

МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
имени М. В. ЛОМОНОСОВА

На правах рукописи

Яшунский Алексей Дмитриевич

**Исследования по теории
итеративных систем, порождаемых
конечными случайными величинами.**

**Арифметический и
комбинаторно-логический подход**

01.01.06 — математическая логика, алгебра и теория чисел

АВТОРЕФЕРАТ

**диссертации на соискание ученой степени
доктора физико-математических наук**

Москва — 2021

Работа выполнена в Федеральном государственном учреждении «Федеральный исследовательский центр Институт прикладной математики им. М.В. Келдыша Российской академии наук».

Официальные оппоненты: **Аблаев Фарид Мансурович**
доктор физико-математических наук, профессор,
член-корреспондент Академии наук Республики
Татарстан, Казанский (Приволжский)
федеральный университет, заведующий кафедрой
теоретической кибернетики
Малышев Вадим Александрович,
доктор физико-математических наук, профессор,
ФГБОУ ВО Московский государственный
университет имени М.В. Ломоносова,
механико-математический факультет, кафедра
теории вероятностей, главный научный
сотрудник
Черемушкин Александр Васильевич,
доктор физико-математических наук, профессор,
член-корреспондент Академии криптографии
Российской Федерации

Защита диссертации состоится «24» сентября 2021 г. в 16 ч. 45 м. на заседании диссертационного совета МГУ.01.17 при Московском государственном университете имени М.В. Ломоносова по адресу: Российская Федерация, 119234, Москва, ГСП-1, Ленинские горы, д.1, МГУ, Механико-математический факультет, аудитория 14-08.

E-mail: VGChdissovet@yandex.ru

С диссертацией, а так же со сведениями о регистрации участия в удаленном интерактивном режиме защиты можно ознакомиться на сайте ИАС «Истина» <https://istina.msu.ru/dissertations/364891994/>

Автореферат разослан «24» июля 2021 г.

Ученый секретарь диссертационного
совета МГУ.01.17 при МГУ
доктор физико-математических наук,
доцент

В. Г. Чирский

Общая характеристика работы

Актуальность темы и степень ее разработанности

Изучение преобразований конечных случайных величин находится на стыке нескольких областей математических исследований. Подобные вопросы можно рассматривать как с позиций теории вероятностей, так и с позиций дискретной математики, при этом многие из полученных к настоящему моменту результатов имеют, по сути, арифметическую природу и формулируются как свойства некоторых числовых множеств. Исторически наибольшее внимание задачам дискретных преобразований конечных случайных величин уделялось в рамках дискретной математики и теоретической информатики, однако во многих случаях продвижение в этих задачах обеспечивалось применением арифметических и комбинаторно-логических методов.

Понятие «преобразователя вероятности» как некоторого детерминированного устройства, получающего на входе значения случайных величин и осуществляющего вычисления с ними, тем самым генерируя новые случайные величины с иными распределениями, регулярно возникает в практических и теоретических исследованиях. Чаще всего речь идет о преобразованиях булевых случайных величин¹, принимающих значения 0 и 1, в двоичных устройствах.

Рассматриваемые преобразователи случайных величин можно условно разделить на два класса. К первому относятся преобразователи, работающие с потенциально бесконечной последовательностью входных величин: это могут быть как преобразования последовательностей конечными автоматами (начиная с работы А. Гилла²), так и общие алгоритмы преобразования случайных последовательностей (начиная с работы Дж. фон Неймана³). С прикладной точки зрения наиболее востребована, по-видимому, задача получения из произвольной случайной или псевдо-случайной последовательности равномерно распределенных случайных величин. Имеющиеся результаты в этой области, называемой «извле-

¹Также называемых «бернуллиевскими».

²Gill A. Synthesis of probability transformers // J. Franklin Inst. 1962. Vol. 274, no. 1. P. 1–19.

³von Neumann J. Various techniques used in connection with random digits // Appl. Math. Ser., Notes by G.E. Forstyle, Nat. Bur. Stand. 1951. Vol. 12. P. 36–38.

чение случайности» («randomness extraction») приведены в обзоре Р. Шалтиеля⁴.

Второй класс рассматриваемых преобразователей не предполагает обработки потенциально бесконечной последовательности случайных величин, а оперирует в каждом преобразовании с некоторым конечным набором случайных величин. Различные постановки задач, приводящие к рассмотрению подобных преобразователей, можно объединить, введя понятие системы случайных величин, порождаемой некоторым набором операций и заданной последовательностью случайных величин. В такой системе, далее называемой *итеративной системой случайных величин*, новые случайные величины получаются путем применения к исходным случайным величинам различных комбинаций имеющихся операций.

Исследования подобных систем случайных величин, принимающих значения в произвольных конечных множествах (далее *конечных случайных величин*), в частности, мотивированы задачами синтеза вероятностных автоматов (см. обзор Р.Г. Бухараева⁵), а также криптографическими приложениями (см., например, обзор В.А. Щербакова⁶) и вероятностными вычислениями. К последним относится как построение вычислительных устройств на вероятностных принципах (например, Л. Чакрапани и др.⁷), востребованное в автономных системах с ограниченными ресурсами, так и моделирование некоторых естественных систем, — см., например, работу Д. Вильгельма, Дж. Брака и Л. Киан⁸ о «биологических» вычислительных системах.

Несмотря на очевидную вероятностную составляющую задачи, она оказалась практически вне поля зрения исследователей, занимающихся непосредственно теорией вероятностей. Так, например, в монографии У. Гренандера «Вероятности на алгебраических

⁴Shaltiel R. An Introduction to Randomness Extractors // Automata, Languages and Programming. ICALP 2011. Aceto L., Henzinger M., Sgall J. (eds.) LNCS V. 6756. Springer, Berlin, Heidelberg. P. 21–41.

⁵Бухараев Р. Г. Вероятностные автоматы // Итоги науки и техн. Сер. Теор. вероятн. Мат. стат. Теор. кибернет. 1978. Т. 15. С. 79–122.

⁶Şcerbacov V. Quasigroups in cryptology // Comp. Sci. J. of Moldova. 2009. Vol. 17, No 2 (50). P. 193–228.

⁷Chakrapani L., Korkmaz P., Akgul B., Palem K. Probabilistic system-on-a-chip architecture // ACM Trans. on Design Automation of Electronic Systems. 2007. 12(3). P. 1–28.

⁸Wilhelm D., Bruck J., Qian L. Probabilistic Switching Circuits in DNA // Proc. Nat. Acad. Sci. U.S.A. 2018. Vol. 115. P. 903–908.

структурах»⁹ рассматриваются практически только случайные величины с континуальными множествами значений: упоминания о конечных случайных величинах единичны и лишь иллюстрируют свойства, установленные для континуальных алгебраических структур.

Анализ и построение преобразователей конечных случайных величин порождают целый ряд задач, среди которых, в частности, присутствуют значимые с прикладной точки зрения вопросы об устойчивости преобразователей к колебаниям вероятностей аргументов и построение управляемого генератора вероятностей, однако центральным вопросом оказывается, собственно, описание множеств случайных величин, реализуемых в различных системах.

Для обзора имеющихся результатов введем ряд понятий и обозначений. Будем считать, что конечная случайная величина X , принимающая значения из множества $E_k = \{0, 1, \dots, k-1\}$, имеет распределение $P(X) = \mathbf{p} = (p_0, \dots, p_{k-1})$, где $p_i, i \in E_k$, — вероятность обращения X в i . Совокупность распределений на E_k образует в $\mathbb{R}^k$ $(k-1)$ -мерный симплекс, обозначаемый $S^{(k)}$. Носителем $\mu(\mathbf{p})$ распределения $\mathbf{p} \in S^{(k)}$ называется множество $\{i \in E_k \mid p_i > 0\} \subseteq E_k$. Для некоторых распределений введем специальные обозначения, положив $\mathbf{e}^{(0)} = (1, 0, \dots, 0)$, $\mathbf{e}^{(1)} = (0, 1, 0, \dots, 0)$, ..., $\mathbf{e}^{(k-1)} = (0, \dots, 0, 1)$, и $\mathbf{u} = (\frac{1}{k}, \dots, \frac{1}{k})$. Обозначим множество n -местных функций на E_k через $P_k(n)$ и положим $P_k = \bigcup_{n=0}^{\infty} P_k(n)$.

Для заданного множества функций $B \subseteq P_k$ и набора независимых в совокупности случайных величин $\mathcal{X}_0$, принимающих значения из E_k , порождаемую итеративную систему случайных величин определим как объединение $\mathcal{X} = \bigcup_{n=1}^{\infty} \mathcal{X}_n$ множеств $\mathcal{X}_n$ случайных величин, выражимых над B бесповторными термами (в которых каждая переменная встречается не более одного раза), содержащими ровно n случайных аргументов из $\mathcal{X}_0$.

Чаще всего предполагается, что порождающее итеративную систему множество случайных величин $\mathcal{X}_0$ бесконечно, однако в

⁹Гренандер У. Вероятности на алгебраических структурах. М.: Мир, 1965.

