величин над E с распределениями из K и любой операции $f(x_1, \ldots, x_n) \in \mathcal{B}$ распределение величины $f(X_1, \ldots, X_n)$ лежит в K. В таких случаях будем говорить, что множество K *сохраняется* операциями из $\mathcal{B}$ (см. также [1, 2]). Обычно множество K строится для некоторого заданного множества *начальных* распределений G так, чтобы $G \subseteq K$.

В данной работе будет рассматриваться k-элементное множество E (далее для удобства считаем, что $E = \{0, 1, \ldots, k-1\}$, множество $E \setminus \{0\}$ будем обозначать E^*) и множество $\mathcal{B}$, состоящее из двух бинарных операций. Первая операция, обозначаемая $+$, является квазигрупповой операцией на E, для которой элемент $0 \in E$ является единицей[1], т. е. $0+i = i+0 = i$ для любого $i \in E$ (все необходимые определения см. в [3]). Вторая операция, обозначаемая $\times$, является квазигрупповой на E^* и, кроме того, удовлетворяет равенствам $0 \times i = i \times 0 = 0$ для любого $i \in E$. Примером множества с указанным набором операций может служить конечное поле порядка k, в котором операции $+$ и $\times$ — сложение и умножение соответственно.

Операции из $\mathcal{B}$, применяемые к независимым случайным величинам, естественным образом индуцируют операции на распределениях случайных величин (стохастических векторах): наборах $(x_0, x_1, \ldots, x_{k-1})$, удовлетворяющих условиям $x_i \geqslant 0, i \in E$ и $\sum\limits_{i \in E} x_i = 1$. Множество таких векторов образует симплекс, который будем называть *пространством распределений*. Будем обозначать операции, индуцированные операциями $+$ и $\times$, через $\oplus$ и $\otimes$. Несложно проверить, что для распределений $x = (x_0, x_1, \ldots, x_{k-1})$ и $y = (y_0, y_1, \ldots, y_{k-1})$ выполнены соотношения:

$$(x \oplus y)_i = \sum_{\substack{j \in E, \\ j+\ell = i}} x_j y_\ell, \ i \in E; \tag{1}$$

$$(x \otimes y)_0 = x_0 + y_0 - x_0 y_0 = x_0 + y_0(x_1 + \ldots + x_{k-1}); \tag{2}$$

$$(x \otimes y)_i = \sum_{\substack{j \in E^*, \\ j \times \ell = i}} x_j y_\ell, \ i \in E^*. \tag{3}$$

Отметим, что в силу квазигрупповых свойств операций $+$ и $\times$ в сум-

[1] Таким образом, $\langle E, + \rangle$ — лупа.

мах (1) и (3) индекс ℓ однозначно определяется по i и j.

Для построения множеств распределений, сохраняемых операциями $+$ и $\times$, докажем одно свойство квазигрупповых преобразований распределений. Пусть $Q = \{1, 2, \ldots, q\}$ — конечное множество, на котором задана бинарная квазигрупповая операция $*$, $\backslash$ — левая обратная операция к $*$, а $\circledast$ — индуцированная операцией $*$ операция на векторах распределений. Легко проверяются равенства:

$$(x \circledast y)_i = \sum_{j \in Q} x_j y_{j\backslash i},\ i \in Q. \tag{4}$$

Заметим, что для каждого $\ell \in Q$ отображение $i \mapsto \ell\backslash i$ определяет подстановку на множестве Q, обозначим ее σ_ℓ. Для распределения $x = (x_1, \ldots, x_q)$ и подстановки s под x^s будем понимать распределение $(x_{s(1)}, \ldots, x_{s(q)})$.

Напомним, что подмножество $K \subseteq \mathbb{R}^k$ называется *выпуклым*, если вместе с любыми двумя точками содержит соединяющий их отрезок, т. е. для любых $x, y \in K$ и $\alpha \in [0, 1]$ имеет место $\alpha x + (1 - \alpha)y \in K$.

Лемма 1. *Пусть K — такое выпуклое подмножество пространства распределений на Q, что для любого $\ell \in Q$ и любого $y \in K$ имеет место $y^{\sigma_l} \in K$. Тогда для любого $y \in K$ и произвольного распределения x выполнено $x \circledast y \in K$.*

Доказательство. Запишем равенство (4) в матричном виде:

$$((x \circledast y)_1, (x \circledast y)_2, \ldots, (x \circledast y)_q) = (x_1, x_2, \ldots, x_q) \begin{pmatrix} y_{1\backslash 1} & y_{1\backslash 2} & \cdots & y_{1\backslash q} \\ y_{2\backslash 1} & y_{2\backslash 2} & \cdots & y_{2\backslash q} \\ \vdots & & \ddots & \vdots \\ y_{q\backslash 1} & y_{q\backslash 2} & \cdots & y_{q\backslash q} \end{pmatrix}.$$

Легко заметить, что строки матрицы в точности равны векторам y^{σ_ℓ}, $\ell \in Q$. Следовательно, $x \circledast y = \sum\limits_{\ell \in Q} x_\ell y^{\sigma_\ell}$.

