ДОКЛАДЫ РОССИЙСКОЙ АКАДЕМИИ НАУК. МАТЕМАТИКА, ИНФОРМАТИКА, ПРОЦЕССЫ УПРАВЛЕНИЯ, 2023, том 510, с. 8–12

МАТЕМАТИКА

УДК 510.647+510.5

ЭЛЕМЕНТАРНЫЕ ИНВАРИАНТЫ ДЛЯ КВАНТОРНОЙ ВЕРОЯТНОСТНОЙ ЛОГИКИ

© 2023 г. С. О. Сперанский[1,*]

Представлено академиком РАН Л.Д. Беклемишевым
Поступило 20.01.2023 г.
После доработки 01.02.2023 г.
Принято к публикации 02.03.2023 г.

Пусть QPL – предложенный в [8] двусортный вероятностный язык, который расширяет хорошо известный "полиномиальный" язык, описанный в [3, раздел 6], посредством добавления кванторов по событиям. Мы показываем, что все безатомные пространства имеют одну и ту же QPL-теорию и эта теория разрешима. Также мы вводим понятие элементарного инварианта для QPL и используем его для получения точных верхних оценок на сложность некоторых интересных вероятностных теорий.

Ключевые слова: вероятностная логика, квантификация по событиям, элементарные инварианты, сложность

DOI: 10.31857/S2686954323600040, **EDN:** XHTJMV

1. ВВЕДЕНИЕ

Нас будет интересовать двусортный вероятностный язык QPL, предложенный в [8]. Можно думать о QPL как о естественной комбинации элементарного языка булевых алгебр и языка упорядоченных полей. Его фрагмент, содержащий только кванторы по вещественным числам (но не по событиям), является вариантом хорошо известного "полиномиального" языка, описанного в [3, раздел 6].

Несколько важных сложностных результатов о QPL было получено в [8]. Мы знаем, что если $\mathcal{K}$ – класс вероятностных пространств, который содержит все бесконечные дискретные пространства, то его QPL-теория имеет как минимум ту же сложность, что и полная арифметика второго порядка. QPL-теория конечных вероятностных пространств намного проще, но по-прежнему неразрешима; точнее, она имеет ту же сложность, что и дополнение проблемы остановки. Кроме того, эти результаты остаются справедливы, если мы исключим кванторы по вещественным числам. С другой стороны, для каждого положительного целого числа n QPL-теория пространств с ровно n элементами является разрешимой. Можно задаться вопросом, существуют ли какие-нибудь другие естественные примеры разрешимых вероятностных теорий. Мы отвечаем на этот вопрос утвердительно, показывая, что все безатомные пространства имеют одну и ту же QPL-теорию и эта теория разрешима.

Другая интересная проблема, возникающая в кванторной вероятностной логике, касается верхних оценок сложности. А именно, вероятностные пространства не могут быть непосредственно закодированы в языке арифметики высших порядков, что затрудняет получение верхних оценок сложности для многих вероятностных теорий. Чтобы преодолеть эту трудность, мы разрабатываем теорию элементарных инвариантов для QPL. В отличие от вероятностных пространств, их инварианты могут быть легко закодированы как множества натуральных чисел, что позволяет нам доказать, что для любого "аналитического" класса вероятностных пространств его QPL-теория имеет как максимум ту же сложность, что и полная арифметика второго порядка. Это решает одну из главных проблем, заявленных в [8].

Настоящую работу можно рассматривать как исследование по элементарным теориям классов вероятностных пространств; ср. [2] и [7].

2. ПРЕДВАРИТЕЛЬНЫЕ СВЕДЕНИЯ

Поскольку многие сложностные результаты о кванторной вероятностной логике формулируются, используя арифметику второго порядка,

[1] *Математический институт им. В.А. Стеклова Российской академии наук, Москва, Россия*
**E-mail: katze.tail@gmail.com*

мы начнем с описания языка последней и лишь затем перейдем к определению QPL.