некоторых работах (Н. Н. Нурмеев¹⁰, а также М. Д. Ридель и др.¹¹) рассматриваются итеративные системы, порождаемые конечным множеством $\mathcal{X}_0$. Наиболее распространены постановки задач, в которых множество $\mathcal{X}_0$ имеет вид $\{X_{i,g}\}_{i \in \mathbb{N}, g \in G}$, где G — некоторое заданное множество *начальных распределений*, и при этом для всех $i \in \mathbb{N}$, $g \in G$ выполнено $P(X_{i,g}) = g$. В дальнейшем мы будем рассматривать итеративные системы случайных величин, порождаемые именно такими наборами $\mathcal{X}_0$, и обозначать их $\mathcal{X}(G, B)$.

Для заданной системы $\mathcal{X} = \mathcal{X}(G, B)$ **задача выразимости** случайных величин, заключается в описании множества распределений $\{P(X) \mid X \in \mathcal{X}\}$. Введя на множестве распределений $S^{(k)}$ метрику (будем использовать метрику $\rho(g, h) = \sum_{i=0}^{k-1} |g_i - h_i|$), можно также рассматривать для системы $\mathcal{X}$ **задачу аппроксимируемости** случайных величин по распределению. Она заключается в описании всех таких случайных величин Y со значениями в E_k , что для любого $\varepsilon > 0$ найдется случайная величина $X \in \mathcal{X}$, удовлетворяющая $\rho(P(X), P(Y)) < \varepsilon$.

Множества распределений случайных величин, выразимых или аппроксимируемых в итеративной системе $\mathcal{X}(G, B)$, можно описать как классы распределений, замкнутые относительно преобразований, связанных с операциями из системы B . Каждой функции $f(x_1, \dots, x_n) \in P_k(n)$ поставим в соответствие *индуцированную* вектор-функцию $\hat{f}(\mathbf{p}^{(1)}, \dots, \mathbf{p}^{(n)}): (S^{(k)})^n \rightarrow S^{(k)}$, вычисляющую по распределениям $\mathbf{p}^{(1)}, \dots, \mathbf{p}^{(n)} \in S^{(k)}$ независимых в совокупности случайных величин $X_1, \dots, X_n$ распределение случайной величины $f(X_1, \dots, X_n)$. Класс распределений $H \subseteq S^{(k)}$ *замкнут* относительно системы индуцированных функций $\hat{B} = \{\hat{f} \mid f \in B\}$, если для любых распределений $\mathbf{h}^{(1)}, \dots, \mathbf{h}^{(n)} \in H$ и любой функции $f(x_1, \dots, x_n) \in B$ выполнено $\hat{f}(\mathbf{h}^{(1)}, \dots, \mathbf{h}^{(n)}) \in H$. Наименьший по включению класс распределений, замкнутый относительно $\hat{B}$ и содержащий заданное множество G , будем обозначать $V_B(G)$.

¹⁰Нурмеев Н. Н. О булевых функциях с аргументами, принимающими случайные значения // Проблемы теоретической кибернетики. Тез. докл. VIII Всесоюзной конференции. Горький, 1988. Часть 2. С. 59–60.

¹¹Qian W., Riedel M.D., Barzagan K., Lilja D. The Synthesis of Combinational Logic to Generate Probabilities // Proc. Int'l Conf. Computer-Aided Design, 2009. P. 367–374.

Этот класс распределений оказывается¹² в точности совпадающим с множеством распределений случайных величин, входящих в итеративную систему $\mathcal{X}(G, B)$. При этом множество распределений случайных величин аппроксимируемых над системой $\mathcal{X}(G, B)$ будет совпадать с топологическим замыканием множества $V_B(G)$ (т. е. с результатом добавления в него всех его предельных точек): обозначим его $W_B(G)$. Таким образом, задачи выразимости и аппроксимируемости случайных величин в итеративных системах $\mathcal{X}(G, B)$ сводятся к исследованию структуры классов распределений, замкнутых относительно операторов V_B и W_B .

Операторы замыкания V_B и W_B можно рассматривать с точностью до *бесповторного замыкания* системы B (совокупности функций, выразимых бесповторными термами над B), обозначаемого $[B]_0$, поскольку выполнено $V_B(G) = V_{[B]_0}(G)$ и $W_B(G) = W_{[B]_0}(G)$. Среди бесповторно замкнутых классов функций содержатся, в частности, *замкнутые по суперпозиции*¹³ классы функций (*клоны*).

Задача выразимости рассматривалась в основном для случайных величин с рациональными распределениями, т. е. исследовались замкнутые подклассы распределений в множестве $S^{(k)} \cap \mathbb{Q}^k$, обозначаемом далее $SQ^{(k)}$. Эти подклассы оказываются связанными с факторизацией компонент вероятностных распределений, и по своей сути являются арифметическими.

При исследовании выразимости случайных величин с рациональными распределениями одним из центральных вопросов (в том числе и из прикладных соображений) была *конечная порожденность* классов случайных величин с распределениями из множества H в итеративных системах $\mathcal{X}(G, B)$, понимаемая как существование такого *конечного* множества $G \subseteq SQ^{(k)}$, что $V_B(G) = H$.

Наиболее исследована задача выразимости булевых случайных величин. Их распределения (называемые *бернуллиевскими*) полностью определяются одной из своих компонент, т. е. имеется взаимно однозначное соответствие между $S^{(2)}$ и отрезком $[0; 1]$. Традиционно оно устанавливается сопоставлением каждому бернуллиевскому распределению вероятности обращения случайной величины в единицу. Функции, индуцированные булевыми, можно в све-

¹²Соответствующее утверждение доказывается в диссертации как Теорема 1.28 и ее следствия, но присутствует в неявном виде в работах многих других исследователей.

¹³Замыкание по суперпозиции системы $B \subseteq P_k$ обозначается далее $[B]$.

те этого соответствия рассматривать как действующие на отрезке $[0; 1]$ и, говоря о преобразованиях бернуллиевских распределений, понимать их как преобразования чисел из отрезка $[0; 1]$. Классы бернуллиевских распределений G естественно понимать как подмножества отрезка $[0; 1]$, т. е. множества чисел.

Важную роль в структуре замкнутых классов рациональных бернуллиевских распределений играют множества дробей, у которых все делители знаменателей принадлежат некоторому множеству $R \subseteq \mathbb{N}$, они обозначаются¹⁴ далее $\Gamma[R]$. Для R , состоящего из простых чисел, выполнено $V_{P_2}(\Gamma[R]) = \Gamma[R]$, однако, как показал Ф. И. Салимов¹⁵ в общем случае $\Gamma[R]$ могут быть незамкнутыми относительно V_{P_2} . Им же установлена¹⁶ структура решетки классов $\Gamma[R]$ и условия их конечной порожденности относительно V_{P_2} . Помимо $\Gamma[R]$ в решетку классов рациональных бернуллиевских распределений, замкнутых относительно V_{P_2} , входят некоторые их подмножества, определяемые арифметическими соотношениями между числителями и знаменателями дробей. Эти классы, их решетка и условия конечной порожденности относительно V_{P_2} описаны Р. М. Колпаковым¹⁷.

Для систем, порождаемых набором функций $B \neq P_2$, практически все имеющиеся результаты относятся к конечной порожденности классов $\Gamma[R]$: они могут оказаться бесконечно порожденным относительно V_B даже в случае, если порождались конечным множеством относительно V_{P_2} . Среди различных систем булевых функций, отличных от P_2 , наибольшее внимание уделялось системе¹⁸ $\{\&, \vee\}$, что обусловлено ее связью с параллельно-последовательными контактными схемами. Р. Л. Схиртладзе установил¹⁹ конечную порожденность $\Gamma[2]$ и $\Gamma[3]$ относительно $V_{\{\&, \vee\}}$.

¹⁴В случае конечного $R = \{r_1, \dots, r_s\}$ будем писать $\Gamma[r_1, \dots, r_s]$, опуская фигурные скобки.

¹⁵Салимов Ф. И. Об одном семействе алгебр распределений // Изв. вузов. Сер. Математика. 1988. № 7. С. 64–72.

¹⁶Там же.

¹⁷Колпаков Р. М. О преобразованиях булевых случайных величин // Математические вопросы кибернетики. Вып. 9. М.: Наука, 2000. С. 227–252; Колпаков Р. М. Замкнутые классы булевых случайных величин с рациональнозначными распределениями // Математические вопросы кибернетики. Вып. 10. М.: Наука, 2001. С. 215–224.

¹⁸Здесь и далее символ $\&$ обозначает конъюнкцию, $\vee$ — дизъюнкцию, $\neg$ — отрицание, c_0 и c_1 — константные функций со значением 0 и 1 соответственно.

¹⁹Схиртладзе Р. Л. О синтезе p -схемы из контактов со случайными дискретными состояниями //

Р. М. Колпаков доказал²⁰ конечную порожденность $\Gamma[r_1, \dots, r_s]$ относительно $V_{\{\&, \vee\}}$ для всех наборов $r_1, \dots, r_s$ из $s \geq 2$ простых чисел.

