МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ
УНИВЕРСИТЕТ
имени М. В. ЛОМОНОСОВА

Механико-математический факультет

В. Е. Плиско, В. Х. Хаханян

ИНТУИЦИОНИСТСКАЯ ЛОГИКА

Москва 2009

УДК 510.24

Интуиционистская логика / В. Е. Плиско, В. Х. Хаханян. — М.: Изд-во при мех.-мат. ф-те МГУ, 2009. — 159 с.

В книге систематически излагаются основные сведения, относящиеся к интуиционистской логике: мотивировка построения интуиционистской логики в виде исчисления Гейтинга, псевдобулевы алгебры и модели Крипке как аппарат исследования интуиционистских логических и логико-математических систем. Часть представленного в книге материала ранее излагалась только в журнальных статьях. Книга написана на основе специальных курсов, читавшихся авторами в течение ряда лет на механико-математическом и философском факультетах Московского Государственного Университета имени М. В. Ломоносова. Для чтения книги не требуется никаких предварительных знаний: все необходимые сведения из математической логики излагаются в книге. Книга может служить для первоначального ознакомления с вопросами оснований математики, а также классической и неклассической математической логикой. Книга предназначена для студентов и аспирантов, а также специалистов по математической логике, информатике и кибернетике.

Оглавление

Предисловие

«Обывательское» представление об интуиционизме, как правило, состоит в том, что интуиционисты — это такие странные люди, которые запрещают себе пользоваться в рассуждениях логическим законом исключенного третьего и критикуют других, когда те делают это. Однако близкое и детальное знакомство с интуиционизмом приводит к мысли, что интуиционистский взгляд на математику является более реалистичным по сравнению с традиционным, классическим.

Интуиционистское направление в математике начало складываться в начале XX века как результат предпринятой голландским математиком Л. Э. Я. Брауэром критики классической математики и логики в связи с обнаружением теоретико-множественных парадоксов. Философские и методологические предпосылки интиуиционизма изложены в книге А. Гейтинга [11], где, в частности, говорится:

«К интуиционистам мы относим тех математиков, которые принимают следуюшие два принципа:

1. Математика обладает не только чисто формальным, но и содержательным значением.

2. Математические предметы непосредственно постигаются мыслящим духом; следовательно, математическое познание не зависит от опыта».

Первый принцип противопоставляет интуиционизм *формализму* — другому направлению в основаниях математики, программа которого была выдвинута немецким математиком Д. Гильбертом. Целью этой программы было доказательство непротиворечивости математики точным математическим способом, для чего применялся метод формализации математических теорий, состоящий в том, что математические утверждения записываются на подходящем формальном языке и таким образом заменяются на последовательности символов, а математические рассуждения представляются как последовательности утверждений, построенные в соответствии с формальными логическими правилами. С формалистской точки зрения математика представляет собой совокупность предложений формализованного языка, выводимых из некоторой системы аксиом, причем выбор аксиом произволен и подчиняется лишь более или менее условным соображениям практического удобства, а также обязательному требованию непротиворечивости. При этом вопрос об истинности или ложности математических суждений не имеет смысла: можно говорить лишь об их доказуемости или опровержимости на основе аксиом.

Таким образом, первый из перечисленных принципов интуиционизма признает за математикой существование предмета исследования, однако второй принцип объявляет его исключительно продуктом мышления, отрицая какой бы то ни было объективный, независимый от мышления характер математических предметов.

Отвергая связь истинности математических суждений с опытом, в качестве единственного критерия истинности в математике Брауэр провозглашает интуицию. При этом, как указывает Гейтинг [11, с. 20], брауэровскую интуицию не следует понимать в каком-то «мистическом» смысле. Речь идет лишь о том, что согласно концепции Брауэра математические объекты рождены человеческой мыслью, и потому истинность суждений о них полностью определяется представлениями об этих объектах того математика, в сознании которого сложились эти объекты. Строго говоря, с точки зрения интуиционизма сколько математиков — столько и математик. Однако в силу каких-то общих свойств человеческого мышления возможно образование в сознании разных людей сходных математических понятий. К ним относится, например, понятие натурального числа. Отправляясь от этого понятия, на основе интуиционистских представлений может быть развита своеобразная математическая теория.

