# Монадическое исчисление и проблема разрешимости

Ж. Мияйлович

В статье рассматривается логика исчисления предикатов первого порядка с точки зрения автоматического доказательства теорем. На примере монадического исчисления иллюстрируется использование модельно-теоретического метода, метода элиминации кванторов и метода интерпретации в доказательствах разрешимости теорий.

## 1. Введение

Целью автоматического доказательства теорем является создание и реализация программ для нахождения доказательств. Возможные применения этой области распространяются, кроме всего прочего, и на верификацию программ, создание экспертных систем, вплоть до применения в коммуникации "человек — вычислительная машина" в форме вопросов и ответов. Доказатели этого типа обычно имеют универсальный характер, то есть, могут применяться к любым аксиоматическим теориям первого порядка. В этой статье мы рассмотрим проблему автоматического доказательства теорем для особого класса теорий, а именно для *разрешимых теорий исчисления предикатов первого порядка* [1].

Анализ разрешимости какой-либо теории $T$ сводится к вопросу о существовании алгоритма, с помощью которого можно установить для любого предложения $\varphi$, записанного в формализме теории $T$, является ли $\varphi$ теоремой этой теории или нет. Если $T$ — разрешимая теория,

[1] Далее сокращением ИП[1] будем обозначать исчисление предикатов первого порядка, а понятие теории будет относиться к теории этой логики, если не оговорено иначе.

то вопрос о том, является ли $\varphi$ теоремой или нет, становится тривиальным. Действительно, применение любого алгоритма не требует изобретательности или особых умственных усилий. Таким образом, разрешимые теории с математической точки зрения являются простыми и неинтересными. Такое мнение существовало до тех пор, пока не обнаружили (в 70-х годах Фишер, Мэйер, Рабин), что многие теории, хотя и считаются разрешимыми, с практической точки зрения таковыми не являются, поскольку алгоритм разрешимости требует огромного числа вычислительных шагов, что часто не осуществимо даже с помощью современных вычислительных машин. Например, обнаружено, что в арифметике Пресбурга для каждого алгоритма $\mathcal{A}$ и каждого натурального числа $n$ существует предложение $\varphi$ длины $n$, для которого нужно $2^{2^n}$ шагов при применении алгоритма $\mathcal{A}$ к $\varphi$. С другой стороны, многие простые высказывания арифметики Пресбурга записываются более чем 50-ю символами, а $2^{2^{50}}$ вычислительных шагов нельзя считать разумной процедурой при утверждении математической истины. Оказалось, что эти алгоритмы такие же сложные, как и алгоритмы для разрешимости исчисления высказываний, а известно, что вопрос о разрешимости этого исчисления связан с центральной, до сих пор еще открытой проблемой теоретического программирования:

*Имеет ли место равенство* **P=NP***?*

**P=NP** представляет собой вопрос о том, является ли недетерминированное вычисление с полиномиальным по отношению к величине входных данных числом шагов эквивалентным обыкновенному (детерминированному) вычислению, которое также имеет полиномиальное число вычислительных шагов. Эта проблема формализована в теории разрешимости в терминах машин Тьюринга и формальных языков. Интересно, что центральную роль в анализе и разрешении этой проблемы занимает обыкновенное исчисление высказываний, а именно, следующий вопрос:

> *Существует ли многочлен $p(x)$ и (детерминированный) алгоритм, который за не более чем $p(n)$ шагов (то есть, за полиномиальное число вычислительных шагов) для произвольной формулы высказывания из $n$ символов утверждает, является ли эта формула тавтологией?*

С. А. Кук доказал [3], что из существования такого алгоритма вытекает положительное решение проблемы **P=NP**, а отсюда следует, что для большого числа математических проблем (теории графов, комбинаторики, вычислительной математики, математического программирования, логики и т.д.) также должны существовать алгоритмы, которые решают эти проблемы за полиномиальное время. При нынешнем положении дел это значило бы, что эти проблемы можно было бы решить не только "в принципе", но и в "реальном времени" с учетом всех ограничений, касающихся объема памяти, скорости процессора и времени вычисления, а не только "в принципе". Под фразой "в принципе" мы подразумеваем только то, что существует алгоритм в смысле теории формальной вычислимости, который решает данную проблему, но, либо вопрос о сложности такого алгоритма остается открытым, либо алгоритм невозможно реализовать в реальном времени. В соответствии с вышеизложенным, решение проблемы **P=NP** для прикладной математики имеет важное значение.

## 1.1. Теории первого порядка

Главными методами для доказательства разрешимости теорий исчисления предикатов первого порядка являются следующие:

- Методы теории моделей.
- Методы элиминации кванторов.
- Метод интерпретации.
- Метод семантических таблиц.
- Методы теории автоматов.

В каждом из этих подходов важную роль имеют следующие теоремы:

**Теорема 1.1.1.** *Если $T$ — аксиоматическая и полная теория, то $T$ разрешима.*

Напомним, что $T$ называется аксиоматической теорией, если существует рекурсивное множество аксиом, то есть, если аксиомы теории $T$

можно эффективно перечислить. С другой стороны, $T$ является полной, если для каждого предложения $\varphi$, записанного в формализме теории $T$, имеет место: либо $\varphi$, либо $\neg\varphi$ является теоремой теории $T$.

**Теорема 1.1.2 (Ю. Ершов).** *Теория $T$ является разрешимой тогда и только тогда, когда существует счетная последовательность полных теорий $T_i$, которые можно эффективно перечислить, так что*

$$T = \cap_i T_i.$$

Говорим, что последовательность теорий $T_i$ можно эффективно перечислить, если существует рекурсивная функция $g$ двух переменных, так что для любого $i$

$$\{g(i,j) : j \in N\} = \{\wp\varphi : \varphi \in T_i\},$$

где $\wp\varphi$ является номером Геделя формулы $\varphi$. Следующий пример представляет особый случай предыдущей теоремы, и, благодаря этому, является очень эффективным в приложениях.

**Теорема 1.1.3.** *Если теория $T$ имеет только счетное количество полных расширений $T_n$, и если их можно эффективно перечислить, то $T$ — разрешимая теория.*

**Доказательство.** Предположим, что $T_n$, $n = 0, 1, 2, \ldots$, есть эффективное и равномерное перечисление всех полных расширений теории $T$, и пусть $\theta \in Sent_L$. Согласно предположению, все теоремы теории $T_n$ можно эффективно и одновременно перечислить способом, показанным на диаграмме.

$$\begin{array}{ll} T_0 \vdash \varphi_{00}, \varphi_{01}, \varphi_{02}, \ldots & T_0 \vdash \psi_0, \psi_1, \psi_3, \ldots \\ T_1 \vdash \varphi_{10}, \varphi_{11}, \varphi_{12}, \ldots & T_1 \vdash \psi_2, \psi_4, \psi_7, \ldots \\ T_2 \vdash \varphi_{20}, \varphi_{21}, \varphi_{22}, \ldots & T_2 \vdash \psi_5, \psi_8, \psi_{12}, \ldots \\ T_3 \vdash \varphi_{30}, \varphi_{31}, \varphi_{32}, \ldots & T_3 \vdash \psi_9, \psi_{13}, \psi_{18}, \ldots \end{array}$$
$$\ldots\ldots\ldots\ldots$$

Здесь $\varphi_{ij} = \psi_{c(i,j)}$, где

$$c(i,j) = \binom{i+j+1}{2} + i$$

функция Кантора для перечисления пар натуральных чисел. Поскольку $T$ является аксиоматической теорией, то существует рекурсивное перечисление всех теорем теории $T$: $\varphi_0, \varphi_1, \varphi_2, \ldots$. Отсюда имеем:

$$\varphi_0,\ \psi_0,\ \varphi_1,\ \psi_1,\ \varphi_2,\ \psi_2,\ \ldots \tag{1}$$

