Математическая Логика. Теория

Александр Сергеев

1 Введение

Силлогизмы
Modus Ponendo Ponens: Если A и $A \to B$, то B
Парадокс Рассела
$X = \{x : x \notin x\}$
$(X \in X)$?
Определение
Номинализм – учение о том, что существуют лишь единичные вещи, а общие понятия – лишь имена
Реализм – учение о том, что общие понятия объективно существуют
Номинализм в вопросе решения парадокса Рассела: надо придумать понятие множества
Реализм в вопросе решения парадокса Рассела: необходимо понять, что такое множество на самом деле, докопаться до сути
Программа Гильберта – мы должны формализовать математику и избавиться от произвола, который может вносить сторонний исследователь
Формализация должна быть проверена, и ее непротиворечивость должна быть доказана
Программмма Гильберта – реализм: мы верим, что мир устроен некоторым образом, а значит существует некоторая идеальная математика, удовлетворяющая этим свойствам. Нам нужно лишь прислушаться к миру и найти ее

2 Исчисление высказываний

Определение
Высказывание – строка, сформулированная по следующим правилам

Предметный язык – язык, который мы изучаем (язык математической логики)
Метаязык – соглачения о записи. Из метаязыка можно получить предметный язык некоторыми неформализованными действиями
$A, B, \ldots$ – Пропозиционная переменная
$\alpha, \beta, \ldots$ – метапеременные (высказывания)
$\alpha \wedge \beta$ – Конъюнкция
$\alpha \vee \beta$ – Дизъюнкция
$\neg\alpha$ – Отрицание
$\alpha \rightarrow \beta$ – Импликация
X, Y, Z – метапеременные для пропозиционных переменных
Приоритет: отрицание, конъюнкция, дизъюнкция, импликация
Дизъюнкция и конъюнкция – левоассоциативные,импликация – правоассоциативная
Выражение на предметном языке – пропозиционные переменные, 4 вида *связкок* и полностью расставленные скобки. Все остальные формы записи – метаязык
Схема – строка, строящаяся по правилам предметного языка, где вместо пропозиционных переменных могут стоять маленькие греческие буквы(метапеременные)
Определение
Оценка высказывания $f : P \rightarrow V$, где $V = \{T, F\}$, P – множество пропозиционных переменных
$[[\alpha]] = T$ – оценка высказывания (значение α – истина)
$[[\alpha]]^{X_1:=v_1,\ldots,X_n:=v_n}$ – оценка высказывания
Определение
Если $[[\alpha]] = T$ при любой оценке переменных, то она *общезначима (тавтология)*: $\models \alpha$
Иначе *опровержима*
Если $[[\alpha]] = T$ при любой оценке переменных, при которой $[[\gamma_1]] = \ldots = [[\gamma_n]] = T$, то α – следствие этих высказываний: $\gamma_1, \ldots, \gamma_n \models \alpha$
Если $[[\alpha]] = T$ при некоторой оценке, то она *выполнима*, иначе *невыполнима*
Аксиомы исчисления высказываний

1. $\alpha \rightarrow \beta \rightarrow \alpha$
2. $(\alpha \rightarrow \beta) \rightarrow (\alpha \rightarrow \beta \rightarrow \gamma) \rightarrow (\alpha \rightarrow \gamma)$

3. $\alpha \to \beta \to \alpha \wedge \beta$

4. $\alpha \wedge \beta \to \alpha$

5. $\alpha \wedge \beta \to \beta$

6. $\alpha \to \alpha \vee \beta$

7. $\beta \to \alpha \vee \beta$

8. $(\alpha \to \gamma) \to (\beta \to \gamma) \to (\alpha \vee \beta \to \gamma)$

9. $(\alpha \to \beta) \to (\alpha \to \neg\beta) \to \neg\alpha$

10. $\neg\neg\alpha \to \alpha$

Определение
Доказательством назовем последовательность высказываний $\delta_1, \ldots, \delta_n$, где каждое высказывание δ_i либо:

- является аксиомой (существует замена метапеременных для какой-либо схемы аксоим, позволяющая получить схему δ_i)

- получается из $\delta_1, \ldots, \delta_{i-1}$ по правилу Modus Ponens: существуют такие $j, k < i : \delta_k \equiv \delta_j \to \delta_i$

Формула *выводима/доказуема*, если существует ее доказательство
Пример
$A \to (A \to A)$
$(A \to (A \to A)) \to (A \to ((A \to A) \to A)) \to (A \to A)$
$(A \to ((A \to A) \to A)) \to (A \to A)$
$A \to ((A \to A) \to A)$
$A \to A$
Определение
Вывод формулы α из гипотез $\gamma_1, \ldots, \gamma_k$ – такая последовательность $\sigma_1, \ldots, \sigma_n$, что σ_i является (одним из следующих):

- аксиомой

- одной из гипотез γ_t

- получена по правилу Modus Ponens из предыдущих

Формула *выводима из гипотез*, если существует ее вывод
Обозначение: $\gamma_1, \dots, \gamma_k \vdash \alpha$
Определение (корректность теории)
Теория *корректна*, если любое доказуемое в ней утверждение общезначимо
То есть, $\vdash \alpha$ влечет $\models \alpha$
Определение (полнота теории)
Теория семантически полна, если любое общезначимое в ней утверждение доказуемо. То есть, $\models \alpha$ влечет $\vdash \alpha$

Теорема (корректность вычисления высказываний)
Доказательство
Докажем, что любая строка доказательства является общезначимой
Докажем индукцией по количеству строк
База: $n = 1$ – аксиома. В ней нет правила Modus Ponens. Она общезначима
Переход: Пусть для любого доказательства длины n формула δ_n общезначима. Рассмотрим δ_{n+1}

1. Аксиома. Убедимся, что аксиома общезначима

2. Modus Ponens j, k – убедимся, что если $\models \delta_j$ и $\models \delta_k, \delta_k = \delta_j \to \delta_{n+1}$, то $\models \delta_{n+1}$

Аксиому проверим через таблицу истинности
Докажем правило Modus Ponens
По индукционному предположению $\models \delta_j, \models \delta_k$
Зафиксируем произвольную оценку
Из общезначимости $[[\delta_j]] = T, [[\delta_k]] = T$
Тогда из таблицы истинности $[[\delta_j]] = [[\delta_k]] = T$ только при $[[\delta_{n+1}]] = T$
Отсюда $\models \delta_{n+1}$
Определение
Контекст – совокупность всех гипотез. Обозначается большой греческой буквой
Пример записи:
$\Gamma = \{\gamma_1, \dots, \gamma_n\}$
$\Delta = \{\delta_1, \dots, \delta_m\}$
$\Gamma, \Delta \vdash \alpha$
Теорема о дедукции

$\Gamma, \alpha \vdash \beta \Leftrightarrow \Gamma \vdash \alpha \to \beta$
Доказательство $\Leftarrow$
Пусть $\Gamma \vdash \alpha \to \beta$
Т.е. существует вывод $\delta_1, \ldots, \delta_{n-1}, \underbrace{\alpha \to \beta}_{\delta_n}$
Дополним вывод: добавим туда α
По правилу Modus Ponens добавим туда β
Отсюда $\Gamma, \alpha \vdash \beta$
Определение
Конечная последовательность – функция $\delta : \{1, \ldots, n\} \to \mathcal{F}$
Конечная последовательность, индексированная дробными числами – функция $\zeta : I \to \mathcal{F}, I \subseteq \mathbb{Q}^+, |I| \in \mathbb{N}$
Доказательство $\Rightarrow$
Пусть $\Gamma, \alpha \vdash \beta$
Пусть дан некоторый вывод: $\delta_1, \ldots, \delta_{n-1}, \underbrace{\beta}_{\delta_n}$
Тогда рассмотрим последовательность: $\alpha \to \delta_1, \ldots, \alpha \to \delta_{n-1}, \alpha \to \beta$
Заметим, что выводом эта формула не является, т.к. в ней нет аксиом
Докажем по индукции по длине вывода
Если $\delta_1, \ldots, \delta_n$ – вывод $\Gamma, \alpha \vdash \beta$, то найдется ζ_k для $\Gamma \vdash \alpha \to \beta$, причем $\zeta_1 = \alpha \to \delta_1, \ldots, \zeta_n = \alpha \to \delta_n$