2.1. Арифметика второго порядка

Напомним, что в *арифметике второго порядка* имеются: (i) *индивидные переменные* x, y, z, ..., которые предназначены пробегать $\mathbb{N}$; (ii) для каждого положительного целого числа k *переменные по множествам* X^k, Y^k, Z^k, ... *типа* k, которые предназначены пробегать подмножества $\mathbb{N}^k$. Обозначим через $\mathfrak{N}$ стандартную модель арифметики и через σ – ее сигнатуру. Для удобства мы будем считать, что σ содержит символ для любой вычислимой функции или отношения. σ-*Формулы второго порядка* строятся из первопорядковых атомарных σ-формул и выражений вида

$$(t_1,\dots,t_k)\in X^k,$$

где k – положительное целое число, X^k – переменная по множествам типа k и t_1, ..., t_k – σ-термы, обычным образом. В дальнейшем под σ-*формулой* мы будем понимать σ-формулу второго порядка.

Пусть n – положительное целое число. Напомним, что σ-формула лежит в Π^1_n, если она имеет вид

$$\underbrace{\forall\vec{X}_1\exists\vec{X}_2\dots\vec{X}_n}_{n-1\text{ перемена кванторов}}\quad\Psi,$$

где $\vec{X}_1$, $\vec{X}_2$, ..., $\vec{X}_n$ суть кортежи переменных по множествам и Ψ не содержит кванторов по множествам. Подмножество $\mathbb{N}$ называется: (a) Π^1_n-*ограниченным*, если оно определимо в $\mathfrak{N}$ посредством Π^1_n-σ-формулы; (b) Π^1_n-*трудным*, если к нему m-сводимо любое Π^1_n-ограниченное подмножество $\mathbb{N}$; (c) Π^1_n-*полным*, если оно одновременно Π^1_n-ограничено и Π^1_n-трудно. Традиционно Π^1_n-ограниченные множества называются Π^1_n-*множествами*. Хорошо известно, что Π^1_n-полные множества существуют. В частности, совокупность всех Π^1_n-σ-предложений, истинных в $\mathfrak{N}$, оказывается Π^1_n-полной. Аналогично для подмножеств $\mathbb{N}^2$, $\mathbb{N}^3$ и т.д.

Теорема 2.1 (см. [9]). *Пусть* σ_+ *обозначает* $\langle +;=\rangle$. *Тогда любое* Π^1_n-*подмножество* $\mathbb{N}^k$ *может быть определено в* $\mathfrak{N}$ *посредством* σ_+-*формулы вида*

$$\underbrace{\forall X^1_1\exists X^1_2\dots X^1_n}_{n-1\text{ перемена кванторов}}\quad\Psi,\qquad(\star)$$

где X^1_1, X^1_2, ..., X^1_n суть переменные по множествам типа 1 и Ψ не содержит переменных по множествам.

Давайте называть Π^1_n-σ_+-формулу *специальной*, если она имеет вид $(\star)$.

Следствие 2.2 (см. [9]). *Совокупность всех специальных* Π^1_n-σ_+-*предложений, истинных в* $\mathfrak{N}$, *является* Π^1_n-*полной.*

Главный (и единственный) результат в [5] тривиальным образом следует из следствия выше. В [1] и [10] он был использован для получения некоторых интересных результатов о нижних оценках сложности для языков, предложенных в [4] и [11] соответственно.

2.2. Кванторная вероятностная логика

Под *вероятностным пространстваом* мы понимаем пару $\langle\mathscr{A},\mathrm{P}\rangle$, где $\mathscr{A}$ – булева алгебра, в которой у всякого счетного множества элементов есть супремум (а потому и инфимум), и P – *вероятностная мера* на $\mathscr{A}$, т.е. функция из $\mathscr{A}$ в [0, 1] такая, что для любого счетного множества S попарно непересекающихся элементов $\mathscr{A}$,

$$\mathrm{P}\Big(\bigvee S\Big)=\sum_{E\in S}\mathrm{P}(E),$$

и к тому же $\mathrm{P}(\top)=1$, где $\top$ обозначает наибольший элемент $\mathscr{A}$.