также есть рекурсивное перечисление некоторых предложений языка $L$. Значит, если $T \vdash \theta$, тогда $\theta = \varphi_n$ для некоторого $n$. Если $\theta$ не является теоремой теории $T$, тогда $T \cup \{\neg\theta\}$ есть непротиворечивая теория, и существует модель $\mathbf{A}$ теории $T$, такая, что $\mathbf{A} \models \neg\theta$. Согласно выбору теорий $T_n$, существует $i$ такое, что множество высказываний, истинных в $\mathbf{A}$, равно $T_i$, и тогда $T_i \vdash \neg\theta$. Значит, существует $j$, такое, что $\neg\theta = \varphi_{ij} = \psi_{c(i,j)}$. Отсюда $\theta$ должна появиться на каком-то четном шаге (т.е. для некоторого $i$, $\theta = \varphi_i$), или $\neg\theta$ должна появиться на каком-то нечетном шаге (т.е. для некоторого $i$, $\theta = \psi_i$) последовательности (1). Согласно этому, алгоритм для эффективного перечисления последовательности (1) даст процедуру разрешимости для теории $T$. $\diamondsuit$

На примере монадического исчисления проиллюстрируем модельно-теоретический метод, метод элиминации кванторов и метод интерпретации в доказательствах разрешимости теорий первого порядка. Применение метода семантических таблиц описано в статье Капетановича и Крапежа [18], где предлагается универсальный доказатель для ИП[1].

## 2. Монадическое исчисление

Следующий пример иллюстрирует некоторые идеи, которые уже были рассмотрены в предыдущем разделе. Рассмотрим т.н. *монадическое исчисление* в исчислении предикатов первого порядка с отношением равенства. Это исчисление, которое мы будем обозначать через **M**, известно еще как теория первого порядка унарных отношений. Отметим попутно, что Л. Левенгейм еще в 1915 году доказал разрешимость исчисления **M** без отношения равенства. Классический пример монадического исчисления представляют силлогизмы Аристотеля [11]. Например, для свойств M, P, S силлогизм *Barbara* [11, стр. 53],

$$\begin{array}{l} \text{aMP} \\ \underline{\text{aSM}}, \\ \text{aSP} \end{array} \quad \text{который интерпретируется как} \quad \begin{array}{l} \text{каждое M есть P} \\ \underline{\text{каждое S есть M}}, \\ \text{каждое S есть P} \end{array}$$

сводится к исследованию общезначимости (логической истинности) формулы предикатов

$$\forall x(Mx \Rightarrow Px) \wedge \forall x(Sx \Rightarrow Mx) \Rightarrow \forall x(Sx \Rightarrow Px).$$

Учитывая, что формула общезначима, следовательно и силлогизм *Barbara* является логически верным.

## 2.1. Решение с помощью теории моделей

Монадическое исчисление $\mathbf{M}$ представляет в сущности теорию первого порядка унарных отношений. В соответствии с этим язык (множество нелогических символов) этой теории выглядит так:

$$L = \{P_0, P_1, ..., P_{n-1}, ...\},$$

где $P_i$ — одноместные предикаты (символы отношений), в то время как в качестве аксиом используются только логические аксиомы исчисления предикатов. Таким образом, не существует особых аксиом для предикатов $P_i$. Монадическое исчисление с $n$ предикатами (обозначается $\mathbf{M}_n$) является сужением теории $\mathbf{M}$ на фрагмент $L_M = \{P_0, P_1, ..., P_{n-1}\}$ языка $L$, в то время как модели этой теории имеют вид

$$\mathbf{A} = (A, S_0, S_1, ..., S_{n-1}),$$

где $A$ — непустое множество и $S_0, S_1, ..., S_{n-1} \subseteq A$. Модели этого типа будем называть *монадическими моделями*. Если $\varphi$ есть предложение языка $L$, то по теореме о полноте исчисления предикатов имеет место

(2) $\mathbf{M} \vdash \varphi$ тогда и только тогда, когда $\varphi$ истинно на всех монадических моделях.

Напомним читателю, что обозначение $\mathbf{M} \vdash \varphi$ означает, что $\varphi$ является теоремой теории $\mathbf{M}$. Свойство (2) представляет фундаментальную связь между синтаксическими и семантическими свойствами теории ИП[1], и этот факт будет одним из ключевых шагов в модельно-теоретическом доказательстве разрешимости монадического исчисления.

Прежде чем привести это доказательство, введем следующие обозначения. Пусть $1 = \{0\}$, $2 = \{0, 1\}$, $3 = \{0, 1, 2\}$, ... . Тогда $2^n$ есть множество отображений множества $n = \{0, 1, 2, ..., n-1\}$ в 2, и для $\alpha \in 2^n$

имеем $\alpha = (\alpha_0, ..., \alpha_{n-1})$, $\alpha_i \in \{0, 1\}$, $1 \leq i \leq n$. Поскольку в этом случае $\alpha$ есть бинарная последовательность, можно считать, что $\alpha$ — натуральное число, и что $\alpha_0, ..., \alpha_{n-1}$ суть его цифры в двоичном представлении. Наконец, если $P_0, P_1, ..., P_{n-1}$ есть последовательность символов предикатов и $\alpha \in 2^n$, тогда

$$P^\alpha \stackrel{\text{def}}{=} P_0^{\alpha_0} \wedge P_1^{\alpha_1} \wedge ... \wedge P_{n-1}^{\alpha_{n-1}},$$

где $P_j^0 = \neg P_j$ и $P_j^1 = P_j$. Аналогично, если $S_0, S_1, ..., S_{n-1}$ есть последовательность подмножеств некоторой области, тогда

$$S^\alpha \stackrel{\text{def}}{=} S_0^{\alpha_0} \cap S_1^{\alpha_1} \cap ... \cap S_{n-1}^{\alpha_{n-1}},$$

где $S_j^0 = S_j^c$ и $S_j^1 = S_j$. Кардинальное число (число элементов) множества $A$ будем обозначать через $|A|$.

**Лемма 2.1.1.** *Пусть* $\mathbf{A} = (A, S_0, S_1, ..., S_{n-1})$ *и* $\mathbf{B} = (B, R_0, \ldots, R_{n-1})$ — *монадические модели.* $\mathbf{A}$ *и* $\mathbf{B}$ *изоморфны тогда и только тогда, когда*

$$\bigwedge_{\alpha \in 2^n} |S_i^\alpha| = |R_i^\alpha| \qquad \text{для всех } i = 0, 1, 2, \ldots, n-1. \tag{3}$$

**Доказательство.** Предположим, что выполнено условие (3). Множества $\{S^\alpha | \ \alpha \in 2^n\}$ и $\{R^\alpha | \ \alpha \in 2^n\}$ являются соответственно разбиениями областей $A$ и $B$, и согласно предположению (3), существуют биективные отображения $f_\alpha : S^\alpha \to R^\alpha$, $\alpha \in 2^n$. Тогда $f = \bigcup_{\alpha \in 2^n} f_\alpha$ есть изоморфизм моделей $\mathbf{A}$ и $\mathbf{B}$.

С другой стороны, изоморфизм моделей $\mathbf{A}$ и $\mathbf{B}$ очевидно влечет за собой условие (3), тем самым лемма доказана. $\diamondsuit$

Предыдущая лемма наводит нас на идею о введении нумерических констант следующего типа для каждой монадической модели.

**Определение 2.1.1.** *Пусть* $\mathbf{A} = (A, S_0, ..., S_{n-1})$ — *монадическая модель. Тип модели* $\mathbf{A}$ *есть* $\tau\mathbf{A} = (\tau_0, \tau_1, ..., \tau_{2^n-1}) = \langle \tau_\alpha | \alpha \in 2^n \rangle$, *где для* $\alpha \in 2^n$

$$\tau_\alpha = \begin{cases} |S^\alpha| & \text{если } |S^\alpha| \text{ конечно.} \\ \infty & \text{если } |S^\alpha| \text{ бесконечно.} \end{cases}$$

**Пример 2.1.1.** Пусть:
область интерпретации — множество натуральных чисел $N = \{0, 1, 2, ...\}$,
$S_0$ — множество четных чисел, т.е. $S_0 = 2N = \{0, 2, 4, ...\}$ и
$S_1$ — множество простых чисел, т.е. $S_1 = \{2, 3, 5, 7, 11, ...\}$.