1. $n = 1$ – ч.с. перехода без Modus Ponens

2. Пусть $\delta_1, \ldots \delta_{n+1}$ – исходный вывод
   По индукционному предположению по $\delta_1, \ldots, \delta_n$ построен вывод ζ_k утверждения $\Gamma \vdash \alpha \to \delta_n$
   Достроим его для δ_{n+1}

   - δ_{n+1} – аксиома или $\delta_{n+1} \in \Gamma$:
     $\zeta_{n+1/3} = \delta_{n+1} \to \alpha \to \delta_{n+1}$
     $\zeta_{n+2/3} = \delta_{n+1}$
     $\zeta_{n+1} = \alpha \to \delta_{n+1}$

   - $\delta_{n+1} = \alpha$:
     $\zeta_{n+1/5} = a \to a \to a$
     $\zeta_{n+2/5} = (a \to a \to a) \to (a \to (a \to a) \to a) \to (a \to a)$
     $\zeta_{n+3/5} = (a \to (a \to a) \to a) \to (a \to a)$

$\zeta_{n+4/5} = a \to (a \to a) \to a$
$\zeta_{n+1} = a \to a$

- δ_{n+1} – Modus Ponens из δ_j и $\delta_k = \delta_j \to \delta_{n+1}$:
  $\zeta_{n+1/5} = \alpha \to \delta_j$
  $\zeta_{n+2/5} = \alpha \to \delta_j \to \delta_{n+1}$
  $\zeta_{n+3/5} = (\alpha \to \delta_j) \to (\alpha \to \delta_j \to \delta_{n+1}) \to (\alpha \to \delta_{n+1})$
  $\zeta_{n+4/5} = (\alpha \to \delta_j \to \delta_{n+1}) \to (\alpha \to \delta_{n+1})$
  $\zeta_{n+1} = \alpha \to \delta_{n+1}$

Лемма (правило контрапозиции)
Каково бы ни были формулы α, β, справедливо, что $\vdash (\alpha \to \beta) \to (\neg\beta \to \neg\alpha)$
Лемма (правило исключенного третьего)
Какова бы ни была формула α, справедливо, что $\vdash \alpha \vee \neg\alpha$
Лемма (правило исключенного допущения)
Пусть справедливо $\Gamma, \rho \vdash \alpha$ и $\Gamma, \neg\rho \vdash \alpha$
Тогда $\Gamma \vdash \alpha$
Теорема
Если $\models \alpha$, то $\vdash \alpha$
Определение
Зададим некоторую оценку, что $[[\alpha]] = x$
Тогда *условным отрицанием* формулы α называется формула $(|\alpha|) = \begin{cases} \alpha, & x = T \\ \neg\alpha, & x = F \end{cases}$
Если $\Gamma = \gamma_1, \ldots, \gamma_n$, то $(|\Gamma|) = (|\gamma_1|), \ldots, (|\gamma_n|)$
Пример: $(|A|), (|B|) \vdash (|A \to B|)$ позволяет записать таблицу истинности в одну строку, перебрав ее для всех оценок
Доказательство теоремы
Для каждой возможной связки $\star$ докажем формулы $(|\phi|), (|\psi|) \vdash (|\phi \star \psi)$
Теперь построим таблицу истинности для α и докажем в ней каждую строку:
$(|\Xi|) \vdash (|\alpha|), \Xi$ – контекст(все переменные в таблице)
Если формула общезначима, то в ней все строки будут иметь вид $(|\Xi|) \vdash \alpha$. От гипотез можно избавиться индукционно по теореме об исплючении допущения и получить требуемое $\vdash \alpha$
Лемма (Условное отрицание формул)
Пусть пропозиционные переменные $\Xi = X_1, \ldots, X_n$ – все переменные, которые используются в α

