УДК 512.57+519.213

О НЕОБХОДИМЫХ УСЛОВИЯХ ПРЕДЕЛЬНЫХ ВЕРОЯТНОСТНЫХ ТЕОРЕМ В КОНЕЧНЫХ АЛГЕБРАХ

© 2020 г. А. Д. Яшунский^{1,*}

Представлено академиком РАН Б.Н. Четверушкиным 19.03.2020 г.

Поступило 20.03.2020 г.

После доработки 01.06.2020 г.

Принято к публикации 02.06.2020 г.

Рассматриваются условия, при которых в конечном множестве с заданной системой операций (конечной алгебре) выполняется предельная вероятностная теорема, а именно, произвольные вычисления с независимыми случайными величинами имеют распределения значений, стремящиеся к некоторому предельному распределению (предельному закону) с ростом количества случайных величин, участвующих в вычислении. Подобное поведение можно рассматривать как одно из обобщений центральной предельной теоремы, имеющей место для сумм непрерывных случайных величин. Показано, что наличие предельного вероятностного закона в конечной алгебре накладывает существенные ограничения на ее операции. В частности, за некоторыми геометрическими исключениями, наличие предельного закона без нулевых компонент влечет, что все операции алгебры — квазигрупповые, а предельное распределение — равномерное.

Ключевые слова: конечная алгебра, случайная величина, предельная теорема, квазигруппа, равномерное распределение

DOI: 10.31857/S2686954320040219

Изучение предельного поведения сумм случайных величин является одним из важных вопросов в теории вероятностей. Наиболее значимые результаты в этом направлении, собирательно известные как “центральная предельная теорема”, относятся к суммам действительных случайных величин. Вместе с тем известны обобщения предельных теорем на алгебраические структуры, отличные от аддитивной группы действительных чисел. Одно из естественных обобщений заключается в замене сложения произвольной групповой операцией на некотором множестве: примеры предельных теорем для различных континуальных групп можно найти в книге У. Гренандера [1]. Изучение алгебраических структур на конечных множествах (конечных алгебр) с точки зрения выполнения в них предельных вероятностных теорем не получило столь широкого распространения. Однако уже в работе Н.Н. Воробьева [2] рассматриваются предельные вероятностные теоремы для конечных абелевых групп. Обзор современного состояния исследований по предельным законам в конечных группах имеется в [3]. В настоящее время интерес к задачам об алгебра-

ических преобразованиях случайных величин и, в частности, о предельных свойствах таких преобразований связан с изучением вычислительных систем, построенных на вероятностных принципах [4, 5], а также с моделированием биологических систем [6]. Отметим также, что квазигрупповые преобразования случайных величин, особая роль которых вытекает из результатов настоящей работы, используются в криптографических системах [7].

В алгебрах с ассоциативной (и, в частности, групповой) операцией предельные теоремы могут быть доказаны путем моделирования последовательности сумм подходящей цепью Маркова. Если $X_1, \dots, X_n$ — независимые в совокупности одинаково распределенные случайные величины со значениями в некотором конечном множестве, то их “сумма” S_n , получающаяся применением к ним ассоциативной операции $*$, может быть представлена в виде

$$S_n = (\dots(((X_1 * X_2) * X_3) * X_4) * \dots) * X_n, \quad (1)$$

откуда, очевидно, $S_n = S_{n-1} * X_n$. Это позволяет рассматривать значения величины S_n как состояния конечной марковской цепи, матрица переходов которой может быть построена по распределению величин X_i . Если используемая операция групповая, то при некоторых естественных усло-

¹ Институт прикладной математики им. М.В. Келдыша
Российской академии наук, Москва, Россия

*E-mail: yashunsky@keldysh.ru

виях на распределения величин X_i выводится, что предельное распределение величин S_n при $n \rightarrow \infty$ является равномерным. В действительности, равномерность предельного распределения имеет место для более широкого класса операций. В работе [8] показано, что если операция $*$ в выражении (1) – квазигрупповая (определение см. в [7]), то предельное распределение также является равномерным при выполнении естественных ограничений на распределения случайных величин X_i . Этот результат сохраняется, даже если в (1) вместо одной квазигрупповой операции $*$ рассматривать несколько различных квазигрупповых операций, т.е. положить

$$S_n = (\dots(((X_1 *_{i_1} X_2) *_{i_2} X_3) *_{i_3} X_4) *_{i_4} \dots) *_{i_{n-1}} X_n, \quad (2)$$

где $*_{i_1}, *_{i_2}, \dots, *_{i_{n-1}}$ – какие-то квазигрупповые операции, определенные на множестве значений величин $X_1, \dots, X_n$. Дальнейшее усиление результатов [8] получено в [9], где показано, что на равномерность предельного распределения не влияет расстановка скобок в выражении (2). Поскольку квазигрупповые операции не обязательно ассоциативны, различные расстановки скобок в выражении (2) дают разные распределения для величин S_n , но все эти распределения приближаются к равномерному с ростом n . Таким образом, конечное множество с набором квазигрупповых операций является примером алгебры, в которой наличие предельного вероятностного закона обусловлено, в определенном смысле, алгебраическими свойствами этой системы.