Объектами исследования в интуиционистской математике являются прежде всего конструктивные объекты (например, натуральные и рациональные числа) и заданные подходящим образом конечные совокупности конструктивных объектов. Своеобразным объектом исследования являются также так называемые свободно становящиеся (или бесконечно продолжающиеся) последовательности. Такую последовательность можно представлять себе как эффективно заданную функцию, определенную на натуральных числах и принимающую в качестве значений конструктивные объекты. При этом эффективность в интуиционизме никак не уточняется и может пониматься довольно широко. Так, свободно становящуюся последовательность можно задавать алгоритмом, а можно каждое последующее ее значение определять бросанием монеты. Однако в любом случае мы должны учитывать, что в каждый момент нам известен лишь конечный начальный отрезок последовательности, и в своих рассуждениях мы не имеем права считать, что нам дана вся последовательность в целом. В этом проявляется отказ от использования *абстракции актуальной бесконечности*, состоящей в отвлечении от принципиальной незавершаемости неограниченно продолжаемых процессов и рассмотрении воображаемых результатов этих процессов как актуальных, завершенных объектов. Эта абстракция лежит в основе теоретико-множественного построения математики. Вместо нее в интуиционистской математике используется более скромная *абстракция потенциальной осуществимости*, состоящая в идеализации, допускающей неограниченное продолжение процесса получения значений последовательности. Систематическое изложение идей интуиционизма и некоторых разделов интуиционистской математики содержится в книге Гейтинга [12].

Философские предпосылки интуиционизма оказались неприемлемыми для значительной части математиков и были подвергнуты обоснованной критике. Так, А. Н. Колмогоров в предисловии к книге [11] пишет: «Мы не можем согласиться, что математические объекты являются продуктом конструктивной деятельности духа. Для нас математические объекты являются абстракциями реально существующих форм независимой от нашего духа действительности.»

Все же интуиционистская критика оказалась весьма плодотворной для математики в целом, так как привлекла внимание к проблемам конструктивного образования абстрактных математических понятий и к вопросу о границах применимости классической логики. С точки зрения интуиционизма как конструирование математических объектов, так и рассуждения о них должны подчиняться критерию интуитивной ясности и убедительности. Касаясь отношений между математикой и логикой, Гейтинг [11, с. 22] указывает, что в интуиционистской математике умозаключения не производятся по заранее установленным правилам (как в формалистской концепции Гильберта), т. е. не фиксируется какая-либо априорная логическая система. Убедительность каждого логического шага должна проверяться непосредственно в соответствии с интуицией. Однако это не исключает существования общих правил, по которым из одних истинных математических предложений интуитивно ясным путем получаются другие истинные математические предложения. Таким образом, имеет смысл говорить об интуиционистской логике как о совокупности интуитивно примлемых способов математических умозаключений. Основоположник интуиционизма Брауэр предпринял анализ принципов аристотелевской логики и пришел к выводу, что применимость закона исключенного третьего не во всех случаях можно считать очевидной.

Начиная с работ советских математиков А. Н. Колмогорова и В. И. Гливенко и голландского математика А. Гейтинга, относящихся к концу 20-х – началу 30-х годов XX века, большое внимание уделяется построению и исследованию логических и логико-математических формальных систем, корректных с точки зрения интуиционизма. По мере развития математики и математической логики исследования по интуиционистской логике не только не теряли свою актуальность, но, напротив, наполнялись новым содержанием. Так, еще в 30-е годы XX века Колмогоров [25] показал, что интуиционистская логика имеет реальный смысл, не связанный с философскими установками Брауэра, если рассматривать ее как логику решения задач. В 40-е годы XX века американский логик и математик С. К. Клини предложил интерпретацию ряда специфических интуиционистских понятий на основе разработанных к тому времени концепций теории алгоритмов. Введенное им понятие рекурсивной реализуемости [24], [6, §82] послужило отправной точкой для разработки конструктивной математики, начатой в 50-е годы XX века советским математиком А. А. Марковым. Наконец, исследования последней четверти XX века в области теоретического программирования выявили особую роль интуционистской логики в вопросах синтеза программ, поскольку использование этой логики в математических построениях позволяет сделать явными их алгоритмические, вычислительные аспекты. Поэтому интуиционистская логика является одним из важных и актуальных направлений современной математической логики.

