1 Общие замечания

1.1 О тексте

Данный текст представляет из себя краткий конспект лекций по курсу «Математическая логика», рассказанных студентам ИТМО (группы M3234-M3239) в 2017-2018 учебном году.

1.2 Общие определения и обозначения

Прежде чем приступить к изложению содержательного материала, введём несколько базовых определений и обозначений, которые должны быть уже знакомы читателю.

1. *Множество всех подмножеств* обозначим как $\mathcal{P}$: $\mathcal{P}(X) = \{C \mid C \subseteq X\}$
2. *Упорядоченную пару* каких-либо значений a и b будем обозначать как $\langle a, b\rangle$
3. Пусть дано некоторое частично-упорядоченное отношением $\sqsubseteq$ множество S. *Наименьшим* (*наибольшим*) элементом множества назовём такой элемент $t \in S$, что для любого $s \in S$ выполнено $t \sqsubseteq s$ ($s \sqsubseteq t$).
4. Пусть дано некоторое частично-упорядоченное отношением $\sqsubseteq$ множество S. *Минимальным* (*максимальным*) элементом множества назовём такой элемент $t \in S$, что не существует большего (меньшего) $s \in S$. Иными словами, нет такого s, что $s \sqsubseteq t$ ($t \sqsubseteq s$) и $s \neq t$.

   Заметим, что наименьшее (наибольшее) значение всегда единственное, а минимальных (максимальных) значений может быть много.

2 Общая топология

Мы начинаем курс немного издалека: от некоторых базовых тем общей топологии. С одной стороны, эти знания пригодятся нам дальше в курсе, с другой — есть надежда, что они настроят слушателей курса на правильный лад.

Определение 2.1. *Топологическим пространством* мы назовём упорядоченную пару множеств $\langle X, \Omega\rangle$, где $\Omega \subseteq \mathcal{P}(X)$, отвечающую следующим трём свойствам:

1. Какое бы ни было семейство множеств $\{A_\alpha\}$, где $A_\alpha \in \Omega$, выполнено $\cup_\alpha\{A_\alpha\} \in \Omega$
2. Какое бы ни было конечное семейство множеств $\{A_1, \dots, A_n\}$, где $A_i \in \Omega$, выполнено $A_1 \cap A_2 \cap \dots \cap A_n \in \Omega$
3. $\varnothing \in \Omega$, $X \in \Omega$

Определение 2.2. Пусть дано топологическое пространство $\langle X, \Omega\rangle$. Тогда любое множество $A \in \Omega$ назовём *открытым*. Если же $X \setminus A \in \Omega$, то такое множество назовём *замкнутым*.

Теорема 2.1. Следующие объекты являются топологическими пространствами:

1. Топология стрелки: $\langle \mathbb{R}, \{(x, +\infty) | x \in \{-\infty\} \cup \mathbb{R} \cup \{+\infty\}\}\rangle$
2. Дискретная топология на множестве X: $\langle X, \mathcal{P}(X)\rangle$
3. Топология Зарисского на множестве X: $\langle X, \{A \in \mathcal{P}(X) | (X \setminus A) \text{ — конечно }\}\rangle$

Определение 2.3. *Внутренностью* множества X (обозначается как $\text{int}X$) мы назовём наибольшее по включению окрытое подмножество X. *Замыканием* множества X (обозначается как $\text{cl}X$) мы назовём наименьшее по включению замкнутое надмножество X.

Определение 2.4. *Базой* топологического пространства $\langle X, \Omega \rangle$ назовём любое такое семейство множеств $\mathcal{B}$, что каждое открытое множество представляется объединением некоторого подмножества $\mathcal{B}$. Или, в формальной записи, $\Omega = \{\cup S | S \subseteq B\}$. Также будем говорить, что данная база $\mathcal{B}$ *задаёт* топологическое пространство $\langle X, \Omega \rangle$.

Теорема 2.2. Классическая топология Евклидова пространства $\mathbb{R}$: Множество

$$\mathcal{B} = \{(a, b) | a, b \in \mathbb{R}\}$$

является базой Евклидова пространства.

Определение 2.5. Топологическое пространство $\langle X, \Omega \rangle$ назовём связным, если единственные одновременно открытые и замкнутые множества в нём — $\varnothing$ и X.

Теорема 2.3. Топологическое пространство $\langle X, \Omega \rangle$ связно тогда и только тогда, когда в нём нет двух непустых открытых множеств A и B, что $A \cup B = X$ и $A \cap B = \varnothing$.

Определение 2.6. Назовём частичным порядком ($\sqsubseteq$) на множестве X любое рефлексивное, транзитивное и антисимметричное отношение на нём.