Из условия леммы вытекает, что при всех $\ell \in Q$ выполнено $y^{\sigma_\ell} \in K$. Так как $\sum\limits_{\ell \in Q} x_\ell = 1$ и $x_\ell \geqslant 0$, $\ell \in Q$, вектор $\sum\limits_{\ell \in Q} x_\ell y^{\sigma_\ell}$ является выпуклой комбинацией векторов y^{σ_ℓ} и, в силу выпуклости множества K, $x \circledast y \in K$. Лемма доказана. □

Лемма 1 позволяет строить множества распределений на E, сохраняемые операцией $+$, однако не может быть непосредственно применена для построения множеств, сохраняемых операцией $\times$, так как эта операция не является квазигрупповой на всем множестве E.

Лемма 2. *Пусть $Q = E^*$ — квазигруппа с операцией $\times$, и пусть σ_ℓ, $\ell \in Q$ — соответствующий этой квазигруппе набор подстановок, доопределенных на E: $\sigma_\ell(0) = 0$. Пусть K — такое выпуклое подмножество пространства распределений на E, что $(1, 0, \ldots, 0) \in K$ и для любого $\ell \in Q$ и любого $y \in K$ имеет место $y^{\sigma_\ell} \in K$. Тогда для любого $y \in K$ и произвольного распределения x выполнено $x \otimes y \in K$.*

Доказательство. Аналогично лемме 1 запишем равенства (2), (3) в матричном виде, используя подстановки σ_ℓ:

$$((x \otimes y)_0, (x \otimes y)_1, \ldots, (x \otimes y)_{k-1}) = (x_0, x_1, \ldots, x_{k-1}) \begin{pmatrix} 1 & 0 & \ldots & 0 \\ y_0 & y_{\sigma_1(1)} & \cdots & y_{\sigma_1(k-1)} \\ \vdots & \vdots & \ddots & \vdots \\ y_0 & y_{\sigma_{k-1}(1)} & \cdots & y_{\sigma_{k-1}(k-1)} \end{pmatrix}.$$

С учетом доопределения $\sigma_\ell(0) = 0$ получаем, что:

$$((x \otimes y)_0, (x \otimes y)_1, \ldots, (x \otimes y)_{k-1}) = x_0(1, 0, \ldots, 0) + \sum_{\ell \in Q} x_\ell y^{\sigma_\ell}.$$

Поскольку $\sum\limits_{i \in E} x_i = 1$ и $x_i \geqslant 0$, $i \in E$, вектор $x \otimes y$ является выпуклой комбинацией векторов $(1, 0, \ldots, 0)$ и y^{σ_ℓ}, $\ell \in Q$, которые по условию леммы лежат в K. В силу выпуклости K имеет место $x \otimes y \in K$. □

Докажем теперь теорему, описывающую класс выпуклых множеств, сохраняемых одновременно операциями $+$ и $\times$.

Теорема. *Пусть $\sigma_\ell^\times$, $\ell \in E^*$ — подстановки, определяемые квазигруппой $\langle E^*, \times \rangle$, доопределенные $\sigma_\ell^\times(0) = 0$; пусть σ_ℓ^+, $\ell \in E$ — подстановки, определяемые квазигруппой $\langle E, + \rangle$. Пусть G — такое множество распределений, что для любого $g \in G$ и любого $\ell \in E$ выполнено $g^{\sigma_\ell^\times} \in G$, $g^{\sigma_\ell^+} \in G$. Пусть K — выпуклая оболочка множества $G \cup \{(1, 0, \ldots, 0)\}$. Тогда для любых $x, y \in K$ имеет место $x \oplus y \in K$ и $x \otimes y \in K$.*

Доказательство. Покажем, что множество K сохраняется операцией $+$. Пусть K' — выпуклая оболочка множества G. Тогда множество K — выпуклая оболочка $K' \cup \{(1, 0, \ldots, 0)\}$.