Настоящая книга написана на основе специальных курсов, читавшихся авторами на механико-математическом и философском факультетах Московского Государственного Университета имени М. В. Ломоносова. Она состоит из девяти глав. В главе 1 кратко излагается сущность кризиса оснований математики, вызванного обнаружением парадоксов в наивной теории множеств. Глава 2 посвящена основам интуиционизма как одного из направлений выхода из кризиса. Предваряя построение интуиционистской логики, в главе 3 рассматриваются основные понятия и конструкции, относящиеся к классической логике. В главе 4 вводятся интуиционистские пропозициональные исчисления. В главе 5 излагается теория псевдобулевых алгебр, которая затем в главе 6 применяется для исследования интуиционистского исчисления высказываний. В главе 7 вводятся модели Крипке для логики высказываний и доказывается полнота интуиционистского исчисления высказываний относительно семантики Крипке. В главе 8 вводится интуиционистское исчисление предикатов. В главе 9 вводятся модели Крипке для логики предикатов и доказывается полнота интуиционистского исчисления предикатов относительно семантики Крипке.

Книга предназначена для студентов и аспирантов, а также специалистов по математической логике, информатике и кибернетике.

В дальнейшем употребляется следующая общепринятая символика для замены слов и словосочетаний естественного языка: $\leftrightharpoons$ — «есть по определению»; $\forall$ — «для всех»; $\exists$ — «существует»; $\Leftrightarrow$ — «тогда и только тогда, когда»; $\cdots \Rightarrow \ldots$ — «если $\ldots$, то $\ldots$»; & — «и»; $\vee$ — «или». Символ $\Box$ означает конец доказательства.

Авторы будут признательны читателям, сообщившим о замеченных опечатках, ошибках и других погрешностях по адресу veplisko@yandex.ru или valkhakhanian@mtu-net.ru.

Глава 1

Теория множеств и кризис оснований математики

Возникновение интуиционизма связано с кризисом в основаниях математики, который был вызван обнаружением в конце XIX – начале XX веков противоречий в канторовской теории множеств.

§1.1. Три кризиса оснований математики

Слово «кризис» означает резкий крутой перелом, вызванный тяжелым положением. В истории математики насчитывают три так называемых *кризиса оснований математики.* При этом под основаниями математики понимается совокупность понятий, концепций и методов, с помощью которых строятся различные математические дисциплины, а также комплекс математических и философских теорий и направлений, посвященных исследованию этих понятий, концепций и методов.

Первый кризис оснований математики произошел в V веке до н. э. и был связан с обнаружением несоизмеримости стороны квадрата и его диагонали. Тяжесть положения определялась тем, что до того математики знали только целые и дробные числа, и считалось, что с их помощью можно выразить длину любого отрезка. Крутой перелом выразился в признании существования чисел, которые впоследствии были названы иррациональными.

Второй кризис оснований математики развернулся на рубеже XVII – XVIII веков и был порожден противоречивыми результатами в исчислении бесконечно малых в силу неудовлетворительного обоснования исходных понятий и принципов: одни математики считали бесконечно малые нулями и отбрасывали их при вычислениях, другие считали, что все же они отличны от нуля хотя и на очень малую величину. Стремясь преодолеть этот кризис, французский математик О. Л. Коши разработал теорию пределов.