Определение 2.7. Рассмотрим множество X с заданным на нём частичным порядком $\sqsubseteq$. Рассмотрим множество $\mathcal{B}_{\sqsubseteq} = \{\{t \in X | x \sqsubseteq t\} | x \in X\}$. Тогда топологическое пространство $X_{\sqsubseteq}$, задаваемое базой топологии $\mathcal{B}_{\sqsubseteq}$, мы назовём *топологией частичного порядка* ($\sqsubseteq$) на X.

Теорема 2.4. При любом выборе X и ($\sqsubseteq$) $X_{\sqsubseteq}$ является топологическим пространством.

Определение 2.8. Пусть задано топологическое пространство $\langle X, \Omega \rangle$, и пусть задано множество $A \subseteq X$. Тогда рассмотрим $\Omega_A = \{S \cap A | S \in \Omega\}$. Будем называть топологическое пространство $\langle A, \Omega_A \rangle$ пространством с топологией, индуцированной пространством $\langle X, \Omega \rangle$.

Теорема 2.5. При любом выборе топологического пространства $\langle X, \Omega \rangle$ и A (подмножества X) пространство с индуцированной топологией $\langle A, \Omega_A \rangle$ является топологическим пространством.

Определение 2.9. Пусть задано топологическое пространство $\langle X, \Omega \rangle$, и пусть $A \subseteq X$. Тогда множество A называется связным, если оно связно как пространство с индуцированной пространством $\langle X, \Omega \rangle$ топологией.

Теорема 2.6. Рассмотрим ациклический граф G с множеством вершин V. Построим по нему отношение: положим, что $x \sqsubseteq y$, если имеется путь из x в y (в частности, будем считать, что всегда есть путь из x в x). Тогда граф слабо связен тогда и только тогда, когда связно соответствующее топологическое пространство частичного порядка.

3 Исчисление высказываний

Матлогика — это наука о правильных математических рассуждениях, а поскольку рассуждения обычно ведутся на каком-то языке, то она неразрывна связана с идеей двух языков: *языка исследователя* (или иначе его называют *метаязыком*), и *предметного языка.* Как следует из названий, языком исследователя пользуемся мы, формулируя утверждения или доказывая теоремы о разных способах математических рассуждений, или просто их обсуждая. Сами же математические рассуждения, собственно и составляющие предмет исследования, формализованы в некотором предметном языке.

Мы начнём с очень простого предметного языка — языка исчисления высказываний. Элементами (строками) данного языка являются некоторые выражения (формулы), по структуре очень похожие на арифметические, которые называются *высказываниями.*

Каждое высказывание — это либо *пропозициональная переменная* — большая буква латинского алфавита, возможно, с цифровым индексом, либо оно составлено из одного или двух высказываний меньшего размера, соединённых логической связкой.

Связок в языке мы определим 4 (хотя при необходимости этот список может быть в любой момент изменен).

- отрицание: если α — высказывание, то $\neg\alpha$ — тоже высказывание.
- конъюнкция: если α и β — высказывания, то $\alpha \& \beta$ — тоже высказывание.
- дизъюнкция: если α и β — высказывания, то $\alpha \vee \beta$ — тоже высказывание.
- импликация: если α и β — высказывания, то $\alpha \to \beta$ — тоже высказывание.

Также в языке можно использовать скобки вокруг выражений: если α — высказывание, то (α) — тоже высказывание. Если из расстановки скобок не следует иное, мы будем учитывать приоритет связок (связки в перечислении выше указаны в порядке убывания приоритета). Также, конъюнкцию и дизъюнкцию мы будем считать левоассоциативной (скобки в цепочке одинаковых связок расставляются слева направо: $(A \vee B) \vee C$), а импликацию — правоассоциативной: $A \to (B \to C)$).

Высказывания, подробности которых нас не интересуют, мы будем обозначать начальными буквами греческого алфавита (α, β, γ и т.п.). Ещё мы будем называть такие высказывания *метапеременными.* Одинаковым буквам всегда соответствуют одинаковые высказывания, однако, разным буквам не обязаны соответствовать разные высказывания. При подстановке выражений вместо метапеременных мы всегда предполагаем, что эти выражения взяты в скобки.

Покажем эти правила на примере. Выражение

$$\alpha \to \neg\beta \& \gamma \vee \delta \vee \epsilon \to \zeta \vee \iota$$

нужно воспринимать так:

$$(\alpha) \to (((((\neg(\beta))\&(\gamma)) \vee (\delta)) \vee (\epsilon)) \to ((\zeta) \vee (\iota)))$$

3.1 Оценка высказываний

Процесс «вычисления» значения высказываний имеет совершенно естественное определение. Мы фиксируем некоторое множество *истинностных значений* V, для начала мы в качестве такого множества возьмем множество $\{\texttt{И}, \texttt{Л}\}$, здесь И означает истину, а Л — ложь. Всем пропозициональным переменным мы приписываем некоторое значение, а затем рекурсивно вычисляем значение выражения естественным для указанных связок образом.