Заметим, что $2^2 = \{\alpha, \beta, \gamma, \delta\}$, где $\alpha = (11)$, $\beta = (10)$, $\gamma = (01)$, $\delta = (00)$ и что для $\mathbf{N} = (N, S_0, S_1)$, $\tau\mathbf{N} = (|S^\alpha|, |S^\beta|, |S^\gamma|, |S^\delta|)$. С другой стороны,

$$\begin{array}{rcccl} S^\alpha = & S_0 \cap S_1 = & 2N \cap P & = & \{2\}, \\ S^\beta = & S_0 \cap S_1^c = & 2N \cap P^c & = & 2N - P, \\ S^\gamma = & S_0^c \cap S_1 = & (2N+1) \cap P & = & P - \{2\}, \\ S^\delta = & S_0^c \cap S_1^c = & (2N+1) \cap P^c & = & (2N+1) - P. \end{array}$$

Отсюда находим, что $\tau N = (1, \infty, \infty, \infty)$.

В следующем предложении мы будем пользоваться понятием *элементарной эквивалентности* моделей. О двух моделях $\mathbf{A}$ и $\mathbf{B}$ одного и того же языка $L$ говорим, что они *элементарно эквивалентны* (обозначается $\mathbf{A} \equiv \mathbf{B}$), если $\mathbf{A}$ и $\mathbf{B}$ имеют одинаковые свойства первого порядка, т.е. $\mathbf{A} \models \varphi$ тогда и только тогда, когда $\mathbf{B} \models \varphi$, где $\varphi$ — предложение языка $L$.

**Теорема 2.1.1.** 1. *Пусть* $\mathbf{A}$ *и* $\mathbf{B}$ — *не более чем счетные монадические модели. Тогда, чтобы*

$$\mathbf{A} \cong \mathbf{B}, \text{ } \textit{необходимо и достаточно } \tau\mathbf{A} = \tau\mathbf{B}.$$

2. *Пусть* $\mathbf{A}$ *и* $\mathbf{B}$ — *произвольные монадические модели. Тогда, чтобы*

$$\mathbf{A} \equiv \mathbf{B}, \text{ } \textit{необходимо и достаточно } \tau\mathbf{A} = \tau\mathbf{B}.$$

**Доказательство.** 1. Это предложение является непосредственным следствием Леммы 2.1.1.
2. Сначала заметим, что имеют место следующие условия:

$$|S^\alpha| = r \Leftrightarrow \exists x_0 \dots x_{r-1} \Big( \bigwedge_{i<j<r} x_i \neq x_j \wedge \forall y (S^\alpha(y) \Leftrightarrow \bigvee_{i<r} y = x_i) \Big)$$

$$|S^\alpha| = \infty \Leftrightarrow \bigwedge \Phi_\alpha(S),$$

где $(\Phi_\alpha(S) = \{\varphi_n |\ n \in N\})$ и $\varphi_n = \bigwedge_{r<n} |S^\alpha| \neq r$. Для предложения $\varphi_n$ имеет место также следующая эквивалентность:

$$\varphi_n \Leftrightarrow \exists x_0 x_1 \dots x_{n-1}(\bigwedge_{i<j<n} x_i \neq x_j \wedge \bigwedge_{i<n} S^\alpha(x_i)).$$

Для $r_0, r_1, \dots r_{2^k-1} \in N \bigcup \{\infty\}$ несложно найти множество предложений $\Sigma_r$, так что для каждой монадической модели $\mathbf{A} = (A, S_0, S_1, \dots, S_{k-1})$ имеет место:

(4) $\tau\mathbf{A} = (r_0, r_1, \dots r_{2^k-1})$ тогда и только тогда, когда в $\mathbf{A}$ истинны все предложения из $\Sigma_r$.

Действительно, пусть

$$\Delta = \{\alpha \in 2^k |\ r_\alpha < \infty\}, \quad \Gamma = \{\alpha \in 2^k |\ r_\alpha = \infty\}.$$

Тогда

(5) $$\Sigma_r = \{|S^\alpha| = r_\alpha |\ \alpha \in \Delta\} \cup \bigcup_{\alpha \in \Gamma} \Phi_\alpha(S).$$

Пусть

$$\mathbf{A} = (A, S_0, S_1, \dots, S_{k-1}),\ \mathbf{B} = (B, R_0, R_1, \dots, R_{k-1}),\ \tau\mathbf{B} = (r_0, r_1, \dots r_{2^k-1})$$

и $\Sigma_r$ есть множество формул (5). Тогда из $\mathbf{A} \equiv \mathbf{B}$ следует, что в $\mathbf{A}$ и в $\mathbf{B}$ истинны одни и те же предложения, и, поскольку в $\mathbf{B}$ истинны все предложения из $\Sigma_r$, то и в $\mathbf{A}$ истинны все предложения из $\Sigma_r$, и, в соответствии с (4), $\tau\mathbf{A} = (r_0, r_1, \dots, r_{2^k-1}) = \tau\mathbf{B}$. Но если $\tau\mathbf{A} = \tau\mathbf{B}$ и если $\mathbf{A}$ и $\mathbf{B}$ — счетные модели, то из п.1 следует, что $\mathbf{A} \cong \mathbf{B}$, а также и $\mathbf{A} \equiv \mathbf{B}$. Если какая-либо из моделей $\mathbf{A}$ и $\mathbf{B}$ не является счетной, то по теореме Левенгейм-Сколема существуют перечислимые модели $\mathbf{A}'$ и $\mathbf{B}'$, такие, что $\mathbf{A}' \equiv \mathbf{A}$ и $\mathbf{B}' \equiv \mathbf{B}$. Учитывая, что $\tau\mathbf{A} = \tau\mathbf{B}$, согласно (4), в $\tau\mathbf{A}$ и $\tau\mathbf{B}$ истинны предложения из $\Sigma_r$, следовательно и в $\mathbf{A}'$ и $\mathbf{B}'$ истинны предложения из $\Sigma_r$, а значит, $\tau\mathbf{A}' = \tau\mathbf{B}'$. Тогда в соответствии с п.1, $\mathbf{A}' \cong \mathbf{B}'$, следовательно $\mathbf{A}' \equiv \mathbf{B}'$. Поскольку отношение $\equiv$ транзитивно, получаем, что $\mathbf{A} \equiv \mathbf{B}$. $\diamondsuit$

Теория $T$ является полным расширением монадического исчисления тогда и только тогда, когда существует монадическая модель $\mathbf{A}$, в которой имеют место все теоремы теории $T$. Отсюда, по Теореме 2.1.1 все

полные расширения монадического исчисления $\mathbf{M}_k$ определены типами моделей вида $\mathbf{A} = (A, S_0, S_1, \ldots, S_{k-1})$, то есть $2^k$-местными кортежами $(r_0, r_1, \ldots r_{2^k-1})$, $r_i \in N \cup \{\infty\}$. Например, каждое полное расширение монадического исчисления с двумя предикатами $P_0$ и $P_1$ определено одним из 16 типов:

$$(a, b, c, d),\ (a, b, c, \infty),\ (a, b, \infty, d), \ldots, (\infty, \infty, \infty, \infty),$$

где $a, b, c, d \in N$, $a + b + c + d \geq 1$. Заметим, что конечной модели $(A, S_0, S_1)$ соответствует первый тип из этой последовательности (и в этом случае $|A| = a + b + c + d$), в то время как бесконечным моделям соответствуют остальные типы из этой последовательности.