Пусть задана некоторая оценка переменных
Тогда $(|\Xi|) \vdash (|\alpha|)$
Доказательство
Докажем по индукции по длине формулы α

- База: формула атомарная, т.е. $\alpha = X_i$
  Тогда при любом Ξ выполнено $(|\Xi|)^{X_i=T} \vdash X_i$ и $(|\Xi|)^{X_i=F} \vdash \neg X_i$

- Переход:
  $\alpha = \phi \star \psi, (|\Xi|) \vdash (|\phi|)$ и $(|\Xi|) \vdash (|\psi|)$
  Тогда построим вывод
  Сначала запишем доказательство $(|\phi|)$
  Потом припишем доказательство $(|\psi|)$
  Потом припишем доказательство леммы о связках

3 Интуиционистская логика

Примеры:
Теорема Брауэра о неподвижной точке
Любое непрерывное отображение f шара $\mathbb{R}^n$ на себя имеет неподвижную точку
Замечание
Заметим, что теорема (и доказательство) не говорит ничего о том, как эту точку найти
Теорема
$\exists\, a, b$ – иррациональные : a^b – рациональное
Доказательство
Пусть $a = b = \sqrt{2}$

- $\sqrt{2}^{\sqrt{2}}$ – рациональное

- $\sqrt{2}^{\sqrt{2}}$ – иррациональное
  Тогда $(\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = \sqrt{2}^2 = 2$ – рациональное

Замечание
Т.о. мы доказали теорему, не предоставив пример. Наше знание о рациональных и иррациональных числах от этого не увеличилось
Определение

Доказательство чистого существования – доказательство существования объекта без приведения реального примера/рецепта создания этого объекта
(Неконструктивное доказательство существования объекта)
Замечание
Парадокс брадобрея – результат работы с чистым существованием. Мы предполагаем существование абстрактного объекта, не приводя рецепта для его создания

Может ли быть, что, работая с чистым существованием, мы сможем получить парадоксальные объекты и в других областях математики?
Давайте запретим доказательства чистого существования
Интуиционизм

- Математика не формальна
  (не надо ограничивать математику формальностями)
- Математика независима от окружающего мира
- Математика не зависит от логики – это логика зависит от математики
  (если мы сможем придумать более удобную логику для математики, мы можем ее использовать)

ВНК-интерпретация логических связок
(сокращение от: Брауэр, Гейтинг, Колмогоров)
Пусть α, β – некоторая конструкция (что угодно – физическая конструкция, логическое построение, программа, доказательство)

- $\alpha \& \beta$ построено, если построены α и β
- $\alpha \vee \beta$ построено, если построено α или β, <u>и мы знаем, что именно</u>
- $\alpha \rightarrow \beta$ построено, если есть способ перестроения α в β
- $\perp$ – конструкция, не имеющая построения
- $\neg\alpha$ – построено, если построено $\alpha \rightarrow\perp$

Дизъюнкция
$\alpha \vee \neg\alpha$ не может быть построено в общем виде, потому что мы не знаем, что именно было построено
Пример
Пусть α – это задача $P = NP$
Тогда $\alpha \vee \neg\alpha$ не может быть построено, т.к. мы не знаем, $P = NP$ или $P \neq NP$
Импликация
Пусть: A – сегодня в СПб идет дождь
B – сегодня в СПб светит солнце
C – сегодня я получил «отлично» по матлогу
Рассмотрим $(A \to B) \vee (B \to C) \vee (C \to A)$
Заметим это выражение не может быть построено, в отличие от классической логики
Отсюда: импликацию можно понимать как «формальную» и «материальную»
Формализация
Заметим, что формализация интуиционистской логики возможна, но интуитивное понимание – основное
Аксиоматика интуиционистского исчисления высказываний в гильбертовском стиле: аксиоматика КИВ, в которой 10 схема аксиом $\neg\neg\alpha \to \alpha$ заменена на $\alpha \to \neg\alpha \to \beta$