Поскольку само наше определение вероятностной меры подразумевает два различных рода объектов, нам нужны два сорта переменных: (a) *булевы переменные* X, Y, Z, ..., которые предназначены бегать по событиям; (b) *переменные по полю* x, y, z, ..., которые предназначены бегать по вещественным числам. Это, в свою очередь, приводит к расмотрению двух множеств символов:

$$\{\bot,\top,\wedge,\vee,\neg\}\quad\text{и}\quad\{0,1,+,\cdot,-,\le\},$$

а именно функциональных символов языка булевых алгебр и символов языка упорядоченных полей (где – соответствует одноместной операции). Для обозначения данной меры будет использоваться специальный символ μ.

Булевы термы строятся из $\bot$, $\top$ и булевых переменных с использованием $\wedge$, $\vee$ и $\neg$ следующим образом: если T_1 и T_2 – булевы термы, то таковы и $(T_1\wedge T_2)$, $(T_1\vee T_2)$ и $\neg T_1$. Они представляют булевы комбинации событий. Под *атомарной* QPL-*формулой* мы понимаем выражение вида

$$f(\vec{x},\mu(T_1),\dots,\mu(T_m))\le g(\vec{y},\mu(T_{m+1}),\dots,\mu(T_{m+n})),$$

где f и g суть полиномы с целыми коэффициентами, $\vec{x}$ и $\vec{y}$ – кортежи переменных по полю и T_1, ..., T_{m+n} – булевы термы.

Мы будем использовать $\wedge$, $\vee$ и $\neg$ для обозначения не только булевых операций, но также и обычных логических связок. Поскольку их булевы версии не будут встречаться вне области действия μ, интерпретации $\wedge$, $\vee$ and $\neg$ будут всегда ясны из контекста. В качестве наших кванторных символов возьмем $\forall$ и $\exists$. Тогда QPL-*формулы* строятся из атомарных QPL-формул с использованием символов логических связок и кванторов – связывающих булевы переменные или переменные по полю – обычным образом. Мы сокращаем $\neg\Phi \vee \Psi$ как $\Phi \to \Psi$ и $(\Phi \to \Psi) \wedge (\Psi \to \Phi)$ – как $\Phi \leftrightarrow \Psi$. Кроме того, $=$ и $<$ трактуются как определенные в терминах $\leq$.

Отношение выполнимости $\Vdash$ для QPL может быть определено очевидным образом, и оно ведет себя так, как можно ожидать. Например, рассмотрим

$$\Theta := \forall x(0 \leq x \leq 1 \to \exists Y \mu(Y) = x).$$

Пусть $\mathcal{P} = \langle \mathcal{A}, \mathrm{P}\rangle$ – вероятностное пространство. Тогда $\mathcal{P} \Vdash \Theta$, если и только если для каждого $r \in [0,1]$ существует $E \in \mathcal{A}$ такое, что $\mathrm{P}(E) = r$.

Замечание 2.3. *Фрагмент* QPL*, содержащий только кванторы по вещественным числам* (*но не по событиям*), *можно воспринимать как "полиномиальную" логику, описанную ранее в* [3], *разделе 6. В этой логике булевы переменные трактуются как константные символы и называются "пропозициональными переменными"; поэтому булевы термы становятся "пропозициональными формулами".*