Проблема конечной порожденности множеств $\Gamma[r]$ остается открытой для простых $r > 3$ относительно $V_{\{\&, \vee\}}$, но решена для некоторых более сильных операторов. Ф. И. Салимов установил²¹ конечную порожденность $\Gamma[r]$ для простых r относительно оператора V_B для системы $B = \{(x_1 \& x_2) \vee (\neg(x_1) \& x_3), c_0, c_1\}$. Р. М. Колпаков построил²² в классе функций, реализуемых неповторными контактными схемами, такие системы B , что классы $\Gamma[5]$ и $\Gamma[7]$ конечно порождены относительно V_B . Им же предложена²³ подсистема B клонна $[\{\&, \vee\}]$, не входящая в множество функций, реализуемых неповторными контактными схемами, такая что $\Gamma[r]$ конечно порождено относительно V_B для всех простых r .

Часть результатов о выразимости и конечной порожденности, полученных для классов рациональных бернуллиевских распределений, переносится на распределения из классов $SQ^{(k)}$ при $k > 2$. Классы бернуллиевских распределений $\Gamma[R]$ естественным образом обобщаются до классов $\Gamma^{(k)}[R]$ рациональных распределений, у которых все делители знаменателей каждой из компонент принадлежат R . Ф. И. Салимов показал²⁴, что если R содержит только простые числа, то классы $\Gamma^{(k)}[R]$ замкнуты относительно V_{P_k} , и являются конечно порожденными, если R конечно. Окончательное описание всей решетки замкнутых относительно V_{P_k} классов рациональных распределений и условия их конечной порожденности установлены Р. М. Колпаковым²⁵.

Сообщ. АН Груз. ССР. 1961. Т. 26, № 2. С. 181–186.

²⁰Колпаков Р. М. О порождении некоторых классов рациональных чисел π -сетями // Вестник МГУ. Серия 1. Математика. Механика. 1991. № 2. С. 27–30.

²¹Салимов Ф. И. Об одной системе образующих для алгебр над случайными величинами // Изв. вузов. Матем. 1981. № 5. С. 78–82.

²²Колпаков Р. М. О порождении рациональных чисел вероятностными контактными сетями // Вестник МГУ. Серия 1. Математика. Механика. 1992. № 5. С. 46–52.

²³Колпаков Р. М. О порождении рациональных чисел монотонными функциями // Теоретические и прикладные аспекты математических исследований: Сб. науч. тр. М.: Изд-во Моск. ун-та, 1994. С. 13–17.

²⁴Салимов Ф. И. Конечная порожденность некоторых алгебр над случайными величинами // Вопросы кибернетики. № 86. М., 1982. С. 122–130.

²⁵Колпаков Р. М. Замкнутые классы конечных распределений рациональных вероятностей // Дискретный анализ и исследование операций. 2004. Т. 11, № 3. С. 16–31.

Для рациональных распределений на произвольном конечном множестве почти не рассматривались итеративные системы случайных величин с набором операций, отличным от P_k . Практически единственным исключением оказывается обобщение булевых систем с операциями $\{\&, \vee\}$, рассматривавшееся в работе Д. Ли и Дж. Брака²⁶. В ней для линейного порядка $0 < 1 < \dots < k-1$ на множестве E_k вводятся операции минимума $\wedge$ и максимума $\vee$, обобщающие булевы функции $\&$ и $\vee$ соответственно. Показано, что относительно оператора $V_{\{\wedge, \vee\}}$ все распределения из класса $\Gamma^{(k)}[r]$, где r — произвольное (не обязательно простое), порождаются множеством распределений $G = \{e^{(0)}, \dots, e^{(k-1)}\} \cup \{(\frac{t-1}{t}, 0, \dots, 0, \frac{1}{t}) \mid t = 2, \dots, r\}$.

Задача выразимости рассматривалась в основном для случайных величин с рациональными распределениями. Исключениями являются работа Н. Н. Нурмеева²⁷ где анонсированы некоторые результаты о распределениях из $V_{P_2}(\{p\})$ для произвольного распределения $p \in S^{(2)}$, а также работы М. Д. Риделя и др.²⁸ и Дж. Брака и др.²⁹, где решается задача поиска распределения p , удовлетворяющего $V_{P_2}(\{p\}) \supseteq \Gamma[R]$ для заданного $R \subset \mathbb{N}$.

Результаты, которые можно отнести к задаче об аппроксимируемости случайных величин в итеративных системах, существенно менее многочисленны, чем результаты о выразимости случайных величин с рациональными распределениями. Часть результатов, фактически относящихся к задаче аппроксимируемости, была получена при исследованиях в других областях математики.

Один из первых результатов, касающихся аппроксимируемости случайных величин, был получен Р. Л. Схиртладзе³⁰. Он показал, что для любого бернуллиевского распределения $p \in S^{(2)} \setminus \{e^{(0)}, e^{(1)}\}$ вы-

²⁶Lee D., Bruck J. Generating Probability Distributions using Multivalued Stochastic Relay Circuits // IEEE Intl. Symp. on Inf. Theory Proc. (ISIT), 2011. P. 308–312.

²⁷Нурмеев Н. Н. О сложности реализации преобразователей вероятностей схемами из функциональных элементов // Методы и системы технической диагностики: Межвуз. сборник научных трудов. Вып. 18. Саратов: Саратовский гос. ун-т, 1993. С. 131–132.

²⁸Qian W., Riedel M.D., Barzagan K., Lilja D. The Synthesis of Combinational Logic to Generate Probabilities // Proc. Int'l Conf. Computer-Aided Design, 2009. P. 367–374.

²⁹Qian W., Riedel M. D., Zhou H., Bruck J. Transforming probabilities with combinational logic // IEEE Trans. on Computer-Aided Design of Integrated Circuits and Systems. 2011. Vol. 30. P. 1279–1292.

³⁰Схиртладзе Р. Л. О методе построения булевой случайной величины с заданным распределением вероятностей // Дискретный анализ: Сб. науч. тр. Новосибирск: Ин-т математики СО АН СССР, 1966. Вып. 7. С. 71–80.

полнено равенство $W_{\{\&, \vee, \neg\}}(\{p\}) = S^{(2)}$. Таким образом, множество $S^{(2)}$ оказывается конечно порожденным относительно оператора $W_{\{\&, \vee, \neg\}}$, и, более того, порождается любым невырожденным бернуллиевским распределением. Этот результат явно демонстрирует большую силу операторов замыкания W_B и позволяет рассчитывать на более простое устройство классов распределений, замкнутых относительно операторов W_B , в том числе и в случае $B \neq P_k$.

Результат Р. Л. Схиртладзе был независимо воспроизведен а также частично усилен в работах А. Д. Яшунского³¹, а также Х. Жу и Дж. Брака³². В них, в частности, установлено равенство $W_{\{\&, \vee\}}(\{p\}) = S^{(2)}$ для $p \in S^{(2)} \setminus \{e^{(0)}, e^{(1)}\}$.

Вопросы аппроксимируемости булевых случайных величин также рассматривались в работах и Н. Н. Нурмеева³³ и М. Д. Риделя и др.³⁴. В обоих случаях исследуется вопрос об оптимальном выборе конечного множества булевых случайных величин $\mathcal{X}_0$ для аппроксимации произвольных булевых случайных величин с помощью всевозможных операций из P_2 .

Из установленного Р. Л. Схиртладзе равенства $W_{\{\&, \vee, \neg\}}(\{p\}) = S^{(2)}$ при $p \in S^{(2)} \setminus \{e^{(0)}, e^{(1)}\}$ естественно вытекает, что $W_{P_2}(\{p\}) = S^{(2)}$. В случае распределений на k -элементном множестве при $k > 2$ равенство $W_{P_k}(\{p\}) = S^{(k)}$ для $p \in SQ^{(k)} \setminus \{e^{(0)}, \dots, e^{(k-1)}\}$ вытекает из результатов Р. М. Колпакова о строении замкнутых классов рациональных распределений, однако для произвольного распределения $p \in S^{(k)} \setminus \{e^{(0)}, \dots, e^{(k-1)}\}$ вывести это непосредственно из результатов Р. М. Колпакова, вообще говоря, нельзя.

Помимо результатов Р. Л. Схиртладзе и их обобщений, к вопросам аппроксимируемости конечных случайных величин в итеративных системах можно также отнести ряд результатов, касающихся

³¹Яшунский А. Д. О преобразованиях вероятности неповторными булевыми формулами // Материалы XVI Международной школы-семинара «Синтез и сложность управляющих систем» (Санкт-Петербург, 26–30 июня 2006 г.). М.: Изд-во механико-математического факультета МГУ, 2006. С. 150–155.

³²Zhou H., Bruck J. On the expressibility of stochastic switching circuits // Proc. IEEE ISIT (2009). P. 2061–2065.

³³Нурмеев Н. Н. О булевых функциях с аргументами, принимающими случайные значения // Проблемы теоретической кибернетики. Тез. докл. VIII Всесоюзной конференции. Горький, 1988. Часть 2. С. 59–60.