Отметим, что подобная ситуация имеет место далеко не всегда: имеются примеры конечных алгебр, в которых различные последовательности выражений со случайными величинами стремятся к разным предельным законам. В частности, в работе [4] приведены примеры алгебр на двухэлементном множестве, в которых можно строить последовательности выражений с растущим числом независимых случайных величин, распределения которых стремятся к любому наперед заданному распределению. То есть в таких алгебрах любое распределение может являться предельным – фактически имеет место явление, по смыслу противоположное предельным вероятностным теоремам.

В любой алгебре можно строить последовательности выражений, аналогичных (1), содержащих растущее число независимых случайных величин. При этом класс последовательностей выражений, допускающих моделирование цепями Маркова, достаточно широк: он включает, в том числе, выражения, в которых не все операции бинарные. Для каждой такой последовательности выражений анализ соответствующей марковской цепи позволяет установить предельный закон, если он существует, однако, как было упомянуто

ранее, в рамках одной и той же системы различные последовательности могут приводить к различным предельным законам.

Несомненный интерес представляет выявление таких алгебр, в которых любая последовательность выражений с растущим числом случайных величин стремится к одному и тому же предельному закону, зависящему от рассматриваемой системы операций, но не зависящему от конкретной рассматриваемой последовательности. Необходимые условия наличия предельного вероятностного закона в конечной алгебре устанавливаются в данной работе.

1. ОСНОВНЫЕ РЕЗУЛЬТАТЫ

Формализуем наличие предельного закона в конечной алгебре. Будем рассматривать конечные алгебры на множестве $E_k = \{0, 1, \dots, k-1\}$ с набором операций B . Без ограничения общности можно считать, что у всех операций из набора B все переменные существенные (напомним, что переменная x_i операции $f(x_1, \dots, x_n): E_k^n \rightarrow E_k$ существенная, если найдутся такие значения $a_1, \dots, a_n, b \in E_k$, что

$$f(a_1, \dots, a_{i-1}, a_i, a_{i+1}, \dots, a_n) \neq f(a_1, \dots, a_{i-1}, b, a_{i+1}, \dots, a_n).$$

Распределения случайных величин на множестве E_k являются k -мерными действительными векторами $(p_0, \dots, p_{k-1})$, координаты которых дополнительно удовлетворяют условиям $p_i \geq 0$,

$i = 0, \dots, k-1$ и $\sum_{i=0}^{k-1} p_i = 1$. Множество таких векторов, являющееся $(k-1)$ -мерным симплексом в k -мерном пространстве $\mathbb{R}^k$, будем обозначать $S^{(k)}$. Равномерное распределение на E_k – вектор $(\frac{1}{k}, \dots, \frac{1}{k})$.

Будем говорить, что множество распределений $H \subseteq S^{(k)}$ замкнуто относительно преобразований операциями из B , если при подстановке вместо всех переменных любой операции $f \in B$ независимых в совокупности случайных величин с распределениями из H получается случайная величина, распределение которой также лежит в H .

Рассмотрим всевозможные вычисления над системой операций B , в которых все аргументы – независимые в совокупности случайные величины с распределениями из некоторого конечного множества $G \subseteq S^{(k)}$. Тогда распределения результатов этих вычислений, очевидно, будут образовывать множество H , содержащее G и замкнутое относительно преобразований операциями из B . Наличие предельного закона в алгебре с набором операций B , а именно, приближению распределе-

ний результатов случайных вычислений к некоторому пределу с ростом числа аргументов, будет в точности соответствовать наличие у множества H единственной предельной точки q , т.е. точки, в любой проколотовой окрестности которой содержатся элементы множества H . Эта предельная точка q и будет предельным законом для рассматриваемой конечной алгебры. Априори предельный закон зависит не только от операций конечной алгебры, но и от выбора множества G , однако во многих случаях этой зависимости в действительности нет.

Для формулировки основного результата нам также потребуются следующие понятия. Напомним, что аффинной оболочкой множества $H \subseteq S^{(k)} \subseteq \mathbb{R}^k$ называется множество:

$$\text{Aff}(H) = \left\{ \sum_{i=1}^s \alpha_i h_i \mid h_1, \dots, h_s \in H, \right. \\ \left. \alpha_1, \dots, \alpha_s \in \mathbb{R}, \sum_{i=1}^s \alpha_i = 1 \right\}.$$

Определение 1. Множество распределений $H \subseteq S^{(k)}$ называется существенно неплоским, если для любого конечного подмножества $H' \subseteq H$ выполнено $\text{Aff}(H \setminus H') \supseteq S^{(k)}$ и существенно плоским в противном случае.