Пусть $\mathcal{K}$ – класс вероятностных пространств. Под QPL-*теорией* $\mathcal{K}$, обозначаемой $\mathrm{Th}(\mathcal{K})$, мы понимаем совокупность всех QPL-предложений, истинных в любом пространстве из $\mathcal{K}$. Мы используем $\mathrm{Th}^{\mathrm{e}}(\mathcal{K})$ для обозначения множества предложений из $\mathrm{Th}(\mathcal{K})$, которые не содержат кванторов по вещественным числам. Мы будем часто писать $\mathrm{Th}(\mathcal{P})$ и $\mathrm{Th}^{\mathrm{e}}(\mathcal{P})$ вместо $\mathrm{Th}(\{\mathcal{P}\})$ и $\mathrm{Th}^{\mathrm{e}}(\{\mathcal{P}\})$ соответственно. Два пространства $\mathcal{P}_1$ и $\mathcal{P}_2$ называются *элементарно эквивалентными*, если их QPL-теории совпадают, т.е. $\mathcal{P}_1$ и $\mathcal{P}_2$ не различимы посредством QPL-предложений.

Используя следствие 2.2, можно получить следующее.

Теорема 2.4 (см. [8]). *Пусть $\mathcal{K}$ – класс вероятностных пространств, который содержит все бесконечные дискретные пространства. Тогда теория второго порядка $\mathfrak{N}$ m-сводима к* $\mathrm{Th}^{\mathrm{e}}(\mathcal{K})$.

3. ФАКТОР-ПРОСТРАНСТВА

Пусть $\mathcal{P} = \langle \mathcal{A}, \mathrm{P}\rangle$ – вероятностное пространство. Рассмотрим формулу

$$X \approx Y := \mu((X \wedge \neg Y) \vee (Y \wedge \neg X)) = 0.$$

Она определеляет весьма естественное отношение эквивалентности на $\mathcal{A}$, а именно

$$\mathcal{E} := \{(E_1, E_2) \in \mathcal{A} \times \mathcal{A} \mid \mathcal{P} \Vdash E_1 \approx E_2\}.$$

Для каждого $E \in \mathcal{A}$ обозначим через $[E]_{\approx}$ класс эквивалентности E по $\mathcal{E}$. Теперь возмем $\mathcal{A}_{\approx}$ равным совокупности всех таких классов эквивалентности и определим функцию $\mathrm{P}_{\approx}$ из $\mathcal{A}_{\approx}$ в $[0, 1]$ посредством

$$\mathrm{P}_{\approx}([E]_{\approx}) := \mathrm{P}(E).$$

Нетрудно проверить, что $\mathcal{P}_{\approx} = \langle \mathcal{A}_{\approx}, \mathrm{P}_{\approx}\rangle$ является вероятностным пространством, которое называется *фактор-пространством $\mathcal{P}$ по модулю $\mathcal{E}$*. Более того, QPL-теории $\mathcal{P}$ и $\mathcal{P}_{\approx}$ совпадают.

Замечание 3.1. *Что касается языков из* [4], *мы не можем безопасно переходить от структур к их фактор-структурам по модулю событий меры ноль, поскольку теория данной структуры может отличаться от теории ее фактор-структуры* (*см. дискуссию в* [8]).

Напомним, что $E \in \mathcal{A}$ является *атомом* $\mathcal{A}$, если $E \neq \bot$ (где $\bot$ обозначает наименьший элемент $\mathcal{A}$) и для каждого $F \in \mathcal{A}$ мы имеем $E \wedge F = \bot$ или $E \wedge F = E$. Рассмотрим формулу

$$\mathrm{At}(X) := \mu(X) \neq 0 \wedge \forall Y(\mu(X \wedge Y) = 0 \vee X \wedge Y \approx X).$$

Очевидно, $\mathcal{P} \Vdash \mathrm{At}(E)$ тогда и только тогда, когда $[E]_{\approx}$ является атомом $\mathcal{A}_{\approx}$. Мы называем $\mathcal{P}$ *безатомным*, если $\mathcal{P} \Vdash \neg\exists X\,\mathrm{At}(X)$. Например, пространство Лебега на $[0, 1]$ является безатомным. Разумеется, существуют альтернативные определения безатомности, но приведенное выше – в духе булевых алгебр; ср. [6].