В соответствии с вышесказанным, монадическое исчисление $\mathbf{M}_k$ с $k$ предикатами имеет счетное число полных расширений, и все они могут быть эффективно, равномерно и одновременно перечислены, т.е. существует примитивно-рекурсивная функция $f$, такая что

$$\wp T_i = \{f(i, j) | j \in N\},$$

где $\langle T_i |\ i \in I\rangle$ является последовательностью *всех* полных расширений теории $\mathbf{M}_k$, а $\wp T_i$ есть множество кодов аксиом Геделя теории $T_i$. Согласно Теореме 1.1.3 $M_k$ является разрешимой теорией для каждого $k \in N$. С другой стороны, если $\varphi$ — произвольное предложение монадического исчисления $\mathbf{M}$, и, учитывая, что $\varphi$ содержит только конечное число предикатов, существует $k \in N$, (например, если $k$ равно числу символов предикатов в $\varphi$), так что

$$\mathbf{M} \vdash \varphi \text{ тогда и только тогда, когда } \mathbf{M}_k \vdash \varphi,$$

следовательно, и $\mathbf{M}$ — разрешимая теория. Заметим, однако, что процедура разрешимости для монадического исчисления, которая основывается на этом доказательстве, очень неэффективна. А именно, уже для самых простых предложений этот алгоритм имеет такое большое число вычислительных шагов, что его невозможно осуществить в реальном времени даже с помощью имеющихся сейчас самых мощных вычислительных машин. Таким образом, это доказательство разрешимости монадического исчисления подтверждает принципиальное существование алгоритма, но ничего не говорит о его сложности. Вышеизложенное

свидетельствует и о других свойствах монадического исчисления, например, что существует точно счетное количество пополнений. Разрешимость этой теории получена попутно, на основе анализа структуры полных расширений монадического исчисления. В следующих параграфах мы увидим некоторые более эффективные процедуры разрешимости.

Напомним, что мы смогли получить доказательство предыдущей теоремы, пользуясь так называемыми насыщенными моделями монадического исчисления. Точнее, можно показать, что типы этих моделей выглядят так: в случае конечной модели имеем типы $(a, b, c, d)$, $a, b, c, d \in N$, а в случае бесконечной модели тип имеет форму $(\infty, \infty, \infty, \infty)$, и утверждение теоремы следует из единственности этих структур.

## 2.2. Элиминация кванторов

Теория $T$ *допускает элиминацию кванторов* по отношению к множеству предложений $\Lambda$, если для каждого предложения $\varphi$ языка этой теории существует булевская комбинация формул из $\Lambda$ эквивалентная $\varphi$. Иными словами, существует формула высказываний $\psi(p_1, p_2, ..., p_n)$ и $\lambda_1, \lambda_2, ..., \lambda_n \in \Lambda$, так что

$$T \vdash \varphi \Leftrightarrow \psi(\lambda_1, \lambda_2, ..., \lambda_n).$$

Мы пользуемся понятием элиминации кванторов, поскольку формула высказываний $\psi(p_1, p_2, ..., p_n)$ не содержит кванторов. В этом разделе мы определим одно множество $\Lambda$, в отношении которого монадическое исчисление допускает элиминацию кванторов, что приведет нас к альтернативному доказательству разрешимости этой теории.

В дальнейшем изложении будем пользоваться следующими обозначениями для любого предиката $S(x)$:

$$\exists_r x S(x) \Leftrightarrow \exists x_0 \dots x_{r-1}\Big(\bigwedge_{i<j<r} x_i \neq x_j \wedge \bigwedge_{i<r} S(x_i)\Big).$$

$\exists_r x S(x)$ выражает свойство, что $S(x)$ истинно хотя бы для $r$ элементов, т.е. имеет место $\exists_r x S(x) \Leftrightarrow r \leq |S|$. Также введем и квантор $\exists_r^\flat$ следующим способом:

$$\exists_r^\flat x S(x) \Leftrightarrow \exists x_0 \dots x_{r-1}\Big(\bigwedge_{i<j<r} x_i \neq x_j \wedge \forall y(S(y) \Leftrightarrow \bigvee_{i<r} y = x_i)\Big).$$

Предложение $\exists_r^\flat x S(x)$ выражает свойство, что $S(x)$, истинно ровно для $r$ элементов, т.е. имеет место $\exists_r^\flat x S(x) \Leftrightarrow |S| = r$. Заметим, что это свойство можно описать и так:

$$\exists_r^\flat x S(x) \Leftrightarrow \exists_r x S(x) \wedge \neg \exists_{r+1} x S(x).$$

Также введем следующие сокращения: $+S = S$, $-S = \neg S$. Тогда $\pm S$ обозначает один из предикатов $S$, $\neg S$. Далее заметим, что

$$\exists x(\bigwedge_{i<s} x \neq z_i \wedge \bigwedge_{i<j<s} z_i = z_j \wedge S(x)) \Leftrightarrow \exists x(x \neq z_1 \wedge S(x)) \wedge \bigwedge_{i<j<s} z_i = z_j.$$

Для каждого разбиения $\Delta = \{\delta_0, \ldots, \delta_{s-1}\}$ множества переменных

$$Z = \{z_0, \ldots, z_{l-1}\}$$

введем конъюнкцию $\sigma_\Delta$ следующих формул:

$u = v$, если $u$ и $v$ принадлежат одному и тому же члену разбиения $\Delta$.

$u \neq v$, если $u$ и $v$ принадлежат различным членам этого разбиения.

Значит,

$$\sigma_\Delta = \bigwedge_{i<s} \bigwedge_{u,v \in \delta_i} u = v \wedge \bigwedge_{i<j<s} \bigwedge_{\substack{u \in \delta_i \\ v \in \delta_j}} u \neq v.$$

Если $\Pi$ — множество всех разбиений множества $Z$, нетрудно увидеть, что $\bigvee_{\Delta \in \Pi} \sigma_\Delta$ является тавтологией. Рассмотрим следующие примеры.

**Пример 2.2.1.** 1. Пусть $Z = \{z_0, z_1\}$ — множество переменных. Все разбиения множества $\Delta$ и соответствующие формулы $\sigma_\Delta$ следующие:

$$\begin{array}{cc} \{z_0, z_1\}, & z_0 = z_1 \\ \{z_0\},\ \{z_1\}, & z_0 \neq z_1 \end{array}$$

2. Пусть $Z = \{z_0, z_1, z_2\}$ — множество переменных. Тогда имеем:

$$\begin{array}{cc} \{z_0, z_1, z_2\}, & z_0 = z_1 \wedge z_0 = z_2 \wedge z_1 = z_2 \\ \{z_0, z_1\},\ \{z_2\}, & z_0 = z_1 \wedge z_0 \neq z_2 \wedge z_1 \neq z_2 \\ \{z_0, z_2\},\ \{z_1\}, & z_0 = z_2 \wedge z_0 \neq z_1 \wedge z_1 \neq z_2 \\ \{z_1, z_2\},\ \{z_0\}, & z_1 = z_2 \wedge z_0 \neq z_1 \wedge z_0 \neq z_2 \\ \{z_0\},\ \{z_1\},\ \{z_2\}, & z_0 \neq z_1 \wedge z_0 \neq z_2 \wedge z_1 \neq z_2 \end{array}$$

Согласно теореме о предваренной нормальной форме, теореме о дизъюнктивной нормальной форме и общезначимым формулам

$$\begin{array}{rcl} \exists x(\varphi(x) \vee \psi(x)) & \Leftrightarrow & \exists x\varphi(x) \vee \exists x\psi(x), \\ \forall x\varphi(x) & \Leftrightarrow & \neg\exists x\neg\varphi(x), \\ \exists x(\varphi(x) \wedge \psi) & \Leftrightarrow & \exists x\varphi(x) \wedge \psi, \end{array}$$

где формула $\psi$ не содержит свободную переменную $x$, можем ограничиться в наших рассуждениях формулами вида $\varphi = \exists x\theta(x)$, где $\theta(x)$ является конъюнкцией формул вида

$$x = y, \quad x \neq y, \quad S(x), \quad \neg S(x),$$

а $S(x)$ есть унарный предикат монадического исчисления. Поэтому различаем следующие случаи для $\varphi$.