Пусть P — множество пропозициональных переменных языка. Тогда функцию $M : P \to V$, приписывающую истинностное значение пропозициональным переменным, мы назовём *моделью* (иначе: *интерпретацией* или *оценкой* переменных).

Функцию, сопоставляющую высказыванию α и модели M истинностное значение, мы назовём *оценкой* высказывания и будем это записывать так: $[\![\alpha]\!]^M$. Обычно для указания модели M мы будем перечислять значения пропозициональных переменных, входящих в формулу: $[\![P \to Q]\!]^{P:=\text{Л},Q:=\text{И}} = \text{И}$. Если конкретная модель ясна из контекста или несущественна для изложения, мы можем указание на модель опустить: $[\![P \to P]\!] = \text{И}$

Если $[\![\alpha]\!]^M = \text{И}$, то мы будем говорить, что высказывание α истинно в модели M, или, иными словами, M — *модель высказывания* α.

Тавтологией или *общезначимым высказыванием* мы назовём высказывание, истинное в любой модели. На языке исследователя общезначимость высказывания α можно кратко записать как $\models \alpha$.

Указанный способ оценки высказываний мы будем называть классическим. В дальнейшем мы будем брать необычные множества истинностных значений и будем давать неожиданный смысл связкам, однако, классический способ будет всегда подразумеваться, если не указано иного. Если же мы захотим сделать на этом акцент, мы будем говорить о *классических моделях исчисления высказываний*, подразумевая, что если мы приписываем переменным классические значения истина и ложь, то и высказывание целиком мы оцениваем тоже по классическим правилам.

3.2 Доказательства

В любой теории есть некоторые утверждения (аксиомы), которые принимаются без доказательства. В исчислении высказываний мы должны явно определить список всех возможных аксиом. Например, мы можем взять утверждение $A \& B \to A$ в качестве аксиомы. Однако, есть множество аналогичных утверждений, например, $B \& A \to B$, которые не отличаясь по сути, отличаются по записи, и формально говоря, являются другими утверждениями.

Для решения вопроса мы введём понятие *схемы аксиом* — некоторого обобщённого шаблона, подставляя значения в который, мы получаем различные, но схожие аксиомы. Например, схема аксиом $\alpha \& \beta \to \alpha$ позволяет получить как аксиому $A \& B \to A$ (при подстановке $\alpha := A, \beta := B$), так и аксиому $B \& A \to B$.

Возьмем следующие схемы аксиом для исчисления высказываний.

(1) $\alpha \to \beta \to \alpha$
(2) $(\alpha \to \beta) \to (\alpha \to \beta \to \gamma) \to (\alpha \to \gamma)$
(3) $\alpha \to \beta \to \alpha \& \beta$
(4) $\alpha \& \beta \to \alpha$
(5) $\alpha \& \beta \to \beta$
(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) $\neg\neg\alpha \to \alpha$

Напомним, что импликация — правоассоциативная операция, поэтому скобки в схеме аксиом 1, например, расставляются так: $(\alpha) \to ((\beta) \to (\alpha))$

Помимо аксиом, нам требуется каким-то образом научиться преобразовывать одни верные утверждения в другие. Сделаем это с помощью правил вывода. У нас пока будет одно правило вывода — Modus Ponens. Это также схема, она позволяет при доказанности двух формул ψ и $\psi \to \phi$ считать доказанной формулу ϕ.

Определение 3.1. *Доказательство* в исчислении высказываний — это некоторая конечная последовательность выражений α_1, $\alpha_2 \dots \alpha_n$ из языка L, такая, что каждое из утверждений $\alpha_i (1 \le i \le n)$ либо является аксиомой, либо получается из других утверждений α_{P_1}, $\alpha_{P_2} \dots \alpha_{P_k}$ $(P_1 \dots P_k < i)$ по правилу вывода.

Определение 3.2. Высказывание α называется доказуемым, если существует доказательство α_1, $\alpha_2 \dots \alpha_k$, и в нем α_k совпадает с α.

Вообще, схемы аксиом и правила вывода существуют для удобства задания исчисления. В дальнейшем будет очень неудобно возиться с этими объектами. Поэтому мы считаем, что в исчислении имеется бесконечно много аксиом и правил вывода, которые порождаются подстановкой всех возможных формул вместо параметров в схемы.

В качестве сокращения записи в языке исследователя мы будем писать $\vdash \alpha$, чтобы сказать, что α доказуемо.