Теорема 3.2. *Любые два безатомных вероятностных пространства элементарно эквивалентны. Кроме того,* QPL-*теория безатомных вероятностных пространств разрешима.*

Это наводит на мысль, что хорошая "элементарная" классификация вероятностных пространств должна основываться на понятии атома (ср. [6]). Вместе с тем теорема выше обобщает результат Тарского о том, что первопорядковая теория упорядоченного поля вещественных чисел является разрешимой; см. [12].

4. ЭЛЕМЕНТАРНЫЕ ИНВАРИАНТЫ

Пусть $\mathcal{P} = \langle \mathcal{A}, \mathrm{P}\rangle$ – вероятностное пространство. Возьмем $\mathcal{D}$ равным совокупности всех атомов $\mathcal{A}_{\approx}$. Под *элементарным инвариантом* $\mathcal{P}$ мы

понимаем функцию $\sharp_{\mathcal{P}}$ из $(0,+\infty)$ в $\mathbb{N}$, заданную посредством

$$\sharp_{\mathcal{P}}(r) := \text{число элементов в} \{D \in \mathcal{D} | \mathrm{P}_{\approx}(D) = r\}.$$

Значит, в частности, $\mathcal{P}$ является безатомным, если и только если $\sharp_{\mathcal{P}}$ – функция, тождественно равная нулю.

Поскольку дискретные пространства состоят из атомов, их элементарные инварианты могут рассматривать как их абстрактные представления. К примеру, рассмотрим дискретное распределение g на $\mathbb{N}$, заданное посредством

$$g(n) := \frac{1}{2^{n+1}}.$$

Пусть $\mathcal{P} = \langle \mathcal{A}, \mathrm{P} \rangle$ – соответствующее вероятностное пространство. Значит, $\mathcal{A}$ – совокупность всех подмножеств $\mathbb{N}$ и для каждого $E \subseteq \mathbb{N}$ мы имеем

$$\mathrm{P}(E) = \sum_{n \in E} g(n).$$

Тогда $\mathcal{D} = \{\{n\} | n \in \mathbb{N}\}$ и для любого положительного $r \in \mathbb{R}$,

$$\sharp_{\mathcal{P}}(r) = \begin{cases} 1 & \text{если } r = \frac{1}{2}, \frac{1}{4}, \frac{1}{8}, \ldots \\ 0 & \text{иначе.} \end{cases}$$

Таким образом, $\sharp_{\mathcal{P}}$ очень похож на g. Как было показано в [8], $\mathrm{Th}(\mathcal{P})$ и $\mathrm{Th}^{\mathrm{e}}(\mathcal{P})$ обе m-эквивалентны теории второго порядка $\mathfrak{N}$.

Теорема 4.1. *Для любых вероятностных пространств $\mathcal{P}_1$ и $\mathcal{P}_2$,*

$$\sharp_{\mathcal{P}_1} = \sharp_{\mathcal{P}_2} \Leftrightarrow \mathrm{Th}(\mathcal{P}_1) = \mathrm{Th}(\mathcal{P}_2).$$

Другими словами, два пространства имеют один и тот же инвариант, если и только если они элементарно эквивалентны.

Замечание 4.2. *Аналогичные формулировки возникают в метаматематике булевых алгебр*; *ср.* [6]. *Хотя эти два направления исследований явно связаны, они в некотором смысле несравнимы*, *поскольку* QPL *имеет дело с мерами на булевых алгебрах специального рода.*

Для наших текущих целей мы можем отождествить каждое пространство с его элементарным инвариантом. Отметим, что такие инварианты могут быть легко закодированы как подмножества $\mathbb{N}$. Назовем класс пространств $\mathcal{K}$ *аналитическим*, если $\{\sharp_{\mathcal{P}} | \mathcal{P} \in \mathcal{K}\}$ определимо в $\mathfrak{N}$ (как множество подмножетсв $\mathbb{N}$).