Третий кризис оснований математики начался на рубеже XIX – XX веков и, как отмечается в [3], до сих пор не преоделен. Он связан с проникновением в математику методов теории множеств и обнаружением противоречий в этой теории.

§1.2. Арифметизация математики

Математический анализ как раздел математики начал складываться в трудах английского физика и математика И. Ньютона, немецкого философа, математика и физика Г. В. Лейбница и других ученых XVII – XVIII вв. Как отмечается в [3], под впечатлением мощи и плодотворности исчисления бесконечно малых большинство математиков активно применяли его методы, не задумываясь над тем, насколько прочна его основа. Внедрение в математику повышенной строгости началось лишь в XIX веке. Как уже отмечалось, Коши разработал теорию пределов. Чешский математик и философ Б. Больцано выдвинул идею арифметической теории действительных чисел. Эта идея была систематически разработана немецким математиком К. Т. В. Вейерштрассом, который начал так называемую *арифметизацию* математики, состоящую в сведении принципов математического анализа к простейшим арифметическим понятиям. Эта деятельность была продолжена немецкими математиками Л. Кронекером, Ю. В. Р. Дедекиндом и Г. Кантором. В результате арифметизации анализа все его основные понятия были сведены к рассмотрению натуральных чисел и бесконечных систем натуральных чисел. Как отмечается в [3], «это упрочение основ было настолько успешным, что Пуанкаре в 1900 г. ... смог гордо заявить, что математика уже обрела совершенно прочный и надежный фундамент». Глубокое исследование исходных понятий математического анализа было связано с развитием теории множеств, созданной Кантором. Эта теория явилась совершенно новой областью математических исследований, удовлетворяющей самым суровым требованиям к строгости.

§1.3. Элементы теории множеств

На начальном этапе своего развития теория множеств опиралась на интуитивные представления о множествах, и ныне этот этап характеризуется как *наивная теория множеств*. Согласно Кантору *множество* — это любое объединение в одно целое определенных объектов, которые называются *элементами* этого множества. Множество, элементами которого являются объекты $a_1, a_2, \ldots$, обозначается $\{a_1, a_2, \ldots\}$. Если x является элементом множества A, пишут $x \in A$. В противном случае пишут $x \notin A$. Множества A и B считаются *равными* ($A = B$), если $\forall x\,(x \in A \Leftrightarrow x \in B)$. Если $\forall x\,(x \in A \Rightarrow x \in B)$, говорят, что A является *подмножеством* множества B или что A *включено* в B. Семейство всех подмножеств множества A обозначается $\mathcal{P}(A)$. Если $A \subseteq B$ и $A \neq B$, то A называют *собственным подмножеством* множества B, а B — *собственным расширением* множества A, и пишут $A \subset B$.

Один из основных приемов наивной теории множеств — *принцип свертывания* (или *принцип абстракции*), согласно которому для всякого свойства $\Phi(x)$, которым произвольный объект x может обладать или не обладать, существует множество, обозначаемое $\{x \mid \Phi(x)\}$, элементами которого являются те и только те объекты x, которые обладают свойством $\Phi(x)$. С помощью принципа свертывания легко доказывается существование *пустого множества*: $\emptyset = \{x \mid x \neq x\}$.

Множество

$$A \cup B = \{x \mid x \in A \vee x \in B\}$$

называется *объединением* множеств A и B. *Пересечением* множеств A и B называется множество

$$A \cap B = \{x \mid x \in A \,\&\, x \in B\}.$$

Разностью множеств A и B называется множество

$$A \setminus B = \{x \mid x \in A \,\&\, x \notin B\}.$$

Порядок элементов в двухэлементном множестве $\{a, b\}$ не играет роли: $\{a, b\} = \{b, a\}$. Один из способов определения *упорядоченной пары* был предложен польским математиком К. Куратовским: упорядоченная пара $\langle a, b\rangle$ определяется как множество $\{\{a\}, \{a, b\}\}$. Для любого $n \geq 2$ можно индуктивно определить упорядоченный набор (*кортеж*) $\langle a_1, \ldots, a_n \rangle$ длины n:

$$\langle a_0, a_1, \ldots, a_n \rangle \risingdotseq \langle a_0, \langle a_1, \ldots, a_n \rangle \rangle.$$