Традиционно правило вывода Modus Ponens записывают так:

$$\frac{\alpha \quad \alpha \to \beta}{\beta}$$

4 Теорема о дедукции

Соглашение об обозначениях. Будем обозначать буквами $\Gamma, \Delta, \Sigma, \Pi$ списки формул (возможно, пустые).

Определение 4.1. Вывод из допущений. Пусть Γ – некоторый список высказываний, а α — некоторое высказывание. Тогда мы будем говорить, что высказывание α *выводимо* из Γ (и записывать это как $\Gamma \vdash \alpha$), если существует такая последовательность высказываний $\alpha_1, \alpha_2, \dots \alpha_{n-1}, \alpha$ (называемая *выводом* α из Γ), что каждое из высказываний α_i — это

- либо аксиома,
- либо получается по правилу Modus Ponens из предыдущих высказываний,
- либо — высказывание из списка Γ.

Элементы Γ мы будем называть *допущениями*. Также эти элементы называют предположениями или гипотезами.

В свете данного определения можно заметить, что доказательство — это вывод из пустого списка допущений.

Теорема 4.1. Теорема о дедукции. Утверждение $\Gamma \vdash \alpha \to \beta$ справедливо тогда и только тогда, когда справедливо, что $\Gamma, \alpha \vdash \beta$.

Для доказательства рассмотрим следующую лемму:

Лемма 4.2. $\vdash \alpha \to \alpha$

Доказательство.

(1)	$\alpha \to (\alpha \to \alpha)$	Сх. акс. 1
(2)	$(\alpha \to (\alpha \to \alpha)) \to (\alpha \to ((\alpha \to \alpha) \to \alpha)) \to (\alpha \to \alpha)$	Сх. акс. 2
(3)	$(\alpha \to ((\alpha \to \alpha) \to \alpha)) \to (\alpha \to \alpha)$	M.P. 1,2
(4)	$(\alpha \to ((\alpha \to \alpha) \to \alpha))$	Сх. акс. 1
(5)	$\alpha \to \alpha$	M.P. 4,3

□

Доказательство теоремы 4.1. Сперва докажем прямое следствие. Для этого нам достаточно научиться по любому выводу $\alpha \to \beta$ из Γ строить вывод β из Γ, α. Возьмем вывод формулы $\alpha \to \beta$, то есть некоторую последовательность формул $\delta_1 \dots \delta_{m-1}; \alpha \to \beta$. Добавив к выводу 2 формулы, получаем требуемый вывод:

(1)	δ_1	
	$\dots$	
$(m-1)$	δ_{m-1}	
(m)	$\alpha \to \beta$	
$(m+1)$	α	«Свежедобавленная» аксиома
$(m+2)$	β	M.P. m, $m+1$

Теперь докажем обратное. Нам необходимо построить вывод утверждения $\Gamma \vdash \alpha \to \beta$ по имеющемуся выводу $\delta_1 \dots \delta_{m-1}, \beta$. Мы поступим так: сперва набросаем план вывода – разместим по тексту «ключевые» формулы, которые потом дополним до полноценного вывода промежуточными формулами.

План вывода будет такой:

(1)	$\Gamma \vdash \alpha \to \delta_1$
$\dots$	
$(m-1)$	$\Gamma \vdash \alpha \to \delta_{m-1}$
(m)	$\Gamma \vdash \alpha \to \beta$

Теперь надо дополнить его до полноценного вывода. Будем рассматривать формулы подряд и перед каждой формулой добавлять некоторое количество формул, обосновывающих соответствующий шаг доказательства. Рассмотрим формулу номер i. Возможны следующие варианты:

1. δ_i — это аксиома или предположение, входящее в Γ. Тогда перед этой формулой вставим формулы δ_i и $\delta_i \to (\alpha \to \delta_i)$, и окажется, что i-я формула выводится из предыдущих двух формул путем применения правила Modus Ponens.

2. δ_i совпадает с α. Тогда мы вставим перед ней 4 первые формулы из леммы, и $\delta_i \to \alpha$ будет получаться по правилу Modus Ponens.

3. δ_i выводится по правилу Modus Ponens из каких-то других утверждений δ_j и δ_k (при этом $\delta_k \equiv \delta_j \to \delta_i$), где $j < i$ и $k < i$. Покажем, что $\alpha \to \delta_i$ тоже может быть выведена из утверждений $\alpha \to \delta_j$ и $\alpha \to (\delta_j \to \delta_i)$.