³⁴Qian W., Riedel M.D., Barzagan K., Lilja D. The Synthesis of Combinational Logic to Generate Probabilities // Proc. Int'l Conf. Computer-Aided Design, 2009. P. 367–374.

ся преобразований случайных величин групповыми операциями и их обобщениями. Подобные задачи, в отличие от всех приведенных ранее, рассматривались прежде всего в теории вероятностей.

Итеративная система конечных случайных величин, порождаемая бинарной полугрупповой операцией, заданной на E_k , может быть исследована с помощью аппарата марковских цепей в силу ассоциативности полугрупповой операции. Соответствующие построения упоминаются в книге У. Гренандера, а также исследуются для более общего случая дискретных полугрупп в работе П. Мартина-Лёфа³⁵. В терминах замкнутых классов распределений фактически изучается множество $V_{\{\circ\}}(\{p\})$, где $\circ$ — полугрупповая операция. При этом из свойств цепей Маркова вытекает, что множество $W_{\{\circ\}}(\{p\}) \setminus V_{\{\circ\}}(\{p\})$ конечно, а если соответствующая цепь эргодическая, то в множестве $W_{\{\circ\}}(\{p\})$ имеется единственная предельная точка. Содержательно это соответствует выполнению в соответствующей полугруппе некоторого предельного вероятностного закона. Некоторые результаты о связи между структурой полугруппы и свойствами этого предельного закона рассмотрены в работе Дж. Р. Барнеса, П. Б. Черрито и И. Леви³⁶.

В случае, если операции $\circ$ является не только полугрупповой, но и групповой, соответствующая цепь Маркова имеет бистохастическую матрицу переходов и при некоторых дополнительных условиях на носитель $\mu(p)$ единственным предельным распределением соответствующей итеративной системы является равномерное распределение u . Это утверждение наряду с другими свойствами сумм случайных величин в конечных абелевых группах присутствует в работе Н. Н. Воробьева³⁷. В настоящее время основные усилия исследователей в этой области нацелены на установление связей между свойствами групп и скоростью сходимости к предельному распределению (см. обзор Л. Салофф-Коста³⁸).

Непосредственный перенос результатов о полугруппах на дру-

³⁵Martin-Löf P. Probability theory on discrete semigroups // Z. Wahrscheinlichkeitstheorie und Verw. Gebiete. 1965. Vol. 4. P. 78–102.

³⁶Barnes G. R., Cerrito P. B., Levi I. Random walks on finite semigroups // J. Appl. Probab. 1998. V. 35, N 4. P. 824–832.

³⁷Воробьев Н. Н. Сложение независимых случайных величин на конечных абелевых группах // Матем. сб. 1954. Т. 34(76), № 1. С. 89–126.

³⁸Saloff-Coste L. Random walks on finite groups // Probability on discrete structures. Encyclopaedia Math. Sci., 110. Springer, Berlin, 2004. P. 263–346.

гие операции неосуществим, поскольку снятие требования ассоциативности операций лишает возможности непосредственного сведения к марковским цепям и, как следствие, использования соответствующего аппарата. Однако, даже если марковские цепи не позволяют моделировать все вычисления в итеративной системе, можно рассматривать подмножества случайных величин из итеративной системы, заведомо моделируемых цепями Маркова. Именно так С. Марковски, Д. Глигорски и В. Бакева устанавливают³⁹ некоторые свойства итеративных систем, порождаемых конечным набором квазигрупповых операций, а именно принадлежность $W_{\{\circ_1, \dots, \circ_s\}}(\{p\}) \ni u$, где $\circ_1, \dots, \circ_s$ — какие-то квазигрупповые операции.

Таким образом, для групповых операций и их обобщений имеется ряд результатов о множестве предельных распределений итеративных систем, порождаемых последовательностью независимых одинаково распределенных случайных величин. Вместе с тем, за исключением систем, порождаемых одной полугрупповой (и, как частного случая, групповой) операцией на E_k , эти результаты не позволяют хоть сколько-нибудь полно охарактеризовать множество всех аппроксимируемых в системе случайных величин.

Приведенный выше обзор результатов показывает, что наиболее исследованы итеративные системы, порождаемые случайными величинами с рациональными распределениями и системой операций P_k . Для других итеративных систем имеющиеся результаты достаточно разрознены и касаются преимущественно булевых случайных величин.

Аппроксимируемость случайных величин в итеративных системах изучена еще меньше, хотя полученные результаты позволяют рассчитывать на более простую (чем для задачи выразимости) структуру замкнутых классов распределений. Хотя бы частичное описание классов распределений, замкнутых относительно оператора W_B для $B \neq P_k$, позволит не только расширить представления о возможностях аппроксимации конечных случайных величин в итеративных системах, но и даст дополнительную информацию выразимости случайных величин в системах, порождаемых системами операций, отличными от P_k .

³⁹Markovski S., Gligoroski D., Bakeva V. Quasigroup String Processing: Part 1 // Proc. of Maked. Academ. of Sci. and Arts for Math. And Tech. Sci. XX. 1–2. 1999. P. 13–28.

Цели и задачи диссертации

Главными целями диссертации являются:

1. Обобщение результата Р. Л. Схиртладзе об аппроксимируемости булевых случайных величин в системе с операциями $\{\&, \vee, \neg\}$ на другие системы булевых и произвольных конечных случайных величин, установление границ возможности подобных обобщений.
2. Исследование условий единственности предельного распределения в итеративной системе, описание различных необходимых и/или достаточных условий.
3. Описание замкнутых классов распределений конечных случайных величин в итеративных системах, порождаемых важными (с арифметической, логической, алгебраической) точки зрения системами операций — клонами булевых функций, кольцами и полями вычетов, группами и их обобщениями.

Объект и предмет исследования

Диссертация посвящена изучению итеративных систем, порождаемых в результате применения к конечным случайным величинам функций k -значной логики, и замкнутых классов вероятностных распределений, возникающих в таких системах.

Научная новизна

Все основные результаты диссертации являются новыми и получены автором самостоятельно.

Теоретическая и практическая ценность

Диссертация носит теоретический характер. Ее результаты могут быть использованы в теории функциональных систем, универсальной алгебре, теории вероятностей на алгебраических структурах, дискретной математике, математической кибернетике и теоретической информатике.

Методы исследования

В диссертации используется комбинация методов арифметики, алгебры, теории функциональных систем и дискретной математики, в том числе теории булевых функций и функций многозначной

логики, а также методов математического анализа. Именно авторское сочетание этих методов является одним из источников новых результатов.

Положения, выносимые на защиту

Следующие результаты являются основными и выносятся на защиту.

1. Определение понятия аппроксимационной полноты для систем операций, используемых в итеративных системах конечных случайных величин, необходимые условия аппроксимационной полноты.
2. Достаточные условия аппроксимационной полноты и критерий аппроксимационной полноты класса многочленов над кольцом вычетов.
3. Условия конечности множества предельных распределений в итеративных системах булевых случайных величин.
4. Условия единственности предельного распределения в произвольных итеративных системах случайных величин.
5. Описание классов случайных величин, аппроксимируемых по распределению в итеративных системах булевых случайных величин, порождаемых клонами булевых функций.
6. Конструкции замкнутых классов распределений случайных величин из итеративных систем с операциями конечной цепи.
7. Конструкции замкнутых классов распределений случайных величин из итеративных систем с операциями колец и полей вычетов, а также некоторых их обобщений.

Степень достоверности и апробация результатов

Все результаты диссертации математически строго доказаны. Они многократно докладывались на объединенном семинаре кафедры дискретной математики, кафедры математической теории интеллектуальных систем механико-математического факультета и кафедры математической кибернетики факультета вычислительной математики и кибернетики МГУ имени М.В. Ломоносова «Математические вопросы кибернетики», семинаре кафедры высшей

алгебры и семинаре «Анализ и физика» кафедры математических и компьютерных методов анализа механико-математического факультета МГУ имени М.В. Ломоносова, семинаре «Теоретическая кибернетика» и семинаре имени К.И. Бабенко в ИПМ им. М.В. Келдыша РАН, на семинаре отдела дискретной математики Математического института им. В.А. Стеклова РАН, на семинаре лаборатории дискретного анализа Института математики им. С.Л. Соболева СО РАН, на семинаре «Алгебра, геометрия и квантование» в МФТИ, на международной школе-семинаре «Синтез и сложность управляющих систем» имени академика О. Б. Лупанова (Пенза, 2009 г.), международном семинаре «Дискретная математика и ее приложения» имени академика О.Б. Лупанова (Москва, 2010, 2016, 2019 гг.), международной конференции «Проблемы теоретической кибернетики» (Нижний Новгород, 2011 г.; Пенза, 2017 г.), международной конференции LOOPS по квазигруппам и лупам (Трешт, Чехия, 2011 г.; Будапешт, Венгрия, 2019 г.) молодежной школе по дискретной математике и ее приложениям (Москва, 2011 и 2013 гг.), Индо-Российской конференции по алгебре, теории чисел, дискретной математике и приложениям (Москва, МГУ, 2014 г.), международной конференции «Дискретные модели в теории управляющих систем» (Красновидово, 2015 и 2018 гг.), конференции Ломоносовские чтения (2016, 2018, 2019, 2020 гг.), конференции AAA'95 по общей алгебре (Братислава, Словакия, 2018 г.), всероссийской конференции по алгебре и теории алгоритмов (Иваново, 2018 г.), международной алгебраической конференции памяти А.Г. Куроша (Москва, 2018 г.), международной конференции по алгебраическим структурам, математической логике, теории чисел памяти Э.Артина (Ереван, Армения, 2018 г.), Мальцевских чтениях (Новосибирск, 2016 и 2018 гг.), международной конференции «Вероятностные методы в дискретной математике» (Петрозаводск, 2019 г.), международной конференции «Алгебра, теория чисел и дискретная геометрия: современные проблемы, приложения и проблемы истории» (Тула, 2015 и 2019 гг.).