Рассмотрим распределения $x, y \in K$. Тогда существуют такие $\alpha, \beta \in \in [0, 1]$, что $x = \alpha(1, 0, \ldots, 0) + (1 - \alpha)x'$ и $y = \beta(1, 0, \ldots, 0) + (1 - \beta)y'$, где $x', y' \in K'$. В силу билинейности операции $x \oplus y$ (см. (1)), а также $(1, 0, \ldots, 0) \oplus y' = y'$ и $(1, 0, \ldots, 0) \oplus x' = x'$, имеет место равенство:

$$\begin{aligned} x \oplus y &= (\alpha(1, 0, \ldots, 0) + (1 - \alpha)x') \oplus (\beta(1, 0, \ldots, 0) + (1 - \beta)y') = \\ &= \alpha\beta(1, 0, \ldots, 0) + \alpha(1 - \beta)y' + (1 - \alpha)\beta x' + (1 - \alpha)(1 - \beta)(x' \oplus y'). \end{aligned}$$

Множество K' удовлетворяет условиям леммы 1, поэтому $x' \oplus y' \in K'$. Тогда $x \oplus y$ — выпуклая комбинация векторов из $K' \cup \{(1, 0, \ldots, 0)\}$, и, следовательно, $x \oplus y \in K$.

Сохранение множества K операцией $\times$ вытекает непосредственно из леммы 2. Теорема доказана. □

Далее будем рассматривать задачу построения сохраняемого множества K, содержащего заданное начальное распределение g. Чтобы воспользоваться доказанной теоремой, требуется построить множество G, содержащее распределение g и при этом инвариантное относительно подстановок координат σ_ℓ^+ и $\sigma_\ell^\times$, $\ell \in E$. Легко видеть, что множество G можно выбрать конечным.

Обозначим через S группу подстановок, порожденную всеми подстановками $\sigma_\ell^+, \sigma_\ell^\times$, $\ell \in E$. Положим $G = \{g^s \mid s \in S\}$. Несложно видеть, что такое множество G содержит g и удовлетворяет условиям теоремы. Пусть далее $K(g)$ — выпуклая оболочка множества $G \cup \{(1, 0, \ldots, 0)\}$. Согласно теореме, $K(g)$ сохраняется операциями $+$ и $\times$. Легко видеть, что $g \in K(g)$, и $K(g)$ — многогранник, вершины которого принадлежат $G \cup \{(1, 0, \ldots, 0)\}$.

Утверждение 1. *Многогранник $K(g)$, содержащий заданное распределение g, имеет не более $|S| + 1$ вершин.*

Все распределения g^s являются вершинами так называемого перестановочного многогранника. В случае, когда все компоненты g различны, все распределения g^s также различны и, по следствию из результатов Радо [4], ни одно из них не принадлежит выпуклой оболочке остальных [5]. То есть многогранник K', являющийся выпуклой оболочкой множества G, имеет в точности $|S|$ вершин, и только при рассмотрении выпуклой оболочки множества $K' \cup \{(1, 0, \ldots, 0)\}$ количество вершин может стать меньше $|S|$.

Поскольку S содержит не более $k!$ элементов, имеет место

Утверждение 2. *Многогранник $K(g)$, содержащий заданное распределение g, имеет не более $k! + 1$ вершин.*

Отметим, что можно построить пример операций $+$ и $\times$, для которых группа S будет содержать все подстановки. Покажем это, определив специальным образом операцию $\times$.

Поскольку $\sigma_\ell^\times(i) = l \backslash i$, наборы значений $\sigma_\ell^\times(i)$, $\ell, i \in E^*$ фактически задают квазигрупповую операцию $\backslash$, являющуюся левой обратной к операции $\times$. Пусть на множестве E^* операция $\ell \backslash i$ для $\ell = 1, 2$ определена

следующим образом.

$\setminus$	1	2	3	4	...	$k-2$	$k-1$
1	2	1	3	4	...	$k-2$	$k-1$
2	1	3	4	5	...	$k-1$	2

Тогда, по теореме Холла [6], операцию $\setminus$ можно так доопределить для остальных $\ell \in E^*$, что она будет квазигрупповой операцией на E^*, которой соответствует (также квазигрупповая) операция $\times$. При этом легко проверить, что при выбранных значениях для $\sigma_1^\times(i)$ и $\sigma_2^\times(i)$ эти две подстановки порождают циклы $(1\,2)$ и $(1\,2\,\ldots\,k-1)$, а следовательно (см. [7]), и всю подгруппу подстановок, оставляющих на месте элемент $0 \in E$.