4 Топология

Обозначение
$\mathcal{P}(X)$ – множество всех подмножеств X
Определение
Топологическое пространство – упорядоченная пара $\langle X, \Omega \rangle$, X – множество (носитель), $\Omega \subseteq \mathcal{P}(X)$ – *топология*, причем

1. $\varnothing, X \in \Omega$
2. если $A_1, \dots, A_n \in \Omega$, то $A_1 \cap A_2 \cap \dots \cap A_n \in \Omega$ (конечное пересечение)
3. если $\{A_\alpha\}$ – семейство множеств из Ω, то $\bigcup\limits_\alpha A_\alpha \in \Omega$ (произвольное объединение)

Элементы Ω – *открытые множества*

Определение

$\mathcal{B}$ – *база* топологического пространства $\langle X, \Omega\rangle (\mathcal{B} \subseteq \Omega)$, если всевозможные объединения элементов (в т.ч. пустые) из $\mathcal{B}$ дают Ω

Определение

Дискретная топология – $\langle X, \mathcal{P}(X)\rangle$

Топология стрелки – $\langle \mathbb{R}, \{(x, +\infty) : x \in \mathbb{R}\} \cup \{\varnothing, \mathbb{R}\}\rangle$

Примеры

$\{(x, y) : x, y \in \mathbb{R}\}$ – база евклидовой топологии на $\mathbb{R}$

$\{\{x\} : x \in X\}$ – база дискретной топологии

Определение

Метрикой на X назовем множество, на котором определена функция расстрояния $d : X^2 \to \mathbb{R}^+$:

1. $d(x, y) = 0 \Leftrightarrow x = y$
2. $d(x, y) = d(y, x)$
3. $d(x, z) \leq d(x, y) + d(y, z)$

Определение

Открытым ε-шаром с центром в $x \in X$ назовем $\{t \in X : d(x, y) < \varepsilon\}$

Определение

Если X – некоторое множество и d – метрика на X, то будем говорить, что топологическое пространство, задаваемое базой $\mathcal{B} = \{O_\varepsilon(x) : \varepsilon \in \mathbb{R}^+, x \in X\}$ порождено метрикой d

Определение

Функция $f : X \to Y$ непрерывна, если прообраз любого открытого множества открыт

Определение

Будем говорить, что множество компактно, если из любого его открытого покрытия можно выбрать конечное подпокрытие

Определение

Пространство $\langle X_1, \Omega_1\rangle$ – подпространство пространства $\langle X, \Omega\rangle$, если $X_1 \subseteq X$ и $\Omega_1 = \{A \cap X_1, A \in \Omega\}$

Определение

Пространство $\langle X, \Omega\rangle$ связно, если нет $A, B \in \Omega$, что $A \cup B = X, A \cap B = \mathbb{0}$ и $A, B \neq \varnothing$

Определение (топология на деревьях)

Пусть некоторый лес задан конечным множеством вершин V и отношением $\prec$: $a \prec b \Leftrightarrow a$ – предок b

Тогда подмножество вершин $X \subseteq V$ назовем открытым, если из $a \in X, a \preceq b$ следует, что $b \in X$ (множество вершин и всех их потомков)

Теорема

Лес связен (как граф) тогда и только тогда, когда соответствующее ему топологическое пространство связно

Доказательство $\Rightarrow$

Пусть лес связен, но топологически не связен. Тогда найдутся непустые A, B, что $A \cup B = V, A \cap B = \varnothing$

Пусть $v \in V$ – корень дерева V и $v \in A$

Тогда $A = \{x : v \preceq x\} = V, B = \varnothing$

Доказательство $\Leftarrow$

Пусть лес топологически связен, но есть несколько корней $v_1, \dots, v_k$

Возьмем $A_i = \{x : v_i \preceq x\}$. Тогда все A_i открыты, непусты и дизъюнктны

$V = \bigcup\limits_i A_i$

Определение

Линейная связность – любые точки соединены путем

Определение

Множество нижних границ (lwb_Ω) – ...