**А.** $$\exists x(\bigwedge_{i<k} x = y_i \wedge \bigwedge_{i<l} x \neq z_i \wedge P^\alpha(x)),$$

где $k, l \in N$, $\alpha \in 2^n$. Но тогда очевидно

$$\varphi \Leftrightarrow \bigwedge_{i<k} y_1 = y_i \wedge \bigwedge_{i<l} y_1 \neq z_i \wedge P^\alpha(y_1).$$

Заметим, что формула с правой стороны этой эквивалентности не содержит кванторов.

**Б.** $$\exists x(\bigwedge_{i<k} x = y_i \wedge P^\alpha(x))$$

В этом случае также находим

$$\varphi \Leftrightarrow \bigwedge_{i<k} y_1 = y_i \wedge P^\alpha(y_1),$$

и здесь также формула с правой стороны этой эквивалентности не содержит кванторов.

Теперь рассмотрим самый сложный случай формулы $\varphi$:

**В.** $$\exists x(\bigwedge_{i<l} x \neq z_i \wedge P^\alpha(x)),$$

Согласно вышеизложенному, формула $\varphi$ эквивалентна формуле

$$\begin{array}{ll} \exists x & (\bigwedge\limits_{i<l} x \neq z_i \wedge (\bigvee\limits_{\Delta\in\Pi} \sigma_\Delta) \wedge P^\alpha(x) \wedge \\ & \wedge(P^\alpha(z_0) \vee \neg P^\alpha(z_0)) \wedge \ldots \wedge (P^\alpha(z_{l-1}) \vee \neg P^\alpha(z_{l-1}))), \end{array}$$

в то время как эта формула эквивалентна дизъюнкции формул вида

$$(9)\qquad \begin{array}{ll}\exists x & (\bigwedge\limits_{i<l} x \neq z_i \wedge \sigma_\Delta \wedge \\ & \wedge P^\alpha(x) \wedge \pm P^\alpha(z_0) \wedge \pm P^\alpha(z_1) \wedge \ldots \wedge \pm P^\alpha(z_{l-1})).\end{array}$$

Пусть $\Delta = \{\delta_0, \ldots, \delta_{s-1}\}$, и $u_i$ — представитель класса $\delta_i$, т.е. $u_i \in \delta_i$, $i = 0, 1, \ldots, s-1$. Тогда (9) эквивалентна формуле вида

$$(10)\qquad \begin{array}{ll}\exists x & (\bigwedge\limits_{i<s} x \neq u_i \wedge \bigwedge_{i<j<s} u_i \neq u_j \wedge \\ & \wedge P^\alpha(x) \wedge \pm P^\alpha(u_0) \wedge \pm P^\alpha(u_1) \wedge \ldots \wedge \pm P^\alpha(u_{s-1})) \wedge \psi,\end{array}$$

где $\psi$ является конъюнкцией формул вида $z_i = z_j$, $z_i \neq z_j$. Значит, формула $\psi$ не содержит кванторов. Наконец, для первого члена конъюнкции (10) нетрудно проверить, эквивалентен ли он формуле вида

$$\exists_{r+1} x P^\alpha(x) \wedge \bigwedge_{i<j<s} u_i \neq u_j \wedge \pm P^\alpha(u_0) \wedge \ldots \wedge \pm P^\alpha(u_{s-1}),$$

где $r$ представляет число позитивных появлений предикатов $P^\alpha$ в (10). Имея ввиду вышеизложенное, получим, что каждое предложение монадического исчисления эквивалентно булевской комбинации формул вида

$$\exists_r^\flat x P^\alpha(x), \quad \tau_r, \quad r \in N,$$

где

$$\tau_r = \exists x_0 \ldots x_{r-1} (\bigwedge_{i<j<r} x_i \neq x_j \wedge \forall y \bigvee_{i<r} y = x_i).$$

Заметим, что предложение $\tau_r$ описывает свойство модели, согласно которому она содержит точно $r$ элементов.

Из последнего утверждения следует процедура разрешимости для монадического исчисления:

Пусть $\varphi$ – произвольное предложение монадического исчисления.

**Шаг 1.** Согласно описанному алгоритму определить формулу высказываний $\psi(p_1, \ldots, p_m)$ и базовые формулы $\exists_r^\flat x P^\alpha(x)$, $\tau_r$, так что

$$\varphi \Leftrightarrow \psi(\exists_r^\flat x P^\alpha(x), \exists_s^\flat x P^\beta(x), \ldots, \exists_t^\flat x P^\gamma(x), \tau_k, \ldots, \tau_l)$$

есть теорема монадического исчисления.

**Шаг 2.** Если $\theta$ – правая часть этой эквивалентности, получаем, что $\mathbf{M} \vdash \theta$, тогда и только тогда, когда $\theta$ имеет место на всех *конечных* монадических моделях, область интерпретации которых имеет не более $n+1$ элементов, где $n$ – максимум из чисел $r, s, \ldots, t, k, \ldots, l$. Учитывая, что $|P^\alpha|$ принимает любое значение независимо от $|P^\beta|$, не нужно проверять истинность формулы $\theta$ на этих моделях. Действительно, пусть аргументы формулы $\theta$ распределены в следующем порядке:

$$\begin{aligned}\theta = \quad & \theta(\exists^\flat_{r_1} x P^\alpha(x), \exists^\flat_{r_2} x P^\alpha(x), \ldots, \exists^\flat_{r_a} x P^\alpha(x); \\ & \exists^\flat_{s_1} x P^\beta(x), \ldots, \exists^\flat_{s_b} x P^\beta(x); \ldots; \sigma_{k_1}, \ldots, \sigma_{k_c}).\end{aligned}$$

Если $\tilde{\theta} = \theta(X; Y; \ldots; Z)$, где

$$X = (x_1, \ldots, x_a), \quad Y = (y_1, \ldots, y_b), \quad Z = (z_1, \ldots, z_c)$$

есть последовательности различных букв высказываний, то очевидно, что $\mathbf{M} \vdash \theta$ , тогда и только тогда, когда $\tilde{\theta}$ истинно на векторах вида:

$$X = (0, 0, \ldots, 0), \text{ и } X \in \{(0, 0, \ldots, 0, 1), (0, 0, \ldots, 1, 0), \ldots, (1, 0, \ldots, 0, 0)\}$$

и аналогично для $Y, \ldots, Z$.

**Пример 2.2.1.** *Если*

$$\begin{aligned}\theta = \quad & \theta(\exists^\flat_2 x P^\alpha(x), \exists^\flat_3 x P^\alpha(x); \\ & \exists^\flat_2 x P^\beta(x), \exists^\flat_4 x P^\beta(x), \exists^\flat_7 x P^\beta(x); \sigma_2, \sigma_5, \sigma_6); \\ \tilde{\theta} = \quad & \theta(x_1, x_2; y_1, y_2, y_3; z_1, z_2, z_3),\end{aligned}$$

*то $\tilde{\theta}$ необходимо проверить в общей сложности для* $3 \cdot 4 \cdot 4 = 48$ *значений.*

Ясно, что описанную процедуру можно осуществить на вычислительной машине. Заметим и следующее. Доказательство того, что монадическое исчисление допускает элиминацию кванторов, можно получить и методом теории моделей, но при таком подходе мы не получили бы алгоритм, с помощью которого кванторы элиминируются из монадических предложений.