Заметим теперь, что, поскольку операция $+$ — квазигрупповая на множестве E, множество значений $\sigma_\ell^+(0)$, $\ell \in E$ совпадает с E. То есть для любого $j \in E$ среди подстановок σ_ℓ^+, $\ell \in E$ найдется такая, что $\sigma_\ell^+(0) = j$.

Покажем, что произвольная подстановка s порождается подстановками $\sigma_\ell^+, \sigma_\ell^\times$, $\ell \in E$. Пусть $s(0) = j$. Тогда существует такая подстановка $\tau = \sigma_\ell^+$, что $\tau(0) = j$. В силу выбора τ выполнено $(\tau^{-1}s)(0) = 0$, и, следовательно, $\tau^{-1}s$ выражается через построенные выше подстановки $\sigma_\ell^\times$, откуда вытекает, что s порождается набором подстановок $\sigma_\ell^+, \sigma_\ell^\times$, $\ell \in E$.

Итак, группа S может совпадать со всей группой подстановок на E. Вместе с тем специальные свойства операций $+$ и $\times$ могут существенно упростить структуру группы S и, как следствие, многогранника $K(g)$.

Пусть $+$ и $\times$ — сложение и умножение в поле. Тогда квазигруппы $\langle E, + \rangle$ и $\langle E^*, \times \rangle$ — группы порядков k и $k-1$ соответственно. Применение к элементу $i \in E$ подстановок $\sigma_\ell^\times$ соответствует умножению i на ℓ^{-1}, а подстановки из σ_ℓ^+ прибавляют $-l$ к i. В силу дистрибутивности умножения относительно сложения легко видеть, что любая последовательность таких преобразований сводится к одному умножению i на элемент поля и одному сложению в поле, откуда следует, что группа S содержит $k(k-1)$ элементов.

Утверждение 3. *Пусть операции $+$ и $\times$ — сложение и умножение в конечном поле порядка k. Тогда многогранник $K(g)$, содержащий заданное распределение g, имеет не более $k^2 - k + 1$ вершин.*

Ранее в работах автора [1, 2] уже строились множества, сохраняемые операциями $+$ и $\times$. Сравним построенные ранее семейства с теми, которые строятся в данной работе.

Ранее построенное семейство многогранников представляло собой пересечение пространства распределений с многогранниками, имеющими следующий набор вершин (их координаты зависят от параметра a, $0 \leqslant a \leqslant \frac{1}{k}$):

1. $(1, 0, \ldots, 0)$;
2. $(1/k - k(k-1)a^2, 1/k + ka^2, \ldots, 1/k + ka^2)$;
3. $(1/k, d_1, \ldots, d_{k-1})$,

где $d_1, \ldots, d_{k-1}$ — всевозможные такие наборы, в которых одно d_i, возможно, нулевое, а остальные равны $1/k \pm a$.

Эти многогранники вложены друг в друга, и каждое распределение, исключая те, что лежат на границе пространства распределений, может лежать на границе только одного многогранника. Для заданного распределения g без нулевых компонент, многогранник, на границе которого оно лежит, — минимальный среди многогранников семейства содержащий g.

Рассмотрим взаимное расположение сохраняемых множеств, в зависимости от распределения g, которое они содержат, на примере поля из трех элементов. На рисунках ниже изображено пространство распределений (x_0, x_1, x_2) в проекции на плоскость (x_1, x_2).

Черными сплошными линиями показаны границы пространства распределений, черными пунктирными линиями — оси симметрии этого пространства. Красным показан многоугольник «старой» серии, зеленым — многоугольник «новой» серии, построенный по распределению g, отмеченному зеленым кружочком, лежащему на границе многоугольника «старой» серии. Зеленым пунктиром отмечены стороны многоугольника K', не являющиеся сторонами многоугольника K.

В зависимости от положения распределения g «новый» многоугольник может быть расположен целиком внутри «старого» (рис. 1) или же наоборот — целиком содержать «старый» (рис. 2).

Наконец, при некоторых положениях распределения g «новый» и «старый» многоугольник имеют непустую симметрическую разность (рис. 3), что иллюстрирует, в определенном смысле, «независимость» построенных семейств сохраняемых множеств. При этом в случае, изображенном на рис. 3, пересечение «старого» и «нового» многоугольника дает еще одно сохраняемое множество распределений, не принадлежащее ни одному из построенных семейств.