   Для этого добавим два высказывания:

$(\alpha \to \delta_j) \to ((\alpha \to (\delta_j \to \delta_i)) \to (\alpha \to \delta_i))$	Сх. акс. 2
$((\alpha \to (\delta_j \to \delta_i)) \to (\alpha \to \delta_i))$	М.Р. из j и $i - 6$

□

По аналогии мы можем рассмотреть отношение *следования*. Будем говорить, что высказывание α следует из высказываний Γ, если при любой оценке пропозициональных переменных, входящих в высказывания Γ и α, на которых все высказывания из Γ истинны, α также истинно. Записывать, что α следует из Γ, будем так: $\Gamma \models \alpha$.

5 Теорема о полноте исчисления высказываний

Определение 5.1. Введем обозначение. Пусть α — это некоторое высказывание, а x — некоторое истинностное значение. Тогда обозначим за ${}_{[x]}\alpha$ высказывание α, если x — истина, и $\neg(\alpha)$, если x — ложь. Также, если формула α — это формула с n пропозициональными переменными $P_1 \dots P_n$, и $x_1 \dots x_n$ — некоторые истинностные значения, то за $[\![\alpha]\!]^{P_1:=x_1,\dots P_n:=x_n}$ обозначим значение формулы α при подстановке значений $x_1 \dots x_n$ вместо переменных $P_1 \dots P_n$.

Лемма 5.1. Если $\Gamma, \Sigma \vdash \alpha$, то $\Gamma, \Delta, \Sigma \vdash \alpha$. Если $\Gamma, \Delta, \Sigma, \Pi \vdash \alpha$, то $\Gamma, \Sigma, \Delta, \Pi \vdash \alpha$.

Доказательство. Упражнение □

Лемма 5.2. Если справедливы 3 утверждения: $\Gamma \vdash \gamma$, $\Delta \vdash \delta$ и $\gamma, \delta \vdash \alpha$, то справедливо и $\Gamma, \Delta \vdash \alpha$

Доказательство. Упражнение □

Возьмем некоторую связку исчисления высказываний, например конъюнкцию: $A\&B$. Построим для нее таблицу истинности. По каждой строчке построим утверждение, в котором отрицания появляются там, где в таблице истинности находится *Л*:

A	B	$A\&B$	утверждение
Л	Л	Л	$\neg A, \neg B \vdash \neg(A\&B)$
Л	И	Л	$\neg A, B \vdash \neg(A\&B)$
И	Л	Л	$A, \neg B \vdash \neg(A\&B)$
И	И	И	$A, B \vdash A\&B$

Лемма 5.3. Каждое из построенных по таблицам истинности утверждений доказуемо.

Доказательство. Упражнение. □

Лемма 5.4 (Правило контрапозиции)**.** Каковы бы ни были формулы α и β, справедливо, что $\vdash (\alpha \to \beta) \to (\neg\beta \to \neg\alpha)$

Доказательство. Сперва докажем, что $\alpha \to \beta, \neg\beta \vdash \neg\alpha$.

(1)	$(\alpha \to \beta) \to (\alpha \to \neg\beta) \to \neg\alpha$	Сх. акс. 9
(2)	$\alpha \to \beta$	Допущение
(3)	$(\alpha \to \neg\beta) \to \neg\alpha$	М.Р. 2,1
(4)	$\neg\beta \to (\alpha \to \neg\beta)$	Сх. акс. 1
(5)	$\neg\beta$	Допущение
(6)	$\alpha \to \neg\beta$	М.Р. 5,4
(7)	$\neg\alpha$	М.Р. 6,3

Тогда, применив 2 раза Теорему о дедукции, получим вывод требуемого утверждения. □

Лемма 5.5. Правило исключенного третьего. Какова бы ни была формула α, $\vdash \alpha \vee \neg\alpha$

Доказательство. Доказательство проведем в 3 этапа.

1. Для начала покажем $\vdash \neg(\alpha \vee \neg\alpha) \to \neg\alpha$:

(1)	$\alpha \to \alpha \vee \neg\alpha$	Сх. акс. 6
$(2)\ldots(n+1)$	$\gamma_1, \ldots \gamma_{n-1}, (\alpha \to \alpha \vee \neg\alpha) \to (\neg(\alpha \vee \neg\alpha) \to \neg\alpha)$	Д-во из леммы 5.4
$(n+2)$	$\neg(\alpha \vee \neg\alpha) \to \neg\alpha$	М.Р. 1,$n+1$

2. Затем докажем $\vdash \neg(\alpha \vee \neg\alpha) \to \neg\neg\alpha$:

(1)	$\neg\alpha \to \alpha \vee \neg\alpha$	Сх. акс. 7
$(2)\ldots(k+1)$	$\delta_1, \ldots \delta_{k-1}, (\neg\alpha \to \alpha \vee \neg\alpha) \to (\neg(\alpha \vee \neg\alpha) \to \neg\neg\alpha)$	Д-во из леммы 5.4
$(k+2)$	$\neg(\alpha \vee \neg\alpha) \to \neg\neg\alpha$	М.Р. 1,$k+1$