Прямым (или *декартовым*) *произведением* множеств A и B называется множество

$$A \times B = \{\langle a, b \rangle \mid a \in A \,\&\, b \in B\}.$$

Аналогично определяется прямое произведение множеств $A_1, A_2, \ldots, A_n$ как множество

$$A_1 \times A_2 \times \cdots \times A_n = \{\langle a_1, \ldots, a_n \rangle | a_1 \in A_1,\ a_2 \in A_2, \ldots, a_n \in A_n\}.$$

Если $A_1 = A_2 = \cdots = A_n$, то множество $A_1 \times A_2 \times \cdots \times A_n$ называется *декартовой степенью* множества A и обозначается A^n.

§1.4. Соответствия и функции

Соответствием между множествами A и B называется любое множество $G \subseteq A \times B$. *Областью определения* соответствия G называется множество

$$D(G) = \{x \mid \exists y \, \langle x, y \rangle \in G\}.$$

Множеством значений соответствия G называется множество

$$E(G) = \{y \mid \exists x \, \langle x, y \rangle \in G\}.$$

Обратным соответствием для соответствия G называется соответствие

$$G^{-1} = \{\langle x, y \rangle \mid \langle y, x \rangle \in G\}$$

между множествами B и A. Если G — соответствие между множествами A и B, а F — соответствие между множествами B и C, то их *произведением* (или *композицией*) называется соответствие

$$G \circ F = \{\langle x, z \rangle \mid \exists y \, [\langle x, y \rangle \in G \,\&\, \langle y, z \rangle \in F]\}$$

между множествами A и C.

Соответствие G между множествами A и B называется *инъективным соответствием*, или *инъекцией*, если

$$\forall x_1, x_2, y \, [(\langle x_1, y \rangle \in G \,\&\, \langle x_2, y \rangle \in G) \Rightarrow x_1 = x_2];$$

тотальным или *всюду определенным соответствием*, если

$$D(G) = A;$$

сюръективным соответствием, или *сюръекцией*, если

$$E(G) = B;$$

функциональным соответствием, или *функцией из A в B*, если

$$\forall x, y_1, y_2\, [(\langle x, y_1\rangle \in G \,\&\, \langle x, y_2\rangle \in G) \Rightarrow y_1 = y_2].$$

Функцию f из A в B обозначают так: $f : A \to B$. Если $\langle x, y\rangle \in f$, пишут $y = f(x)$. Тотальная функция $f : A \to B$ называется *отображением A в B*. Тотальная и сюръективная функция $f : A \to B$ называется отображением A *на* B.

Соответствие G между множествами A и B называется *взаимно-однозначным соответствием* или *биекцией*, если оно функционально, инъективно, тотально и сюръективно. Множества A и B называются *равномощными*, если существует взаимно-однозначное соответствие между A и B. Чтобы выразить, что A и B равномощны, пишут $A \sim B$. Равномощные множества называются также *эквивалентными*.

Согласно Кантору, под *кардинальным числом* или *мощностью* множества A понимается то общее, что присуще всем множествам, эквивалентным множеству A. Независимо от способа представления того абстрактного объекта, который называется кардинальным числом, фундаментальное значение имеет то, что два множества A и B имеют одну и ту же мощность, если и только если они эквивалентны. Мощность множества A обозначается $|A|$. Если множество A равномощно некоторому подмножеству множества B, пишут $|A| \le |B|$. Если A и B не равномощны и выполнено неравенство $|A| \le |B|$, то пишут $|A| < |B|$.