Как уже было отмечено, метод элиминации кванторов действительно является общим, учитывая также и то, что для большинства известных разрешимых теорий разрешимость доказывается именно таким методом. Все эти доказательства следуют в большей или меньшей мере

общему направлению рассуждений, которое здесь показано на примере монадического исчисления. Для некоторых особых, но, однако, достаточно интересных формул монадического исчисления процедуру разрешимости невозможно упростить. Но это уже тема следующего раздела.

## 2.3. Метод интерпретации

В этой части мы рассмотрим на примере монадического исчисления в $\text{ИП}^1$ без равенства и одного варианта модального исчисления метод интерпретации в анализе разрешимости теорий. Прежде всего объясним, что подразумевается под понятием интерпретации. В данном случае мы не будем приводить ни общее определение, ни разные формы этого понятия, ни детали самого определения, поскольку это потребовало бы введения формальных понятий из теории доказательств. Тем не менее, определение, которое мы приведем, достаточно для иллюстрации упомянутых примеров. Напомним, что метод уже давно введен в логику, и читатель может найти его основные применения в логике, арифметике и алгебре, например в [16]. А. Тарский доказал с помощью метода интерпретации, что элементарная геометрия разрешима, сводя вопрос о ее разрешимости к разрешимости элементарной теории поля действительных чисел (теории реально-закрытых полей, см. [8, глава 4]).

Обозначим через $\text{Sent}(T)$ множество предложений теории $T$. Теория $S$ *интерпретируется* в теории $T$ тогда и только тогда, когда существует эффективное (вычислимое) отображение

$$\sigma : \text{Sent}(S) \longrightarrow \text{Sent}(T),$$

так что для всех $\varphi \in \text{Sent}(S)$

$$S \vdash \varphi \text{ тогда и только тогда, когда } T \vdash \sigma(\varphi).$$

Отметим сразу следующий факт:

*Если $T$ – разрешимая теория, тогда и $S$ – тоже разрешимая теория.*

Действительно, предположим, что $\mathcal{A}$ — алгоритм, на основе которого $T$ есть разрешимая теория, и пусть $\mathcal{B}$ есть алгоритм, с помощью которого вычисляются значения отображения $\sigma$. Тогда композиция $\mathcal{C} = \mathcal{A}\mathcal{B}$ этих двух алгоритмов (например, в смысле композиции

машин Тьюринга) есть алгоритм разрешимости теории $S$. А именно, для $\varphi \in \mathrm{Sent}(S)$ с помощью $\mathcal{C}$ можно вычислить $\sigma(\varphi)$ и проверить, какая из альтернатив $T \vdash \sigma(\varphi)$ или *не* $T \vdash \sigma(\varphi)$, имеет место. Если $T \vdash \sigma(\varphi)$, тогда и $S \vdash \varphi$, а если *не* $T \vdash \sigma(\varphi)$, то $\varphi$ не является теоремой теории $S$. Если $T$ – непротиворечивая теория, что и является интересным случаем, тогда эти альтернативы исключают друг друга.

В интерпретации монадического исчисления будем пользоваться так называемым модальным S5 исчислением. В свое время Приор предсказал, что кванторы *всеобщности* и *существования* могут при определенных условиях интерпретироваться соответственно как модальные операторы *необходимо* и *возможно*. Именно этот случай мы имеем в монадическом исчислении и S5 исчислении.

Исчисление S5 есть исчисление высказываний, в котором кроме классических логических операций появляются и одноместные операции $\mathbf{L}$ и $\mathbf{M}$, которые интерпретируются следующим способом:

$$\begin{aligned} \mathbf{L}p &= \textit{необходимо, что } p, \\ \mathbf{M}p &= \textit{возможно, что } p, \end{aligned}$$

Например, формулу

$$\mathbf{M}p \wedge \mathbf{L}(p \Rightarrow q) \Rightarrow \mathbf{M}q \tag{11}$$

читаем так:

*Если $p$ возможно и $p$ необходимо влечет за собой $q$, тогда и $q$ возможно.*

Это предложение в естественном порядке воспринимается, конечно, как истинное. Оказывается, что истинно и предложение (11) в исчислении S5.

Аксиомы S5 исчисления следующие:

- Аксиомы исчисления высказываний
- $\mathbf{L}p \Rightarrow p$ – аксиома необходимости.
- $\mathbf{L}(p \Rightarrow q) \Rightarrow (\mathbf{L}p \Rightarrow \mathbf{L}q)$
- $\mathbf{M}p \Rightarrow \mathbf{LM}p$

Правила вывода исчисления S5 есть практически правила вывода обыкновенного исчисления высказываний (Модус Поненс и правило однородного замещения) и это, так называемое *правило необходимости*:

Если $\varphi$ – теорема, тогда и $\mathbf{L}\varphi$ – теорема.

Интерпретация монадического исчисления в исчислении S5 основывается на следующих фактах:

**Лемма 2.3.1.** *Каждая формула $\varphi$ монадического исчисления предикатов $P_1, P_2, \ldots, P_k$ эквивалентна булевской комбинации вида $\psi = \beta(\theta_1, \theta_2, \ldots, \theta_k)$, где $\beta(p_1, p_2, \ldots, p_k)$ является формулой высказываний, а формула $\theta_i$ есть какой-либо из предикатов $P_i$, либо имеет вид*

$$\exists x(\pm Q_1 \wedge \ldots \wedge \pm Q_k(x)), \tag{12}$$

*где $Q_i$ – некоторые из предикатов $P_i$. В особом случае, если $\varphi$ – предложение, т.е. не имеет свободных переменных, тогда $\varphi$ есть булевская комбинация формул вида (12).*

Формулы $\theta_i$ из последней леммы будем называть элементарными, а $\psi$ будем называть *редуцированным видом* формулы $\varphi$.

**Пример 2.3.1. А.** $\varphi = \exists x P_1(x) \wedge \forall x(P_1(x) \wedge P_2(x)) \Rightarrow \exists x P_2(x)$

*Эта формула уже имеет редуцированный вид.*

**Б.** $\psi = \forall x \exists y(P_1(x) \wedge P_2(y)) \Rightarrow \exists x(\neg P_1(x) \wedge P_2(x))$

*Эта формула в нередуцированном виде. Ее редуцированный вид будет*

$$\forall x P_1(x) \wedge \exists y P_2(y) \Rightarrow \exists x(\neg P_1(x) \wedge P_2(x)).$$

Доказательство последней леммы простое и основывается на уже упомянутых теоремах (общезначимых формулах) исчисления предикатов. Пусть $\mu$ — отображение, которое каждому предикату $P_i$ ставит в соответствие букву высказывания $p_i$, $i = 1, 2, \ldots, n$. *Модальный трансформ* элементарного предложения $\theta = \exists x(\pm Q_1(x) \wedge \ldots \wedge \pm Q_n(x))$ есть $\mu\theta = \mathbf{M}(\pm q_1 \wedge \ldots \wedge \pm q_n)$, где $q_i = \mu Q_i$, $Q_i \in \{P_1, \ldots, P_n\}$.

**Лемма 2.3.2.** *Пусть $\psi(\theta_1, \ldots, \theta_n)$ — редуцированное предложение монадического исчисления и пусть $\mu\psi = \psi(\mu\theta_1, \ldots, \mu\theta_n)$ — перевод формулы $\psi$ в формулу логики* S5. *Тогда имеет место следующее утверждение:*

*$\psi(\theta_1, \ldots, \theta_n)$ является теоремой монадического исчисления тогда и только тогда, когда $\psi(\mu\theta_1, \ldots, \mu\theta_n)$ является теоремой исчисления* S5.