Множество верхних границ (uwb_Ω) – ...

Минимальный элемент ($m \in X$) – Нет элементов, что $x \prec m$

Максимальный элемент ($m \in X$) – ...

Наименьший элемент ($m \in X$) – При всех $y \in X$ выполнено $m \preceq y$

Наибольший элемент ($m \in X$) – ...

Инфинут – наибольшая нижняя граница

Супремум – наименьшая верхняя граница

Определение

Рассмотрим $\langle X, \Omega \rangle$ и возьмем $\subseteq$ как отношение частичного порядка на $\mathcal{P}(X)$

Тогда $A^\circ := \inf\limits_\Omega(\{A\})$ – внутренность множества

Теорема

A° определена для любого A

Доказательство

Пусть $V = \mathrm{lwb}_\Omega\{A\} = \{Q \in \Omega : Q \subseteq A\}$

Тогда $\inf\limits_\Omega\{A\} = \bigcup\limits_{v \in V} v$

Напомним, что $\inf\limits_{\mathcal{U}} T = \text{наиб}(\text{lwb}_{\mathcal{U}}\, T)$

1. Покажем принадлежность: $\bigcup\limits_{v \in V} v \subseteq A, \in \Omega$
2. Покажем, что все из V меньше или равны: пусть $X \in V$. Тогда $X \subseteq \bigcup\limits_{v \in V} v$

Определение
Решетной называется упорядоченная пара $\langle X, (\preceq)\rangle$, где X – некоторое множество, $(\preceq)$ – частичный порядок на X, такой, что для любых $a, b \in X$ определены $a + b = \sup\{a, b\}, a \cdot b = \inf\{a, b\}$
То есть $a + b$ – наименьший элемент c, что $a, b \preceq c$
Определение
Псевдодополнение $a \to b$ – наибольший из $\{x : a \cdot x \preceq b\}$
Определение
Дистрибутивной решеткой называется такая, что $\forall\, a, b, c\ \ a \cdot (b + c) = a \cdot b + a \cdot c$
Импликативная решетка – такая, что для любых элементов есть псевдодополнение
Лемма
Любая импликативная решетка – дистрибутивна
Определение
0 – наименьший элемент решетки, 1 – наибольший элемент решетки
Лемма
В любой импликативной решетке $\langle X, (\preceq)\rangle$ есть 1
Доказательство
Рассмотрим $a \to a$, тогда $a \to a = \text{наиб}\{c : ac \preceq a\} = \text{наиб}\ X = 1$
Определение
Импликативная решетка с 0 – псевдобулева алгебра (алгебра Гейтинга)
В такой решетке определено $\sim a := a \to 0$
Определение
Булева алгебра – псевдобулева алгебра, в которой $a + \sim a \equiv 1$
Замечание
Известная нам булева «алгебра» – булева алгебра
Лемма
$\langle \mathcal{P}(X), (\subseteq)\rangle$ – булева алгебра
Лемма

$\langle \Omega, (\subseteq) \rangle$ – псевдобулева алгебра

Определение

Пусть некоторое вычисление высказываний оценивается значениями из некоторой решетки

Назовем оценку согласованной с исчилсением, если

$[[\alpha \& \beta]] = [[\alpha]] \cdot [[\beta]]$

$[[\alpha \vee \beta]] = [[\alpha]] + [[\beta]]$

$[[\alpha \to \beta]] = [[\alpha]] \to [[\beta]]$

$[[\neg \alpha]] = \sim [[\alpha]]$

$[[A \& \neg A]] = 0$

$[[A \to A]] = 1$

Теорема

Любая псевдобулева алгебра, являющаяся согласованной оценкой интуиционистского исчисления высказываний, является его корректной моделью: если $\vdash \alpha$, то $[[\alpha]] = 1$

Теорема

Любая булева алгебра, являющаяся согласованной оценивается классического исчисления высказываний, является его корректной моделью: если $\vdash \alpha$, то $[[\alpha]] = 1$