Определение 2. Множество распределений $H \subseteq S^{(k)}$ называется X -множеством, если H представляется в виде $H = H_1 \cup H_2$, где

$$\text{Aff}(H_1) \not\supseteq S^{(k)} \quad \text{и} \quad \text{Aff}(H_2) \not\supseteq S^{(k)}.$$

Определение 3. Для заданного подмножества $Q \subseteq E_k$ n -арная операция $f(x_1, \dots, x_n)$ на множестве E_k называется Q -поглощающей квазигрупповой, если для любого $i = 1, \dots, n$ и любых $a_1, \dots, a_{n-1} \in E_k$ унарная операция

$$\varphi(x) = f(a_1, \dots, a_{i-1}, x, a_i, \dots, a_{n-1})$$

является перестановкой на множестве Q и определена произвольным образом на $E_k \setminus Q$. Все нульарные операции по определению считаются Q -поглощающими квазигрупповыми операциями для любого множества Q .

Частным случаем Q -поглощающей квазигрупповой n -арной операции при $Q = E_k$ являются n -арные квазигрупповые операции в обычном понимании этого термина (см. [7]).

Конечные алгебры, обладающие некоторым предельным вероятностным законом, характеризуются следующей теоремой.

Теорема. Если множество распределений H замкнуто относительно преобразований операция-

ми из V и при этом имеет единственную предельную точку $q \in S^{(k)}$, то выполнено одно из следующих утверждений:

1) либо H является существенно плоским;

2) либо H является X -множеством;

3) либо существует такое $Q \subseteq E_k$, что все операции из V являются Q -поглощающими квазигрупповыми операциями, и если не все операции из V унарные, то распределение $q = (q_0, \dots, q_{k-1})$ удовлетворяет условиям

$$q_i = \frac{1}{|Q|} \quad \text{при} \quad i \in Q,$$

$$q_i = 0 \quad \text{при} \quad i \in E_k \setminus Q.$$

В частности, из теоремы вытекает, что если некоторое множество распределений замкнуто относительно операций конечной алгебры, содержащей неунарные операции, не является ни существенно плоским, ни X -множеством и при этом имеет единственную предельную точку без нулевых компонент, то все операции этой алгебры необходимо являются n -арными квазигрупповыми операциями, а само предельное распределение – равномерное на множестве E_k .

Эта теорема обобщает ранее полученный результат для случая $k = 2$, характеризующий алгебры на множестве $\{0, 1\}$, обладающие предельным вероятностным законом [10].

СПИСОК ЛИТЕРАТУРЫ

1. Гренандер У. Вероятности на алгебраических структурах. М.: Наука, 1965. 271 с.
2. Воробьев Н.Н. // Матем. сб. 1954. Т. 34 (76). № 1. С. 89–126.
3. Saloff-Coste L. / In: Probability on discrete structures. H. Kesten (Ed.) Encyc. Math. Sci. V. 110. Berlin: Springer, 2004. P. 263–346.
4. Qian W., Riedel M.D., Zhou H., Bruck J. // IEEE Trans. CAD Integrated Circuits and Systems. 2011. V. 30. № 9. P. 1279–1292.
5. Lee D.T., Bruck J. // IEEE Trans. Comp. 2015. V. 64. № 12. P. 3376–3388.
6. Wilhelm D., Bruck J., Qian L. // Proc. Nat. Acad. Sci. USA. 2018. V. 115 (5). P. 903–908.
7. Markovski S. // Quasigroups and Related Systems. 2015. V. 23. № 1. P. 41–90.
8. Markovski S., Gligoroski D., Bakeva V. // Proc. Maked. Acad. Sci. and Arts for Math. and Tech. Sci. 1999. V. 20. P. 13–28.
9. Яшунский А.Д. // Дискрет. матем. 2013. Т. 25. № 2. С. 149–159.
10. Яшунский А.Д. // Вестн. Моск. ун-та. Сер. 1. Матем., мех. 2019. № 4. С. 3–9.

ON NECESSARY CONDITIONS OF PROBABILITY LIMIT THEOREMS IN FINITE ALGEBRAS

A. D. Yashunsky^a

^a *Keldysh Institute of Applied Mathematics of Russian Academy of Sciences, Moscow, Russian Federation*

Presented by Academician of the RAS B.N. Chetverushkin

We consider the conditions for a finite set with a given system of operations (a finite algebra) to be subject to a probability limit theorem, i.e. arbitrary computations with mutually independent random variables have value distributions that tend to a certain limit (the limit law) as the number of random variables used in the computation grows. Such behavior may be seen as a generalization of the central limit theorem that holds for sums of continuous random variables. We show that the existence of a limit probability law in a finite algebra has strong implications for its set of operations. In particular, some geometric exceptions excluded, the existence of limit law without zero components implies that all operations in the algebra are quasigroup operations and the limit law is uniform.

Keywords: finite algebra, random variable, limit theorem, quasigroup, uniform distribution