Не будем приводить здесь доказательство леммы, но напомним, что его можно получить с помощью метода семантических таблиц, например, используя так называемую теорему редукции для исчисления S5 (см. [6, стр. 51]. Наконец, приведем хорошо известный факт:

**Лемма 2.3.3.** *Модальное исчисление* S5 *разрешимо.*

Известно несколько доказательств, т.е. алгоритмов разрешимости исчисления S5, некоторые из которых читатели могут найти в [6]. Принимая во внимание последнюю лемму и уже рассмотренные особенности монадического исчисления, нетрудно сконструировать алгоритм для разрешимости монадического исчисления в ИП$^1$ без равенства:

Пусть $\varphi$ — предложение монадического исчисления, в котором нет равенства.

**Шаг 1.** Построить редуцированный вид $\theta$ формулы $\varphi$.

**Шаг 2.** Построить модальный трансформ $\psi = \mu\theta$ формулы $\theta$.

**Шаг 3.** Проверить, является ли $\psi$ теоремой исчисления S5;

если является теоремой, тогда $\varphi$ есть теорема монадического исчисления,

если нет, тогда $\varphi$ не является теоремой монадического исчисления.

Следовательно разрешимость монадического исчисления сводится к разрешимость исчисления S5.

**Пример 2.3.2.** **А.** $\varphi = \exists x P_1(x) \wedge \forall x(P_1(x) \wedge P_2(x)) \Rightarrow \exists x P_2(x)$

$\theta = \varphi, \ \psi = \mathbf{M}p_1 \wedge \mathbf{L}(p_1 \wedge p_2) \Rightarrow \mathbf{M}p_2.$

*Поскольку $\psi$ является теоремой исчисления* S5*, то и $\varphi$ является теоремой монадического исчисления.*

**Б.** $\varphi = \forall x \exists y(P_1(x) \wedge P_2(y)) \Rightarrow \exists x(\neg P_1(x) \wedge P_2(x))$

$$\theta = \forall x P_1(x) \wedge \exists y P_2(y) \Rightarrow \exists x(\neg P_1(x) \wedge P_2(x))$$

$$\psi = \mathbf{L}p_1 \wedge \mathbf{M}p_2 \Rightarrow \mathbf{M}(\neg p_1 \wedge p_2).$$

*Учитывая, что $\psi$ не является теоремой исчисления* S5*, то и $\varphi$ не является теоремой монадического исчисления.*

## 2.4. Заключительные замечания

В предыдущих параграфах мы рассмотрели некоторые аспекты разрешимости теорий первого порядка и проиллюстрировали некоторые из методов доказательства разрешимости на примере монадического исчисления. Уже этот пример показывает сложность этой области, как и то, что к анализу проблемы разрешимости некоторой теории можно приступать лишь тогда, когда подробно изучены ее свойства. С другой стороны, мы только упомянули остальные аспекты этой проблематики, самым интересным из которых, с точки зрения вычислительной техники и осуществимости алгоритмов в реальном времени, является вопрос об алгоритмической сложности процедур для разрешимости конкретных теорий. М. Рабин замечает [1], что для известных в настоящее время примеров разрешимых теорий эти алгоритмы имеют экспоненциальный характер, и возникает вопрос, существуют ли действительно теории, для которых проблема разрешимости *практически* решаема. Причина этого сомнения состоит в том, что алгоритмическая сложность этих проблем такая же, как сложность классического исчисления высказываний. С другой стороны, лучший известный алгоритм, с помощью которого проверяется тавтологичность формул высказываний, имеет экспоненциальную сложность по отношению к входным данным. Поэтому, современные исследования, а вероятно, и исследования будущего, направлены на анализ сложности и на возможное ускорение алгоритмов для отдельных классов этого типа проблем.

Упомянем и факты, касающиеся монадического исчисления и алгоритмов разрешимости этих теорий.

Если расширить язык монадического исчисления символами индивидуальных констант: $a_1, a_2, \ldots, a_n$, то получаем также разрешимую теорию, которую обозначим через $\mathbf{M}_a$. Этот факт можно доказать небольшой модификацией любого из доказательств, предложенных в этой

статье. Это имеет место и в случае любого конечно-аксиоматического расширения монадического исчисления или теории $\mathbf{M}_a$. Одно из интересных расширений этого типа получается добавлением аксиомы:

$$\forall x(\bigvee_{1\le i\le n} x = a_i),$$

с помощью которой ограничивается область до множества интерпретации символов $a_i$, $i = 1, 2, \ldots, n$. Эта версия монадического исчисления может представлять интерес для анализа, а также для программной реализации алгоритма для манипуляции с базами данных, где каждая область определения представлена одним предикатом. Приведем пример.

**Пример 2.4.1.** [13, проблема 8, стр. 11] *В международной конференции участвуют семнадцать ученых. На этом собрании используются три языка, и каждый из ученых говорит на одном из этих языков. Также известно, что каждые два из участников конференции могут разговаривать на одном из этих языков. Доказать, что среди участников конференции существуют три человека, которые говорят на одном и том же языке.*

В рамках монадического исчисления с тремя предикатами $P_1, P_2, P_3$ эту проблему можно описать следующим способом. Введем символы констант $a_1, a_2, \ldots, a_{17}$ и следующие предложения:

$$\begin{aligned}
\varphi_1 &= \forall x(\bigvee_{1\le i\le 17} x = a_i)\\
\varphi_2 &= \bigwedge_{1\le i<j\le 17} a_i \neq a_j\\
\varphi_3 &= \forall x(P_1(x) \vee P_2(x) \vee P_3(x))\\
\varphi_4 &= \forall x, y(x \neq y \Rightarrow \bigvee_{1\le i\le 3} (P_i(x) \wedge P_i(y)).\\
\varphi_5 &= \exists x, y, z(x \neq y \wedge x \neq z \wedge y \neq z \wedge \bigvee_{1\le i\le 3} (P_i(x) \wedge P_i(y) \wedge P_i(z)))r
\end{aligned}$$

Здесь $a_1, a_2, \ldots, a_{17}$ обозначают участников конференции, а свойство $P_i(x)$ интерпретируется как "$x$ говорит на языке $P_i$". Тогда, например, предложения $\varphi_1$ и $\varphi_2$ описывают условие, что на конференции находятся 17 ученых, а предложение $\varphi_3$ есть условие, что каждый из ученых

говорит на одном из трех языков $P_1, P_2, P_3$. Согласно этому, решение проблемы, т.е. доказательство приведенного свойства, можно вывести применением описанного алгоритма для разрешимости монадического исчисления к следующему предложению:

$$\varphi_1 \wedge \varphi_2 \wedge \varphi_3 \wedge \varphi_4 \Rightarrow \varphi_5.$$

В математической логике изучается и так называемое *монадическое исчисление второго порядка*. Речь идет о теории и об исчислении предикатов второго порядка ИП$^2$, в котором кроме применений кванторов к индивидуальным переменным допускается применение кванторов к переменным множественного и реляционного типа. Последний вид кванторов называется кванторами второго разряда. Если применение кванторов второго разряда ограничивается одноместными отношениями, получаем монадическое исчисление второго порядка. Т. Столем доказал, что эта теория также разрешима. Интересно, что существует элементарное по сути доказательство этого факта. Это доказательство основывается на так называемом *исчислении конституентов* (см. [7, стр. 27]). Не будем приводить здесь это доказательство, но дадим пример того, как одну проблему можно записать в монадическом исчислении второго порядка.