Публикации

Основные результаты диссертации опубликованы в 33 работах автора, перечисленных в конце автореферата, из которых 16 опубликованы в рецензируемых научных изданиях, рекомендованных для защиты в диссертационном совете МГУ по специально-

сти. В работе [13], опубликованной совместно с А.Р.Еременко, автору диссертации принадлежат все формулировки и доказательства, за исключением результатов раздела 2, которые принадлежат А.Р.Еременко и не включены в диссертацию.

Структура и объем работы

Диссертация состоит из введения, четырех глав и заключения, главы разбиваются на разделы. Текст диссертации изложен на 245 страницах. Список литературы содержит 135 наименований.

Краткое содержание диссертации

Во **введении** приводится обзор результатов, полученных ранее другими авторами по теме исследования диссертации, а также смежным направлениям исследований, и кратко излагаются результаты диссертации.

В **Главе 1** приводится ряд определений и простейших утверждений, связанных с выразимостью и аппроксимируемостью в итеративных системах конечных случайных величин. Помимо уже введенных выше обозначений и понятий, вводятся обозначения $c_0, c_1, \dots, c_{k-1}$ для константных функций со значениями $0, 1, \dots, k-1$, $+_k$ и $\times_k$ для сложения и умножения $\bmod k$, $\wedge$ и $\vee$ для минимума и максимума относительно порядка $0 < 1 < \dots < k-1$, $d_n(x_1, \dots, x_n)$ для булевых функций $\bigvee_{1 \leq i < j \leq n} x_i \& x_j$. Для множеств распределений

$\mathbf{H} \subseteq \mathbf{S}^{(k)}$ определяются *аффинная* и *выпуклая* оболочки:

$$\begin{aligned} \text{Aff}(\mathbf{H}) &= \left\{ \sum_{i=0}^{t-1} \alpha_i \mathbf{h}^{(i)} \mid \mathbf{h}^{(0)}, \dots, \mathbf{h}^{(t-1)} \in \mathbf{H}, \sum_{i=0}^{t-1} \alpha_i = 1 \right\}, \\ \text{Conv}(\mathbf{H}) &= \left\{ \sum_{i=0}^{t-1} \alpha_i \mathbf{h}^{(i)} \mid \mathbf{h}^{(0)}, \dots, \mathbf{h}^{(t-1)} \in \mathbf{H}, \alpha \in \mathbf{S}^{(t)} \right\}, \end{aligned}$$

где умножение распределений $\mathbf{h}^{(i)}$ на числа α_i и их последующее сложение выполняется как для элементов $\mathbb{R}^k$.

Совокупность предельных точек множества распределений $\mathbf{G}$ обозначается через $\lambda(\mathbf{G})$. Для операторов $V_B(\mathbf{G})$ и $W_B(\mathbf{G})$ в случае одноэлементного $\mathbf{G} = \{g\}$ принимается соглашение о записи $V_B(g)$ и $W_B(g)$.

Также вводятся обозначения некоторых замкнутых и неповторно замкнутых классов функций из P_k , необходимых для дальнейшего изложения. В частности, для клонов в P_2 принимаются следу-

ющие обозначения: $L = [\{c_1, +_2\}]$, $M = [\{c_0, c_1, \&, \vee\}]$, $T_0 = [\{+_2, \&\}]$, $S = [\{d_3, \neg\}]$, $O^\mu = [\{\neg(x) \vee y, d_{\mu+1}\}]$, $O^\infty = [\{\neg(x) \vee y\}]$, $K = [\{c_0, c_1, \&\}]$, $D = [\{c_0, c_1, \vee\}]$, $U = [\{c_0, \neg\}]$. Кроме того, классы, двойственные⁴⁰ к T_0 , O^μ и O^∞ обозначаются через T_1 , I^μ и I^∞ соответственно.

Класс функций, выражимых многочленами mod k , обозначается $\mathcal{A}_k$ (в случае составного k он отличен от P_k), класс функций, имеющих не более одной существенной переменной, обозначается P_k^1 . Для каждого из непустых подмножеств $\mathcal{T} \subseteq E_k$ определяются следующие классы: $C_{\mathcal{T}}$ — константные функции со значениями в $\mathcal{T}$; $S_{\mathcal{T}}$ — функции с не более чем одной существенной переменной, являющиеся перестановками на $\mathcal{T}$; $Q_{\mathcal{T}}$ — класс функций (с точностью до добавления несущественных переменных), у которых любая подфункция одной переменной лежит в классе $S_{\mathcal{T}}$; $Q_{\mathcal{T}}^\infty$ — класс функций, у которых какая-то подфункция одной переменной лежит в классе $S_{\mathcal{T}}$.

Помимо определений и обозначений Глава 1 содержит ряд утверждений о свойствах индуцированных функций и замкнутых относительно операторов V_B , W_B классов распределений. Эти свойства используются далее в работе для доказательства основных утверждений.

В **Главе 2** рассматриваются условия, при которых система преобразующих операций $B \subseteq P_k$ обладает свойствами аналогичным системе булевых функций $\{\&, \vee, \neg\}$, т. е. порождает итеративную систему, в которой любая случайная величина аппроксимируется по распределению. Вводится понятие *аппроксимационной полноты* системы функций $B \subseteq P_k$, понимаемое как выполнение равенства $W_B(\mathbf{p}) = \mathbf{S}^{(k)}$ для некоторой совокупности распределений $\mathbf{p}$. Выделяется три типа аппроксимационной полноты: *слабая*, если равенство $W_B(\mathbf{p}) = \mathbf{S}^{(k)}$ выполняется для некоторого $\mathbf{p}$, удовлетворяющего $\mu(\mathbf{p}) = E_k$; *стандартная*, если то же равенство верно для любых $\mathbf{p}$, удовлетворяющих $\mu(\mathbf{p}) = E_k$; *сильная*, если то же равенство выполнено для любых $\mathbf{p}$, удовлетворяющих $|\mu(\mathbf{p})| > 1$.

Из доказываемой в Главе 2 теоремы 2.1, описывающей некоторые замкнутые относительно W_B классы распределений, выводятся необходимые условия аппроксимационной полноты. В частности, доказано

⁴⁰Функция f^* , двойственная f , определяется тождеством $f^*(x_1, \dots, x_n) = \neg(f(\neg(x_1), \dots, \neg(x_n)))$.

Следствие 2.3 [16]. Если для некоторого множества $T \subseteq E_k$, $T \neq \emptyset$, система $B \subset P_k$ удовлетворяет $B \subseteq Q_T^\infty$, то B не является слабо аппроксимационно полной.

Из этого утверждения вытекает, что заведомо аппроксимационно неполны классы булевых функций K , D и L .

Для преобразующей системы $B = P_k$ в Главе 2 доказывается (в теореме 2.19) ее сильная аппроксимационная полнота в смысле определения данного выше.

Набор достаточных условия аппроксимационной полноты системы $B \subseteq P_k$ представлен в весьма общей форме в теореме 2.22. Использование этих достаточных условий позволяет дополнить операции кольца вычетов $\langle E_k; \{+_k, \times_k\} \rangle$ и конечной цепи $\langle E_k; \{\vee, \wedge\} \rangle$ до аппроксимационно полной (в стандартном смысле) системы. Из этих теорем, кроме того, вытекает существование конечных сильно аппроксимационно полных систем операций.

Теорема 2.23 [7]. Система $B = \{c_0, \dots, c_{k-1}, +_k, \times_k, \gamma(x)\} \subset P_k$, где $\gamma(x)$ — функция, принимающая ровно два значения 0 и 1, аппроксимационно полна.

Теорема 2.25 [15]. Система $B = \{c_0, \dots, c_{k-1}, \vee, \wedge, \gamma(x)\} \subset P_k$, где $\gamma(x)$ — функция, принимающая ровно два значения 0 и $k-1$, аппроксимационно полна.

Наконец, важным результатом Главы 2 является критерий аппроксимационной полноты класса многочленов $\mathcal{A}_k$.

Теорема 2.29 [11]. Класс $\mathcal{A}_k$ аппроксимационно полон тогда и только тогда, когда k — степень простого числа.