Предложение 1 (теорема Кантора)**.** *Для любого множества A выполняется условие $|A| < |\mathcal{P}(A)|$.*

Доказательство. Фунция $g : A \to \mathcal{P}(A)$ такая, что $g(x) = \{x\}$, устанавливает взаимно-однозначное соответствие между A и подмножеством $\mathcal{P}(A)$, состоящим из всех одноэлементных подмножеств M, так что $|A| \le |\mathcal{P}(A)|$. Покажем, что $|A| \ne |\mathcal{P}(A)|$. Пусть f — какая-либо функция из A в $\mathcal{P}(A)$, и пусть

$$S = \{x \mid x \in A \,\&\, x \notin f(x)\}.$$

Очевидно, что $S \in \mathcal{P}(A)$. Покажем, что $S \notin E(f)$. Пусть $f(s) = S$ для некоторого $s \in A$. Простые рассуждения показывают, что в этом случае предположения $s \in S$ и $s \notin S$ оба ведут к противоречию. Таким образом, не существует взаимно-однозначного соответствия между A и $\mathcal{P}(A)$ $\square$

§1.5. Бинарные отношения

Когда множества A и B совпадают, соответствие между A и B называется *бинарным отношением на* A. Если R — бинарное отношение на A, то вместо $\langle x, y\rangle \in R$ пишут xRy. Бинарное отношение R на множестве A называется:

рефлексивным, если

$$(\forall x \in A)\,\langle x, x\rangle \in R;$$

иррефлексивным, если

$$(\forall x \in A)\,\langle x, x\rangle \notin R;$$

симметричным, если

$$(\forall x, y \in A)\,[\langle x, y\rangle \in R \Rightarrow \langle y, x\rangle \in R];$$

антисимметричным, если

$$(\forall x, y \in A)\,[(\langle x, y\rangle \in R \,\&\, \langle y, x\rangle \in R) \Rightarrow x = y];$$

транзитивным, если

$$(\forall x, y, z \in A)\,[(\langle x, y\rangle \in R \,\&\, \langle y, z\rangle \in R) \Rightarrow \langle x, z\rangle \in R].$$

Бинарное отношение на непустом множестве A называется *отношением эквивалентности*, или *эквивалентностью*, если оно рефлексивно, симметрично и транзитивно. Эквивалентность обозначают символом $\sim$. *Классом эквивалентности* элемента $x \in A$ по отношению эквивалентности $\sim$ на множестве A называется множество $[x]_\sim = \{y \mid x \sim y\}$. Множество всех классов эквивалентности элементов множества A по отношению эквивалентности $\sim$ называется *фактор-множеством* множества A по отношению эквивалентности $\sim$ и обозначается $A/_\sim$. Очевидно, что классы эквивалентности обладают следующими свойствами:

$$x \in [x]_\sim,$$

$$x \sim y \Rightarrow [x]_\sim = [y]_\sim,$$
$$x \not\sim y \Rightarrow [x]_\sim \cap [y]_\sim = \emptyset.$$

Таким образом, множество A разбивается на непересекающиеся классы эквивалентности по $\sim$.

Бинарное отношение называется *отношением предпорядка*, или *предпорядком*, если оно рефлексивно и транзитивно. Предпорядок обозначают символом $\leq$. Отношение предпорядка называется *отношением частичного порядка*, или *частичным порядком*, если оно антисимметрично. Непустое множество A с заданным на нем частичным порядком называется *частично упорядоченным*.

Предложение 2. *Пусть $\leq$ — предпорядок на множестве A. Тогда отношение $\sim$, определенное так:*

$$x \sim y \leftrightharpoons [x \leq y \,\&\, y \leq x], \tag{1.1}$$

является эквивалентностью на A. Если для любых $x, y \in A$ положить

$$[x]_\sim \leq [y]_\sim \leftrightharpoons x \leq y, \tag{1.2}$$

то отношение $\leq$ на множестве $A/_\sim$ является частичным порядком.

Доказательство. Рефлексивность отношения $\sim$ следует из рефлексивности исходного отношения $\leq$ на A. Симметричность отношения $\sim$ вытекает из определения (1.1). Транзитивность отношения $\sim$ следует из транзитивности отношения $\leq$ на A. Таким образом, $\sim$ является эквивалентностью на A.