Отметим, что ранее построенное семейство сохраняемых множеств покрывало не все пространство распределений, в отличие от «нового»

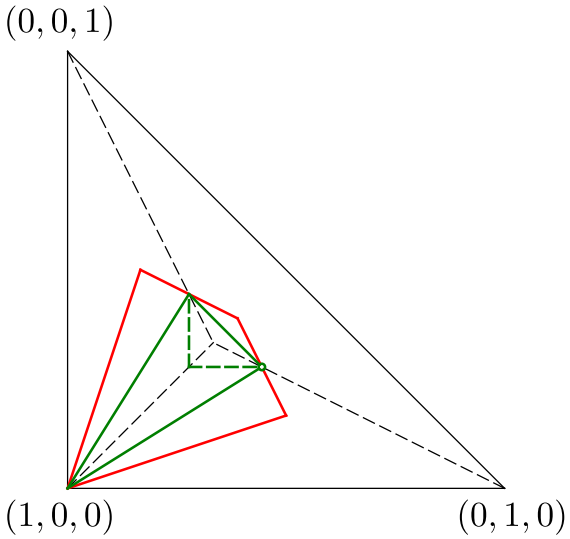

Рис. 1

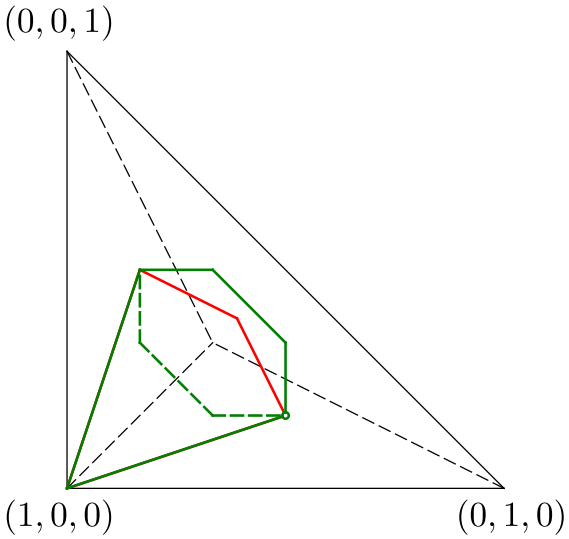

Рис. 2

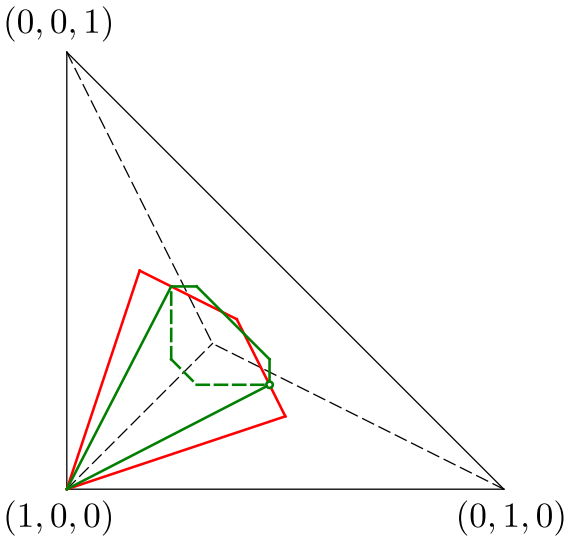

Рис. 3

семейства, многогранники которого могут содержать любое наперед заданное распределение.

Автор выражает глубокую признательность О. М. Касим-Заде за плодотворные обсуждения, способствовавшие написанию данной работы.

Список литературы

[1] Яшунский А. Д. О множествах распределений вероятностей, сохраняемых операциями конечного поля // Преприн-

ты ИПМ им. М. В. Келдыша. 2014. № 51. 20 с. URL: http://library.keldysh.ru/preprint.asp?id=2014-51

[2] Яшунский А. Д. О бесповторных преобразованиях случайных величин над конечными полями // Дискретная математика. 2015. Т. 27, № 3. С. 145–157. http://dx.doi.org/10.4213/dm1341

[3] Белоусов В. Д. Основы теории квазигрупп и луп. М.: Наука, 1967.

[4] Rado R. An inequality // J. London Math. Soc. 1952. Vol. 27. P. 1–6.

[5] Емеличев В. А., Ковалев М. М., Кравцов М. К. Многогранники, графы, оптимизация (комбинаторная теория многогранников). М.: Наука, 1981.

[6] Hall M. An existence theorem for latin squares // Bull. Amer. Math. Soc. 1945. Vol. 51, N6. P. 387–388.

[7] Калужнин Л. А., Сущанский В. И. Преобразования и перестановки. М.: Наука, 1979.