В Главе 3 исследуются условия, при которых у случайных величин из итеративной системы имеется единственное предельное распределение, т.е. фактически в итеративной системе выполняется некоторый предельный вероятностный закон. Такие итеративные системы характеризуются выполнением равенства $|\lambda(V_B(\mathbf{G}))| = 1$ для порождающей системы функций B и множества начальных распределений $\mathbf{G}$.

Для итеративных систем булевых случайных величин удастся продвинуться еще дальше, описав итеративные системы с любым конечным множеством предельных распределений.

Первый из результатов Главы 3 касается итеративных систем булевых случайных величин с конечным множеством распределений (и, как следствие, с пустым множеством предельных распределений).

Теорема 3.4 [6]. Пусть для конечного множества бернуллиевских распределений $G \subset [0; 1]$ и множества булевых функций B выполнено $V_B(G) = G$. Тогда имеет место по крайней мере одно из следующих утверждений:

1. $G \subseteq \{0, 1\}$.
2. $B \subseteq U$.
3. $G = \{p\}$, $p \in (0; 1)$.
4. $G \subseteq \{0, 1, \frac{1}{2}\}$, $B \subseteq L$.

При этом для каждого из четырех случаев, описанных в теореме 3.4, действительно существуют итеративные системы булевых случайных величин $\mathcal{X}(G, B)$ с множествами G и B , удовлетворяющими соответствующим условиям.

Далее описываются итеративные системы булевых случайных величин с единственным предельным распределением. В теореме используется обозначение $\mathcal{B}(q)$ для клонов булевых функций, определяемое как $\mathcal{B}(0) = K$, $\mathcal{B}(\frac{1}{2}) = L$ и $\mathcal{B}(1) = D$.

Теорема 3.7 [10]. Пусть множество бернуллиевских распределений $G \subset [0; 1]$ имеет единственную предельную точку $q \in [0; 1]$ и для некоторой системы булевых функций B выполнено $V_B(G) = G$. Тогда либо $B \subseteq MU$, либо выполнено $q \in \{0, \frac{1}{2}, 1\}$ и $B \subseteq \mathcal{B}(q)$.

Наконец, установлено, что за исключением в определенном смысле тривиального случая $B \subseteq U$, итеративная система булевых случайных величин $\mathcal{X}(G, B)$ не может иметь конечное число предельных распределений большее 1.

Теорема 3.13 [12]. Пусть для $G \subset [0; 1]$ и $B \subseteq P_2$ выполнено $V_B(G) = G$. Если при этом $\lambda(G)$ конечно, то либо $B \subseteq U$, либо $|\lambda(G)| < 2$.

Обобщение теоремы 3.7 с систем булевых случайных величин на произвольные конечные случайные величины опирается на свойства итеративных систем, порождаемых операциями с квазигрупповыми свойствами. В Главе 3 доказывается ряд утверждений об аппроксимируемости равномерно распределенных случайных величин в итеративных системах с квазигрупповыми операциям. Одним из наиболее общих результатов в этом направлении является следующая теорема. Фигурирующие в ней $\mathcal{T}$ -поглощающие квазигрупповые операции составляют класс, ранее обозначенный как $Q_{\mathcal{T}}$. Такие классы обобщают классы $K, L, D \subseteq P_2$, фигурировавшие в теореме 3.7, поскольку для $\mathcal{T} \subseteq E_2$ выполнены равенства $Q_{\{0\}} = K$, $Q_{\{0,1\}} = L$, $Q_{\{1\}} = D$.

Теорема 3.28 [3]. Пусть задано множество $\mathcal{T} \subseteq E_k$, функция $f(x_1, \dots, x_t) \in P_k$, являющаяся t -арной, $t > 1$, $\mathcal{T}$ -поглощающей квазигрупповой операцией и распределение $g \in S^{(k)}$, удовлетворяющее условию $\mu(g) \supseteq \mathcal{T}$. Тогда $\lambda(V_{\{f\}}(g)) \subseteq \{q\}$, где $\mu(q) = \mathcal{T}$ и $q_i = \frac{1}{|\mathcal{T}|}$ для $i \in \mathcal{T}$.

В отличие от случая $k = 2$ полностью охарактеризовать (по аналогии с теоремой 3.7) все итеративные системы с единственным предельным распределением в случае произвольного k не удастся, однако «исключительные» итеративные системы, в которых единственность предельной точки не обязательно влечет ограничения на множество операций, можно описать в терминах «геометрии» классов распределений.

В формулировке следующей теоремы, обобщающей теорему 3.7, используются следующие определения. Множество распределений $G \subseteq S^{(k)}$ называется *существенно плоским*, если для любого конечного $G' \subseteq G$ выполнено $\text{Aff}(G \setminus G') \not\supseteq S^{(k)}$. Множество $G \subseteq S^{(k)}$ называется *X-множеством*, если найдутся такие множества G_1 и G_2 , что $G = G_1 \cup G_2$ и при этом $\text{Aff}(G_1) \not\supseteq S^{(k)}$, $\text{Aff}(G_2) \not\supseteq S^{(k)}$.

Теорема 3.31 [14]. Пусть множество распределений $G \subseteq S^{(k)}$ не является ни существенно плоским, ни X-множеством и имеет единственную предельную точку q . Если $B \subseteq P_k$ — некоторое множество

операций, удовлетворяющее равенству $V_B(\mathbf{G}) = \mathbf{G}$, то выполнено $B \subseteq Q_{\mu(\mathbf{q})} \cup C_{E_k}$, а если $B \setminus P_k^1 \neq \emptyset$, то $q_i = \frac{1}{|\mu(\mathbf{q})|}$ для всех $i \in \mu(\mathbf{q})$ и $q_i = 0$ для всех $i \notin \mu(\mathbf{q})$, т. е. $\mathbf{q}$ — равномерное на $\mu(\mathbf{q})$ распределение.

В **Главе 4** исследуется задача аппроксимируемости случайных величин в итеративных системах, порождаемых некоторыми специальными наборами операций, а именно — клонами булевых функций, конечными цепями, кольцами и полями вычетов, и некоторыми схожими с ними системами. Для означенных систем строятся семейства классов распределений, замкнутых относительно оператора W_B (в отдельных случаях вплоть до полного описания решетки замкнутых классов распределений). Это позволяет частично решать задачу аппроксимируемости случайных величин, указывая в каждом случае множество случайных величин, которые заведомо не могут быть аппроксимированы, и, в частности, доказывать аппроксимационную неполноту некоторых систем.

Первая часть результатов Главы 4 относится к итеративным системам булевых случайных величин, порождаемых клонами булевых функций. В теореме 4.15 получено описание всех классов распределений $W_A(p)$, где A — какой-то клон и $p \in (0; 1)$. На основе этой теоремы полностью описана решетка классов распределений, замкнутых относительно операторов W_A , где A — клон, не содержащийся в K , D или L .

Теорема 4.16 [8]. Пусть $A \subseteq P_2$ — клон и $A \not\subseteq K, D, L$. Тогда совокупность непустых замкнутых классов распределений $G \subseteq [0; 1]$, удовлетворяющих $W_A(G) = G$, исчерпывается следующими множествами:

1. $\{0, 1\}, [0; 1]$ для любого клона A .
2. $\{0\}$ если $A \subseteq T_0$, $\{1\}$ если $A \subseteq T_1$.
3. $\{\frac{1}{2}\}$ если $A \subseteq S$.
4. $[0; p]$, где $p \leq 1 - \frac{1}{\mu}$, если $A \subseteq I^\mu$, $[p; 1]$ где $p \geq \frac{1}{\mu}$ если $A \subseteq O^\mu$.

Для классов распределений, замкнутых относительно W_A , где A — подклон одного из клонов K , D или L , также доказывается набор критериальных свойств (теорема 4.17), однако они не позволяют эффективно описать всю решетку замкнутых классов распределений, подобно тому, как это делается в теореме 4.16.

Также доказываются два утверждения (теоремы 4.18 [1, 2] и 4.22 [13]), демонстрирующие на примере итеративных систем булевых случайных величин неравномерность плотности распределений, выражимых в итеративной системе случайных величин, даже в тех случаях, когда эти распределения всюду плотны в множестве распределений.

Затем в Главе 4 рассматривается класс итеративных систем конечных случайных величин, порождаемых операциями конечной цепи, а именно $\wedge$ и $\vee$, обозначающими соответственно минимум и максимум относительно линейного порядка на множестве E_k . Вводятся два семейства классов распределений, зависящие от числа $\alpha > 1$ и индекса $i \in E_k$:

$$\begin{aligned} \mathbf{L}(i, \alpha) &= \left\{ \mathbf{p} = (p_0, \dots, p_{k-1}) \in \mathbf{S}^{(k)} \left| \sum_{j=0}^{i-1} p_j \leq \left(\sum_{j=0}^i p_j \right)^\alpha \right. \right\}, \\ \mathbf{U}(i, \alpha) &= \left\{ \mathbf{p} = (p_0, \dots, p_{k-1}) \in \mathbf{S}^{(k)} \left| \sum_{j=i+1}^{k-1} p_j \leq \left(\sum_{j=i}^{k-1} p_j \right)^\alpha \right. \right\}, \end{aligned}$$

где сумма, у которой верхний индекс меньше нижнего, считается равной нулю. Доказывается, что множества распределений из этих семейств замкнуты относительно $W_{\{\wedge, \vee\}}$.