3. Теперь докажем все вместе:

(1)	$\neg(\alpha \vee \neg\alpha) \to \neg\alpha$	по пункту 1
(2)	$\neg(\alpha \vee \neg\alpha) \to \neg\neg\alpha$	по пункту 2
(3)	$(\neg(\alpha \vee \neg\alpha) \to \neg\alpha) \to (\neg(\alpha \vee \neg\alpha) \to \neg\neg\alpha) \to (\neg\neg(\alpha \vee \neg\alpha))$	Сх. акс. 9
(4)	$(\neg(\alpha \vee \neg\alpha) \to \neg\neg\alpha) \to \neg\neg(\alpha \vee \neg\alpha)$	М.Р. 1,3
(5)	$\neg\neg(\alpha \vee \neg\alpha)$	М.Р. 2,4
(6)	$\neg\neg(\alpha \vee \neg\alpha) \to (\alpha \vee \neg\alpha)$	Сх. акс. 10
(7)	$\alpha \vee \neg\alpha$	М.Р. 5,6

□

Лемма 5.6. Об исключении допущения. Пусть справедливо $\Gamma, \rho \vdash \alpha$ и $\Gamma, \neg\rho \vdash \alpha$. Тогда также справедливо $\Gamma \vdash \alpha$.

Доказательство. Упражнение □

Теорема 5.7. О полноте исчисления высказываний. Пусть справедливо $\models \alpha$. Тогда также справедливо, что $\vdash \alpha$.

Доказательство. Для доказательства теоремы мы докажем чуть более сильное утверждение — что для любого k от 0 до n и любой оценки переменных $x_1, \dots x_k$ справедливо ${}_{[x_1]}P_1, \dots {}_{[x_k]}P_k \vdash \alpha$. Нетрудно заметить, что утверждение теоремы непосредственно следует из данного утверждения для $k = 0$. Доказательство будет вестись индукцией по $n - k$.

База. Пусть $n - k = 0$, то есть $k = n$. $\models \alpha$ означает, что при любой оценке $x_1, \dots x_n$ пропозициональных переменных $P_1, \dots P_n$ справедливо $\alpha[P_1 := x_1, \dots P_n := x_n] = \texttt{И}$. Возьмем некоторую оценку переменных $x_1, \dots x_n$. Тогда, по лемме 5, ${}_{[x_1]}P_1, \dots {}_{[x_n]}P_n \vdash {}_{\alpha[P_1:=x_1,\dots P_n:=x_n]}\alpha$ то есть ${}_{[x_1]}P_1, \dots {}_{[x_n]}P_n \vdash \alpha$.

Переход. Пусть утверждение уже доказано для некоторого $n - k > 0$, покажем его для $n - k + 1$ (то есть доказано для $k < n$, покажем его для $k - 1$). Возьмем некоторую оценку переменных $x_1, \dots x_{k-1}$. По предположению, ${}_{[x_1]}P_1, \dots {}_{[x_k]}P_k \vdash \alpha$, то есть

$${}_{[x_1]}P_1, \dots {}_{[x_{k-1}]}P_{k-1}, \neg P_k \quad \vdash \alpha$$
$${}_{[x_1]}P_1, \dots {}_{[x_{k-1}]}P_{k-1}, P_k \quad \vdash \alpha$$

Тогда по лемме об исключении допущения, справедливо ${}_{[x_1]}P_1, \dots {}_{[x_{k-1}]}P_{k-1} \vdash \alpha$.

□

Теорема 5.8. О корректности исчисления высказываний. Пусть справедливо $\vdash \alpha$. Тогда также справедливо, что $\models \alpha$.

Доказательство. По условию теоремы, у нас есть доказательство высказывания α, то есть последовательность высказываний $\alpha_1, \dots \alpha_m$. Каждое высказывание — это либо аксиома, либо применение правила Modus Ponens. Докажем, что для каждого k все высказывания α_l при $l \le k$ — тавтологии. Доказательство будем вести индукцией по k.

База. Пусть $k = 0$, тогда нет ни одного высказывания, про которое нужно доказать, что оно — тавтология, то есть утверждение автоматически верно.

Переход. Пусть для некоторого k утверждение справедливо, докажем его для $k + 1$. Выберем некоторую оценку $x_1, \dots x_n$ пропозициональных переменных $P_1, \dots P_n$, использованных в высказываниях $\alpha_1 \dots \alpha_{k+1}$. Рассмотрим случаи.

Пусть α_{k+1} — аксиома. В данную аксиому входят одна, две или три формулы $\beta_1, \beta_2, \beta_3$. Подставив всех возможных истинностных значений вместо данных формул можно проверить, что все аксиомы являются тавтологиями, значит, они будут истинны и на тех конкретных значениях, которые примут данные формулы после подстановки значений $x_1, \dots x_n$.