**Пример 2.4.2.** [13, проблема 8, стр. 11] *Среди студентов, поступивших на факультет, ровно 50 говорят по-английски, ровно 50 говорят по-французски и ровно 50 говорят по-немецки. Конечно, некоторые из этих студентов могут говорить на двух или трех языках, а общее число студентов не превышает 150-ти. Доказать, что всех студентов можно распределить в 5 групп, которые могут содержать различное число членов, так чтобы в каждой группе было точно 10 студентов, говорящих на английском, точно 10 студентов, говорящих на французском и точно 10 студентов, говорящих на немецком языке.*

Введем унарные предикаты $E, F, N$, где $E(x)$ имеет значение "$x$ говорит по-английски", и соответствующие значения имеют предикаты $F$ и $N$. Тогда проблему можно представить в монадическом исчислении второго порядка следующим образом:

$$(|E| = 50 \wedge |F| = 50 \wedge |N| = 50) \wedge \forall x(E(x) \vee F(x) \vee N(x)) \Rightarrow$$
$$\exists P_1, P_2, P_3, P_4, P_5 (\bigwedge_{1 \leq 5} |P_i \cap E| = 10 \wedge \bigwedge_{1 \leq 5} |P_i \cap F| = 10 \wedge \bigwedge_{1 \leq 5} |P_i \cap N| = 10).$$

Здесь для любого унарного предиката $S$, $|S| = n$ замещает $\exists_n^! x S(x)$.

# 3. Примеры теорий

Из большого числа теорий первого порядка, которые известны как разрешимые, выберем самые интересные и приведем их в качестве приложения. Большинство примеров сопровождается описанием модели теории, а также именем математика, который доказал ее разрешимость. Для полноты, приведем также список некоторых неразрешимых теорий.

## 3.1. Список некоторых разрешимых теорий

1) Чистое исчисление высказываний с равенством (Л. Левенгейм, 1915).

2) Теория одноместных отношений, $(X, S_1, \ldots, S_n)$ (Л. Левенгейм, 1915).

3) Теория эквивалентности, $(X, \sim)$ (А. Яничак, 1953).

4) Теория одноместной операции, $(X, f)$ (А. Эренфойхт, 1959).

5) Теория линейной упорядоченности, $(X, \leq)$ (А. Эренфойхт, 1959).

6) Теория плотно упорядоченных множеств, $\mathrm{Th}(Q, \leq)$ (Р. Воот, 1954).

7) Теория вполне упорядоченных множеств (А. Тарский, А. Мостовский, 1949).

8) Теория дискретной упорядоченности, $\mathrm{Th}(N, \leq)$ (Е. Закон, А Робинсон, 1960).

9) Теория булевых алгебр, $(B, +, \cdot, ', 0, 1)$ (А. Тарский, 1949).

10) Теория свободных группоидов (А. И. Мальцев, 1961).

11) $\mathrm{Th}(N, +)$, арифметика Пресбургера — теория суммирования натуральных чисел, (М. Пресбургер, 1929).

12) $\mathrm{Th}(N, \cdot)$, теория умножения натуральных чисел, (А. И. Мальцев).

13) $\mathrm{Th}(\mathrm{ORD}, +)$, теория суммирования ординальных чисел, (А. Эренфойхт, 1957).

14) $\mathrm{Th}(\mathrm{CARD}, +)$, теория суммирования кардинальных чисел множеств, (А. Тарский, 1956).

15) $\mathrm{Th}(P(X), \cup, \cap, \subseteq, \emptyset, X)$, булева алгебра подмножеств, (Т. Сколем, 1917).

16) Теория свободных коммутативных полугрупп (А. Мостовский, 1949).

17) Теория групп Абеля (В. Шмелев, 1949).

18) Теория упорядоченных групп Абеля (И. Гуревич, 1964)

19) Теория циклических групп (Ю. Ершов, 1963).

20) Теория $p$-групп (Ю. Ершов, 1963).

21) Теория алгебраических закрытых полей (А. Тарский, 1949); а) конечной характеристики, б) $\mathrm{Th}(C, +, \cdot, 0, 1)$ – элементарная теория полей комплексных чисел.

22) Теория реально закрытых полей, $\mathrm{Th}(R, +, \cdot, 0, 1)$ – элементарная теория полей действительных чисел (А. Тарский, 1949).

23) Теория $p$-адических полей (Дж. Аш, С. Коэн 1965).

24) Теория закрытых дифференциальных полей (Г. Сакс).

25) Элементарная евклидова геометрия (А. Тарский, 1949).

26) Элементарная гиперболическая геометрия (В. Швабхаусер, 1959).

27) Теория классов конечных полей (Дж. Аш, 1968).

28) $\mathrm{Th}_2(N, ')$ – теория второго порядка функции следования (Дж. Бучи, 1962).

29) $\mathrm{Th}_2(T, r_0, r_1)$ – теория второго порядка двух функций следования на бесконечном дереве (М. Рабин, 1969).

30) Теория второго порядка линейно упорядоченных множеств со счетными областями (М. Рабин, 1969).

### 3.2. Список некоторых неразрешимых теорий

1) Арифметика Пеано (существуют, также, конечные неразрешимые фрагменты этой теории).

2) ZF – теория множеств Цермело-Френекеля.

3) Теория целых чисел; Теория рациональных чисел.

4) Теория групп; Теория простых групп.

5) Теория колец; Теория коммутативных колец.

6) Теория полей; Теория упорядоченных полей.

7) Теория модулярных сетей; Теория дистрибутивных сетей.

8) Теория коммутативных полугрупп.

9) Теория частичной упорядоченности; Теория двух линейных упорядоченностей.

10) Теория симметричного отношения; Теория двух эквивалентностей.

11) Проективная геометрия.

## Список литературы

[1] J. Barwise, editor, *Handbook of mathematical logic*, Part C (Recursion theory), статьи: a) H. Enderton, *Elements of recursion theory,* b) M. Davis, *Unsolvable problems,* c) M. Rabin *Decidable theories.* North-Holland, Amsterdam, 1977.

[2] C. C. Chang, J. Keisler, *Model theory,* North-Holland, Amsterdam 1973.

[3] S.A. Cook, The complexity of theorem proving procedures, proc. Third Annual ACM Symposium on the Theory of Computing, ACM, New York, 1971, 151-158.

[4] M. Davis, E. Weyuker, *Computability, complexity, and languges* (fundamentals of theoretical computer science), Academic press 1983.

[5] Ю. Ершов, И. Лавров, А. Тайманов, М. Тайтслин, *Элементарные теории,* Успехи математических наук, т. XX, вып. 4(124), 1965, 37–108.

[6] G.E. Hughes, M. J. Cresswell, *An introduction to modal logic,* Methuen and Co ltd, London 1973

[7] G. Kreisel, J.L. Krivine, *Elements of mathematical logic,* North-Holland, Amsterdam, 1971.

[8] K. Kuratowski, A. Mostowski, *Set theory*, PWN, Warszawa, 1976.

[9] Ž. Mijajlović, Z. Marković, K. Doshen, *Hilbertovi problemi i logika,* (Matematička biblioteka 48) Zavod za udžbenike i nastavna sredstva, Beograd 1986.

[10] Ž. Mijajlović, *An introduction to model theory,* Univerzitet u Novom Sadu, Prirodnomatematički fakultet, Institut za matematiku, 1987.

[11] D. Monk, *Mathematical Logic,* Part III: Decidable and undecidable theories, Springer-Verlag, Berlin, 1976.

[12] S. Prešić, *Elementi matematičke logike,* (Matematička biblioteka 34), Zavod za izdavanje udžbenika Beograd 1967.

[13] G. Sacks, *Saturated model theory,* W.A. Benjamin, Inc, Reading, Massachusets, 1972.

[14] D. O. Shklyarsky, N.N. Chentov, I.M. Yaglom, *Selected problems and theorems in elementary mathematics,* Mir Publishers, Moscow, 1979.

[15] J. Siekmann, G. Wrightson, editors, *Automation of Reasonong. Classical papers in computational logic 1957–1970,* Springer-Verlag, Berlin, 1983.

[16] Ž. Sokolović, magistarski rad: *Odlučivost matematičkih teorija,* Prirodno matematički fakultet, Beograd, 1987.

[17] A. Tarski, *Undecidable theories,* North-Holland, Amsterdam,1971.

[18] A. Krapež M. Kapetanović, *O jednom algoritmu za dokazivanje valjanih formula*, Računarstvo **1**, 23-34, 1990.