Теорема 4.26 [15]. Для любого $\alpha > 1$ и любого $i \in E_k$ выполнены соотношения $W_{\{\vee, \wedge\}}(\mathbf{L}(i, \alpha)) = \mathbf{L}(i, \alpha)$ и $W_{\{\vee, \wedge\}}(\mathbf{U}(i, \alpha)) = \mathbf{U}(i, \alpha)$.

Теорема 4.26, позволяет, во-первых, установить аппроксимационную неполноту системы $\{\wedge, \vee\}$, а, во-вторых, может быть использована для ограничения снизу некоторых замкнутых классов распределений, т.е. описания распределений, заведомо входящих в $W_{\{\wedge, \vee\}}(\mathbf{G})$ для некоторых множеств $\mathbf{G} \subset \mathbf{S}^{(k)}$. В частности, доказывается следующая теорема.

Теорема 4.28 [15]. Пусть $\mathbf{p} \in \mathbf{S}^{(k)}$ удовлетворяет $\mu(\mathbf{p}) = E_k$. Тогда для всех $i \in E_k \setminus \{0\}$ выполнено $\text{Conv}(\mathbf{e}^{(i-1)}, \mathbf{e}^{(i)}) \subseteq W_{\{\vee, \wedge\}}(\mathbf{p})$.

Далее в Главе 4 исследуются итеративные системы случайных величин, порождаемые операциями колец и полей вычетов. В теореме 4.33 [5] описываются некоторые выпуклые классы распределений, замкнутые относительно $W_{\{+_k, \times_k\}}$, где $+_k, \times_k$ — сложение

и умножение в поле вычетов $\text{mod } k$, k — простое. Затем, за счет усложнения конструкции классов распределений, эти построения обобщаются на случай произвольного, в том числе составного, значения k . Для набора распределений $\mathbf{g}^{(1)}, \dots, \mathbf{g}^{(t)} \in \mathbf{S}^{(k)}$ и подмножества $M \subseteq E_k$ определяются следующие классы распределений:

$$\begin{aligned} \mathbf{K}_{ij} &= \{\mathbf{e}^{(j)} \widehat{\times}_k (\mathbf{g}^{(i)} \widehat{+}_k \mathbf{e}^{(s)}) \mid s \in E_k\} \cup \{\mathbf{e}^{(0)}\}, \\ \mathbf{K}_i(M) &= \{\mathbf{h}^{(ij_1)} \widehat{+}_k \dots \widehat{+}_k \mathbf{h}^{(ij_m)} \mid \{j_1, \dots, j_m\} = M, \mathbf{h}^{(ij_r)} \in \mathbf{K}_{ij_r}\}, \\ \mathbf{K}(\mathbf{g}^{(1)}, \dots, \mathbf{g}^{(t)}; M) &= \{\mathbf{j}^{(1)} \widehat{+}_k \dots \widehat{+}_k \mathbf{j}^{(t)} \mid \mathbf{j}^{(1)} \in \mathbf{K}_1(M), \dots, \mathbf{j}^{(t)} \in \mathbf{K}_t(M)\}. \end{aligned}$$

С использованием этих конструкций описываются семейства выпуклых классов распределений, замкнутых относительно $W_{\{+k, \times_k\}}$. Эти утверждения могут быть распространены и на итеративные системы случайных величин, порожденные другими конечными кольцами. В частности, доказывается следующая теорема, выполненная как для колец вычетов $\text{mod } k$, так и для других ассоциативных колец с единицей.

Теорема 4.38 [9]. Пусть $\langle E_k; \{+k, \times_k\} \rangle$ — ассоциативное кольцо с единицей, $0 \in E_k$ — его нулевой элемент, $U \subset E_k$ — группа обратимых элементов. Обозначим через Z множество $E_k \setminus (U \cup \{0\})$. Для заданных распределений $\mathbf{g}^{(1)}, \dots, \mathbf{g}^{(t)} \in \mathbf{S}^{(k)}$, положим:

$$\mathbf{I} = \{\mathbf{e}^{(j)} \widehat{\times}_k (\mathbf{g}^{(i)} \widehat{+}_k \mathbf{e}^{(s)}) : j \in U, s \in E_k, i = 1, \dots, t\}$$

и $\mathbf{H} = \text{Conv}(\mathbf{I} \cup \mathbf{K}(\mathbf{g}^{(1)}, \dots, \mathbf{g}^{(t)}; Z))$ Тогда $W_{\{+k, \times_k\}}(\mathbf{H}) = \mathbf{H}$.

Наконец, в Главе 4 рассматриваются итеративные системы случайных величин, порождаемые операциями $\circ$ и $\bullet$, которые обобщают операции $+_k$ и $\times_k$ поля вычетов $\text{mod } k$ (k — простое). Предложены конструкции семейств классов распределений (в том числе невыпуклых), замкнутых относительно оператора $W_{\{\circ, \bullet\}}$. В утверждениях ниже предполагается, что $\circ$ — квазигрупповая операция на E_k , удовлетворяющая тождествам $x \circ 0 = 0 \circ x = x$, а $\bullet$ — квазигрупповая операция на $E_k \setminus \{0\}$, удовлетворяющая тождествам $x \bullet 0 = 0 \bullet x = 0$.

Для распределений $\mathbf{x} = (x_0, \dots, x_{k-1}) \in \mathbf{S}^{(k)}$ вводятся величины $\varepsilon(\mathbf{x}) = 1 - x_0$ и $\delta_i(\mathbf{x}) = x_i - \varepsilon(\mathbf{x})/(k-1)$, $i = 1, \dots, k-1$, с помощью

которых определяются следующие классы распределений:

$$\mathbf{H}_{\alpha,b} = \{\mathbf{x} \in \mathbf{S}^{(k)} : \varepsilon(\mathbf{x}) \leq b\} \cap \left(\bigcap_{i \neq 0} \left\{ \mathbf{x} \in \mathbf{S}^{(k)} : |\delta_i(\mathbf{x})| \leq \frac{\varepsilon(\mathbf{x})^\alpha}{k-1} \right\} \right),$$

$$\mathbf{K}_{a,b,c} = \bigcap_{i \neq 0} \left\{ \mathbf{x} \in \mathbf{S}^{(k)} : |\delta_i(\mathbf{x})| \leq a - \frac{a}{b}(\varepsilon - h), |\delta_i(\mathbf{x})| \leq a + \frac{a}{c}(\varepsilon - h) \right\},$$

где $h = \frac{k-1}{k}$, и $\alpha, a, b, c \geq 0$ — параметры. Доказываются теоремы:

Теорема 4.44 [4]. Пусть параметр a удовлетворяет условиям $0 < a \leq \frac{1}{k}$, положим $\mathbf{K} = \mathbf{K}_{a,k(k-1)a^2,h}$. Тогда $W_{\{\circ,\bullet\}}(\mathbf{K}) = \mathbf{K}$.

Теорема 4.45 [4]. Для любого $k \geq 3$ найдется такое $\alpha_0(k)$, что при всех $\alpha \geq \alpha_0(k)$ множества $\mathbf{I}_\alpha = (\mathbf{H}_{\alpha,h} \cup \mathbf{K}_{a,k(k-1)a^2,k(k-1)a^2})$, где $a = \frac{h^\alpha}{k-1}$, удовлетворяют равенству $W_{\{\circ,\bullet\}}(\mathbf{I}_\alpha) = \mathbf{I}_\alpha$.

В **заключении** систематизируются полученные результаты об аппроксимируемости случайных величин и классах распределений, замкнутых относительно операторов W_B , характеризуются возможные направления дальнейших исследований.