Пусть α_{k+1} получается по правилу Modus Ponens из α_p и α_q, причем $\alpha_q \equiv \alpha_p \to \alpha_{k+1}$. Тогда $[\![\alpha_p]\!]^{P_1:=x_1,\dots P_n:=x_n} = \texttt{И}$ и $[\![\alpha_p \to \alpha_{k+1}]\!]^{P_1:=x_1,\dots P_n:=x_n} = \texttt{И}$. Из таблицы истинности импликации следует, что неизбежно $[\![\alpha_{k+1}]\!]^{P_1:=x_1,\dots P_n:=x_n} = \texttt{И}$.

□

Заметим, что вместе из этих двух теорем следует, что если неверно, что $\vdash \alpha$, то неизбежно найдется контрпример.

6 Интуиционистское исчисление высказываний

Одна из главных причин возникновения математической логики — кризис в математике начала XX века. Классический пример такого — парадокс Рассела, утверждающий, что понятие «множества всех не принадлежащих себе множеств» противоречиво. В самом деле, пусть $X = \{t \mid t \notin t\}$. Рассмотрим $X \in X$. Обе возможных альтернативы — $X \in X$ и $X \notin X$ — вступают в противоречие с определением множества X. Значит, мы можем сделать вывод, множества X не существует.

С одной стороны, в этом нет проблемы: мы не переживаем, если не найдём числа $t \in \mathbb{N}$, такого, что $t = t$ и $t \neq t$ одновременно. Но, с другой стороны, в формальном определении множества X на первый взгляд нет никаких проблем. Единственная, по-видимому, для современного читателя непривычная деталь в данном определении — множество, принадлежащее самому себе, но если вспомнить язык Java, то это возражение не должно вызывать никаких серьёзных сомнений. Просто рассмотрите следующее определение:

```
class IntList {
   IntList next;
   int value;
}
```

Парадокс Рассела был получен не сразу, а через несколько лет после появления теории множеств и построения значительного количества математических теорий на её основе. Из этого возникает сомнение, нет ли таких же противоречий и в определении, например, вещественных чисел, просто глубже скрытых. Вдруг через несколько лет какой-то математик найдёт противоречия в математическом анализе — и значительную часть теории придётся пересмотреть или вообще признать ошибочной.

Было предложено много подходов к решению этой проблемы. Современный (классический) подход состоит в том, чтобы так формализовать теорию множеств, чтобы в ней не возникало парадоксов. Была сформулирована программа, предполагавшая своей целью доказательство непротиворечивости такой формальной теории. Однако, в 30-е годы Куртом Гёделем было показано, что такое доказательство минимально удовлетворительной надёжности построить невозможно. Конечно, самая распространённая формализация теории множеств — аксиоматика Цермело-Френкеля — оформилась в современном виде в 1925 году, почти 100 лет назад, и пока никаких противоречий в ней не было найдено. Но здесь всегда остаётся место для сомнений.

Поэтому интерес представляют альтернативные подходы к проблеме. Данный раздел посвящён интуиционистской логике. Математики, стоявшие у истоков данной логики, видели решение в том, чтобы исключить из рассмотрения «неконструктивные» объекты — объекты, метода построения которых не предложено. В частности, множество X из примера выше является примером неконструктивного объекта. Мы слишком легко приняли на веру возможность его существования и получили противоречие.

Столь резкие результаты получаются не всегда, но в целом в математике имеет место довольно много утверждений, пусть и не противоречивых, но выглядящих совершенно антиинтуитивно. Например, широко известна теорема Банаха-Тарского, утверждающая, что трёхмерный шар можно разрезать на конечное число попарно непересекающихся частей, из которых потом можно составить два шара того же размера.

BHK-интерпретация

BHK-интерпретация логики названа по именам математиков, её предложивших (Л. Брауэр, А. Гейтинг и А. Колмогоров). Они решили изменить сам подход к математическому рассуждению, предположив, что математик не думает в стиле классической логики, и что правильно, поэтому, попробовать формализовать «интуитивный» стиль.

Попробуем сформулировать эти соображения применительно к логическим связкам исчисления высказываний. Будем определять интерпретацию индуктивно. Пусть даны высказывания P и Q, тогда:

- мы считаем $P\&Q$ доказанным, если у нас есть доказательство высказывания P и доказательство высказывания Q;
- мы считаем $P \vee Q$ доказанным, если у нас есть доказательство P или есть доказательство Q (т.е. мы знаем, какая из двух альтернатив выполнена);
- мы считаем $P \to Q$ доказанным, если мы умеем перестраивать любое доказательство высказывания P в доказательство высказывания Q;
- мы считаем $\perp$ утверждением, не имеющим доказательства.
- $\neg P$ есть сокращение для $P \to \perp$. Иными словами, мы считаем $\neg P$ доказанным, если мы умеем из доказательства P получить противоречие.