Из транзитивности исходного отношения $\leq$ на множестве A следует, что если $x \leq y$ и $x \sim x'$, $y \sim y'$, то $x' \leq y'$. Поэтому определение (1.2) отношения $\leq$ на $A/_\sim$ является корректным в том смысле, что для любых классов эквивалентности $a, b \in A/_\sim$ неравенство $a \leq b$ не зависит от выбора представителей в a и b. Рефлексивность и транзитивность отношения $\leq$ на $A/_\sim$ следует непосредственно из аналогичных свойств исходного отношения $\leq$ на множестве A. Антисимметричность отношения $\leq$ на $A/_\sim$ доказывается так: если $[x]_\sim \leq [y]_\sim$ и $[y]_\sim \leq [x]_\sim$, то $x \leq y$ и $y \leq x$ в силу определения (1.2), а тогда в силу определения (1.1) $x \sim y$, т. е. $[x]_\sim = [y]_\sim$. Таким образом, отношение $\leq$ на $A/_\sim$ является частичным порядком. $\square$

§1.6. Числовые множества

К концу XIX века наивная теория множеств стала играть в математике роль своеобразного стандарта, в соответствии с которым любой математический объект можно определить как подходящее множество. *Натуральные числа* можно определить так: $0 \leftrightharpoons \emptyset$; если число n уже определено, то $n+1 \leftrightharpoons n \cup \{n\}$. После этого натуральный ряд можно охарактеризовать как наименьшее по включению множество $\mathbf{N}$, которое содержит $\emptyset$ и вместе с каждым элементом x содержит множество $\{x\}$. На таком определении натурального ряда основан принцип индукции. Всякая тотальная функция $f : \mathbf{N} \to A$ называется *последовательностью* (элементов множества A). В этом случае вместо $f(n)$ обычно пишут f_n. Множество называется *счетным*, если оно равномощно множеству $\mathbf{N}$. На множестве $\mathbf{N}$ естественным образом определяется операция сложения.

Теперь мы можем в рамках теории множеств ввести целые числа. На множестве $\mathbf{N}^2$ определим отношение эквивалентности $\sim$ следующим образом: $\langle a, b\rangle \sim \langle c, d\rangle \leftrightharpoons a+d = b+c$. В каждом классе эквивалентности есть ровно одна пара вида $\langle n, 0\rangle$ или $\langle 0, n\rangle$. Для натурального числа k положим $\mathbf{k} = [\langle k, 0\rangle]_\sim$, $-\mathbf{k} = [\langle 0, k\rangle]_\sim$. Элементами фактор-множества $\mathbf{N}^2/_\sim$ будут множества вида $\mathbf{k}$ и $-\mathbf{k}$. Они называются *целыми числами*. На множестве всех целых чисел $\mathbf{Z}$ естественным образом определяются операции сложения, вычитания и умножения.

Целые числа вида $\mathbf{k}$ $(k \in \mathbf{N})$ находятся в естественном взаимно-однозначном соответствии с натуральными числами. Целое число $\mathbf{k}$ считается представителем натурального числа k в $\mathbf{Z}$, и в этом смысле всякое натуральное число является целым числом. Множество всех целых чисел вида $\mathbf{k}$ также будем обозначать $\mathbf{N}$.

На множестве $\mathbf{Z} \times (\mathbf{N} \setminus \{\mathbf{0}\})$ определим отношение эквивалентности $\sim$ следующим образом: $\langle a, b\rangle \sim \langle c, d\rangle \leftrightharpoons a \cdot d = b \cdot c$. В каждом классе эквивалентности есть ровно одна такая пара $\langle k, n\rangle$, что целые числа k и n взаимно просты. Элементы фактор-множества $(\mathbf{Z} \times (\mathbf{N} \setminus \{\mathbf{0}\}))/_\sim$ называются *рациональными числами*.