Теорема 4.3. *Пусть $\mathcal{K}$ – аналитический класс пространств. Тогда $\mathrm{Th}(\mathcal{K})$ m-сводима к теории второго порядка $\mathfrak{N}$.*

Это приводит к следующему.

Следствие 4.4. *Пусть $\mathcal{K}$ – аналитический класс пространств*, *который содержит все бесконечные дискретные пространства. Тогда $\mathrm{Th}(\mathcal{K})$ m-эквивалентна теории второго порядка $\mathfrak{N}$.*

Доказательство. Непосредственно из Теорем 2.4 и 4.3.

В частности, Следствие 4.4 применимо к классу всех пространств и классу всех бесконечных пространств. Это решает одну из главных проблем, заявленных в [8].

ИСТОЧНИК ФИНАНСИРОВАНИЯ

Исследование выполнено за счет гранта Российского научного фонда № 21-11-00318; см. https://rscf.ru/project/21-11-00318/.

СПИСОК ЛИТЕРАТУРЫ

1. *Abadi M., Halpern J.Y.* Decidability and expressiveness for first-order logics of probability // Information and Computation. 1994. V. 112. № 1. P. 1–36.
2. *Ershov Yu.L., Lavrov I.A., Taimanov A.D., Taitslin M.A.* Elementary theories // Russian Mathematical Surveys. 1965. V. 20. № 4. P 35–105.
3. *Fagin R., Halpern J.Y., Megiddo N.* A logic for reasoning about probabilities // Information and Computation. 1990. V. 87. № 1–2. P. 78–128.
4. *Halpern J.Y.* An analysis of first-order logics of probability // Artificial Intelligence. 1990. V. 46. № 3. P. 311–350.
5. *Halpern J.Y.* Presburger arithmetic with unary predicates is Π^1_1 complete // Journal of Symbolic Logic. 1991. V. 56. № 2. P. 637–642.
6. *Koppelberg S.* General theory of Boolean algebras // in *Handbook of Boolean Algebras*, Vol. 1, Ed. by Monk J.D., Bonnet R. (North-Holland, 1989), P. 1–311.
7. *Solovay R.M., Arthan R.D., Harrison J.* Some new results on decidability for elementary algebra and geometry // Annals of Pure and Applied Logic. 2012. V. 163. № 12. P. 1765–1802.
8. *Speranski S.O.* Quantifying over events in probability logic: an introduction // Mathematical Structures in Computer Science. 2017. V. 27. № 8. P. 1581–1600.
9. *Speranski S.O.* A note on definability in fragments of arithmetic with free unary predicates // Archive for Mathematical Logic. 2013. V. 52. № 5–6. P. 507–516.
10. *Speranski S.O.* Complexity for probability logic with quantifiers over propositions // Journal of Logic and Computation. 2013. V. 23. № 5. P. 1035–1055.
11. *Speranski S.O.* Quantification over propositional formulas in probability logic: decidability issues // Algebra and Logic. 2011. V. 50. № 4. P. 365–374.
12. *Tarski A.* A Decision Method for Elementary Algebra and Geometry (University of California Press, 1951).

ELEMENTARY INVARIANTS FOR QUANTIFIED PROBABILITY LOGIC

S. O. Speranski[a]

[a] *Steklov Mathematical Institute of Russian Academy of Sciences, Moscow, Russian Federation*

Presented by Academician of the RAS L.D. Beklemishev

Let QPL be the two-sorted probabilistic language proposed in [8], which expands the well-known 'polynomial' language described in [3, Section 6] by adding quantifiers over events. We show that all atomless spaces have the same QPL-theory, and this theory is decidable. Also we introduce the notion of elementary invariant for QPL and use it for obtaining exact complexity upper bounds for some interesting probabilistic theories.

Keywords: probability logic, quantification over events, elementary invariants, complexity