Публикации автора по теме диссертации

Статьи в рецензируемых научных изданиях, рекомендованных для защиты в диссертационном совете МГУ по специальности 01.01.06

1. Yashunsky A. D. Asymptotics of the probability of values of random Boolean expressions // Journal of Applied and Industrial Mathematics. 2007. Vol. 1, No. 4. P. 509–531. (Scopus. SJR 2008: 0,114)
2. Яшунский А. Д. О равномерном приближении непрерывных функций функциями вероятности булевых базисов // Вестник МГУ. Серия 1. Математика. Механика. 2007. № 2. С. 37–43. Перевод: Yashunskii A. D. Uniform approximation of continuous functions by probability functions of Boolean bases // Moscow Univ. Math. Bull. 2007. Vol. 62, No 2. P. 78–84. (RSCI, Scopus, WoS. SJR 2008: 0,225)

3. Яшунский А. Д. О преобразованиях распределений вероятностей неповторными квазигрупповыми формулами // Дискретная математика. 2013. Т. 25, № 2. С. 149–159. Перевод: Yashunskii A. D. On transformations of probability distributions by read-once quasigroup formulae // Discrete Mathematics and Applications. 2013. Vol. 23, no. 2. P. 211–223. (RSCI, Scopus, WoS. SJR 2013: 0,140)
4. Яшунский А. Д. О неповторных преобразованиях случайных величин над конечными полями // Дискретная математика. 2015. Т. 27, № 3. С. 145–157. Перевод: Yashunsky A. On read-once transformations of random variables over finite fields // Discrete Mathematics and Applications. 2015. Vol. 25, no. 5. P. 311–321. (RSCI, Scopus, WoS. SJR 2015: 0,278)
5. Яшунский А. Д. Выпуклые многогранники распределений, сохраняемые операциями конечного поля // Вестник МГУ. Серия 1. Математика. Механика. 2017. № 4. С. 54–58. Перевод: Yashunskii A.D. Convex polyhedra of distributions preserved by operations over a finite field // Moscow Univ. Math. Bull. 2017. Vol. 72, No. 4. P. 165–168. (RSCI, Scopus, WoS. SJR 2017: 0,195)
6. Яшунский А. Д. Конечные алгебры бернуллиевских распределений // Дискретная математика. 2018. Т. 30, № 2. С. 148–161. (Перевод: Yashunsky A. D. Finite algebras of Bernoulli distributions // Discrete Mathematics and Applications. 2019. Vol. 29, no. 4. P. 267–276.) (RSCI, Scopus, WoS. SJR 2019: 0,157)
7. Yashunsky A. D. Algebras of probability distributions on finite sets // Proceedings of the Steklov Institute of Mathematics. 2018. Vol. 301, no. 1. P. 304–318. (Scopus, WoS. SJR 2018: 0,595; JCR 2018: 0,7)
8. Yashunsky A. D. Clone-induced approximation algebras of Bernoulli distributions // Algebra Universalis. 2019. Vol. 80, no. 1. (Scopus, WoS. SJR 2019: 0,486; JCR 2020: 0,404)
9. Яшунский А. Д. Выпуклые алгебры вероятностных распределений, индуцированные конечными ассоциативными кольцами // Дискретная математика, 2019. Т. 31, № 1. С. 133–142. (RSCI. Импакт-фактор РИНЦ 2019: 0,482)
10. Яшунский А. Д. Алгебры бернуллиевских распределений с

единственной предельной точкой // Вестник МГУ. Серия 1. Математика. Механика. 2019. № 4. С. 3–9. Перевод: Yashunskii A.D. Algebras of Bernoulli distributions with a single limit point // Moscow Univ. Math. Bull. 2019. Vol. 74, No. 4. P. 135–140. (RSCI, Scopus, WoS. SJR 2019: 0,200)

11. Яшунский А. Д. Полиномиальные преобразования случайных величин на конечных множествах // Матем. заметки. 2019. Т. 106, вып. 6. С. 951–954. Перевод: Yashunskii A. D. Polynomial Transformations of Random Variables on Finite Sets // Math. Notes. 2019. Vol. 106, No. 6. P. 1024–1027. (RSCI, Scopus, WoS. SJR 2019: 0,370)
 12. Yashunsky A. D. Limit Points of Bernoulli Distribution Algebras Induced by Boolean Functions // Lobachevskii Journal of Mathematics. 2019. Vol. 40, No. 9. P. 1423–1432. (Scopus, WoS. SJR 2019: 0,422)
 13. Еременко А. Р., Яшунский А. Д. О весе функций, заданных бесповторными И/ИЛИ формулами // Интеллектуальные системы. Теория и приложения. 2019. Т. 23, № 3. С. 41–55. (Импакт-фактор РИНЦ 2019: 0,425)
- В этой работе автору диссертации принадлежат все формулировки и доказательства, за исключением результатов раздела 2, которые принадлежат А. Р. Еременко.
14. Яшунский А. Д. О необходимых условиях предельных вероятностных теорем в конечных алгебрах // Доклады РАН. Математика, информатика, процессы управления. 2020, Т. 493, № 1. С. 47–50. Перевод: Yashunsky A.D. On Necessary Conditions of Probability Limit Theorems in Finite Algebras // Doklady Mathematics. 2020. Vol. 102(1). P. 301–303. (RSCI, Scopus, WoS. SJR 2019: 0,607; JCR 2020: 0,548)
 15. Яшунский А. Д. Об аппроксимации случайных величин над конечной цепью // Дискретный анализ и исследование операций. 2020. Т. 27, № 3. С. 109–125. Перевод: Yashunsky A. D. On the approximation of random variables on a finite chain // J. Appl. Industr. Math. 2020. Vol. 14, No. 3. P. 581–591. (RSCI, Scopus. SJR 2019: 0,200)
 16. Yashunsky A. D. On Necessary Conditions of Finite-valued

Random Variable Algebraic Approximation // Lobachevskii Journal of Mathematics. 2021. Vol. 42, No. 1. P. 216–220. (Scopus, WoS. SJR 2019: 0,422)

Прочие публикации

17. Яшунский А. Д. О преобразованиях вероятности неповторными булевыми формулами // Материалы XVI Международной школы-семинара «Синтез и сложность управляющих систем» (Санкт-Петербург, 26–30 июня 2006 г.) — М.: Изд-во механико-математического факультета МГУ, 2006. — С. 150–155.
18. Яшунский А.Д. Об одном семействе распределений вероятностей, порождаемом неповторными формулами над конечными полями // Материалы IX молодежной научной школы по дискретной математике и ее приложениям. 2013. С. 127–130.
19. Яшунский А.Д. О множествах распределений вероятностей, сохраняемых операциями конечного поля // Препринты ИПМ им. М. В. Келдыша. 2014. № 51. 20 с.
20. Яшунский А.Д. Об операциях с независимыми случайными величинами над конечным линейно упорядоченным множеством // Труды IX Международной конференции «Дискретные модели в теории управляющих систем» (Москва и Подмосковье, 20-22 мая 2015 г.) М.: МАКС Пресс, 2015. С. 272–274.
21. Яшунский А.Д. О преобразованиях случайных величин над линейно упорядоченным трехэлементным множеством // Алгебра, теория чисел и дискретная геометрия: современные проблемы и приложения: Материалы XIII Междунар. конф., посвященной 85-летию со дня рождения профессора Сергея Сергеевича Рышкова. Тула: Изд-во Тул. гос. пед. ун-та им. Л.Н.Толстого, 2015. С. 206–208.
22. Яшунский А. Д. О выпуклых многогранниках распределений, сохраняемых операциями конечного поля // Препринты ИПМ им. М.В. Келдыша. 2016. № 11. 10 с.
23. Яшунский А. Д. Преобразования бернуллиевских распределений булевыми функциями из замкнутых классов // Препринты ИПМ им. М.В. Келдыша. 2016. № 38. 23 с.
24. Яшунский А. Д. Приближения вероятностных распределений функциями k -значной логики // Препринты ИПМ им.

М.В.Келдыша. 2016. № 58. 7 с.

25. Яшунский А. Д. О преобразованиях дискретных случайных величин многочленами // Проблемы теоретической кибернетики: XVIII международная конференция (Пенза, 19–23 июня 2017 г.) : Материалы. М. : МАКС Пресс, 2017. С. 268–271.
26. Яшунский А. Д. Конечные системы операций для аппроксимации дискретных вероятностных распределений // Препринты ИПМ им. М.В. Келдыша. 2017. № 10. 7 с.
27. Яшунский А. Д. О конечных алгебрах бернуллиевских распределений // Препринты ИПМ им. М. В. Келдыша. 2018. № 34. 19 с.
28. Яшунский А.Д. О подалгебрах вероятностных распределений над конечными кольцами // Препринты ИПМ им. М.В.Келдыша. 2018. № 84. 14 с.
29. Яшунский А. Д. Алгебры бернуллиевских распределений с единственной предельной точкой // Препринты ИПМ им. М.В. Келдыша. 2018. № 135. 16 с.
30. Яшунский А.Д. О предельных точках алгебр бернуллиевских распределений // Препринты ИПМ им. М.В.Келдыша. 2018. № 270. 16 с.
31. Яшунский А. Д. Конечные алгебры бернуллиевских распределений // Дискретные модели в теории управляющих систем. Труды X Международной конференции. 2018. С. 288–291.
32. Яшунский А. Д. О необходимых условия алгебраической аппроксимации случайных величин на конечном множестве // Вероятностные методы в дискретной математике. Расширенные тезисы докладов X Международной Петрозаводской конференции. 2019. С. 121–123.
33. Яшунский А. Д. О предельных точках в алгебрах дискретных вероятностных распределений // Алгебра, теория числе и дискретная геометрия: современные проблемы, приложения и проблемы истории. Материалы XVII Международной конференции, посвящённой 100-летию со дня рождения профессора Н. И. Фельдмана и 90-летию со дня рождения профессоров А. И. Виноградова, А. В. Малышева и Б. Ф. Скубенко. 2019. С. 68–72.