Проиллюстрировать подход можно на примере следующей теоремы.

Теорема 6.1. Существуют два таких вещественных иррациональных числа p и q, что $p^q \in \mathbb{Q}$.

Доказательство. Рассмотрим два случая:

1. если $\sqrt{2}^{\sqrt{2}} \in \mathbb{Q}$, то мы нашли требуемые числа: $p = q = \sqrt{2}$;
2. если же $\sqrt{2}^{\sqrt{2}} \notin \mathbb{Q}$, то рассмотрим $p = \sqrt{2}^{\sqrt{2}}$ и $q = \sqrt{2}$, тогда $p^q = \sqrt{2}^{\sqrt{2}^{\sqrt{2}}} = 2 \in \mathbb{Q}$.

□

Данная теорема, хоть и доказывает факт существования таких чисел, ничего не говорит по поводу того, какой из двух случаев имеет место — то есть, она неконструктивна. В самом деле, обозначим факт того, что $\sqrt{2}^{\sqrt{2}} \in \mathbb{Q}$ за P, а итоговое утверждение теоремы — за S. Мы показываем, что $P \to S$, и что $\neg P \to S$. Однако, чтобы перейти к просто S, нам нужно показать $P \vee \neg P$. Несложно видеть, что в ВНК-интерпретации нет простого способа это сделать: чтобы считать дизъюнкцию доказанной, мы должны знать, какой из случаев имеет место. Поэтому, данное рассуждение не является доказательством в ВНК-интерпретации.

Для программистов же здесь важным является следующее соображение: эта теорема не позволяет написать программу, ищущую эти два числа. Скажем, теорема о дедукции не такова: её доказательство позволяет построить такую программу, предъявляющую объект, существование которого утверждает теорема.

Формализация интуиционистской логики

Исходный постулат интуиционистской логики состоит в том, что никакая формализация не является первичной. Мы выбираем те или иные правила только потому, что они соответствуют заявленным целям. Мы также вольны в любой момент правила поменять, если на то будут серьёзные основания.

У интуиционистской логики есть несколько формализаций, рассмотрим наиболее распространённую. Заменим аксиому устранения двойного отрицания (10-ю) на $\alpha \to \neg\alpha \to \beta$. Полученную систему назовём аксиоматикой интуиционистского исчисления высказываний.

В у данной аксиоматики есть интересные свойства, отсутствующие в классическом исчислении высказываний. Например, если $\vdash_{\text{и}} \alpha \vee \beta$, то $\vdash_{\text{и}} \alpha$, либо $\vdash_{\text{и}} \beta$ — сравните с ВНК-интерпретацией дизъюнкции. Данное следствие поясняет обоснованность замены аксиомы, в дальнейшем оно будет доказано формально.

6.1 Булева алгебра и Топологическая интерпретация интуиционистского исчисления высказываний

Мы построим две параллельные интерпретации для классической и интуиционистской логики.

Определение 6.1.

Пусть дано некоторое исчисление высказываний, для которого нам нужно построить модель — предложить способ оценки истинности выражений. Начинаем мы с множества истинностных значений. Возьмем в качестве этого множества все открытые множества некоторого заранее выбранного топологического пространства. Определим оценку для связок интуиционистского исчисления высказываний следующим образом:

$[\![A\&B]\!] = [\![A]\!] \cap [\![B]\!]$
$[\![A \vee B]\!] = [\![A]\!] \cup [\![B]\!]$
$[\![A \to B]\!] = (c[\![A]\!] \cup [\![B]\!])^\circ$
$[\![\neg A]\!] = (c[\![A]\!])^\circ$

Будем считать, что формула истинна в данной модели, если её значение оказалось равно всему пространству.

Например, возьмем в качестве пространства $\mathbb{R}$, и вычислим значение формулы $A \vee \neg A$ при A равном $(0,1)$: $[\![A \vee \neg A]\!] = (0,1) \cup [\![\neg A]\!] = (0,1) \cup (c(0,1))^\circ = (0,1) \cup ((-\infty,0) \cup (1,\infty)) = (-\infty,0) \cup (0,1) \cup (1,\infty)$. Нетрудно видеть, что данная формула оказалась не общезначимой в данной интерпретации.

7 Литература

Список литературы

[1] Виро О.Я., Иванов А.О., Нецветаев Н.Ю., Харламов В.М. Элементарная топология — М.: МЦНМО, 2012