Рациональные числа вида $[\langle k, 1\rangle]_\sim$ находятся в естественном взаимно-однозначном соответствии с целыми числами. Можно считать рациональное число этого вида представителем целого числа k в множестве рациональных чисел, и в этом смысле всякое целое число является рациональным числом. Множество всех рациональныых чисел вида $[\langle k, 1\rangle]_\sim$ также будем обозначать $\mathbf{Z}$.

На множестве всех рациональных чисел $\mathbf{Q}$ нетрудно определить операции сложения, вычитания, умножения и деления на число, отличное от 0, а также естественный порядок $\leq$.

Для определения действительных чисел в рамках теории множеств применялись различные конструкции. Рассмотрим одну из них, предложенную Кантором. Последовательность рациональных чисел $r : \mathbf{N} \to \mathbf{Q}$ называется *фундаментальной*, если для любого положительного рационального числа ε существует такое натуральное число n_ε, что для всех $n, m \geq n_\varepsilon$ выполняется неравенство $|r_n - r_m| < \varepsilon$. Последовательность рациональных чисел r называется *нульпоследовательностью*, если для любого положительного рационального числа ε существует такое натуральное число n_ε, что для всех $n \geq n_\varepsilon$ выполняется неравенство $|r_n| < \varepsilon$. Две фундаментальные последовательности рациональных чисел r и s называются *эквивалентными*, если их разность является нульпоследовательностью. Каждый класс эквивалентности называется *действительным числом*, а всякая фундаментальная последовательность из этого класса называется представителем этого действительного числа. Множество всех действительных чисел обозначается $\mathbf{R}$. Естественым образом определяются сумма и произведение двух действительных чисел.

Пусть $p \in \mathbf{Q}$. Тогда последовательность r, определяемая как $r_n = p$ для любого $n \in \mathbf{N}$, очевидно, является фундаментальной. Класс эквивалентности, содержащий эту последовательность, можно считать представителем рационального числа p в множестве всех действительных чисел.

Поскольку понятие функции из $\mathbf{R}$ в $\mathbf{R}$ определяется в рамках теории множеств, имеется возможность развивать математический анализ и другие разделы математики на основе теории множеств.

§1.7. Парадоксы теории множеств

Таким образом, математический анализ и основанные на нем разделы математики были сведены к теории множеств и, как казалось, получили единое и прочное обоснование. Поэтому обнаружение противоречий в теории множеств явилось драматическим событием в истории математики. Рассмотрим два таких противоречия.

Парадокс Кантора. Пусть M — множество всех множеств. По теореме Кантора (предложение 1) $|M| < |\mathcal{P}(M)|$. Но M содержит в себе все множества, так что $\mathcal{P}(M) \subseteq M$. Значит, $|\mathcal{P}(M)| \leq |M|$. Получили противоречие.

Как отмечается в [3], этот парадокс был известен самому Кантору еще в 1899 г., но был опубликован лишь в 1932 г. (см. [15]).

Парадокс Рассела. Пусть $T = \{x \mid x \notin x\}$, т. е. $x \in T \Leftrightarrow x \notin x$. Взяв здесь T в качестве x, получаем $T \in T \Leftrightarrow T \notin T$. Это также противоречие.

Этот парадокс был обнаружен английским математиком, логиком и философом Б. Расселом в 1902 г. и был опубликован им в 1903 г. (см. [26]).

Обнаружение парадоксов в канторовской теории множеств вызвало третий кризис оснований математики. Поиски выхода из него оказались мощным стимулом для исследований по аксиоматизации теории множеств и математической логике. С этим связано и оформление интуиционистского направления в математике.

Упражнения

1. Доказать, что если $A \subseteq B \subseteq C$ и $|A| = |C|$, то $|B| = |C|$.

2. Доказать *теорему Кантора – Бернштейна*:
$$|A| \leq |B| \,\&\, |B| \leq |A| \Rightarrow |A| = |B|.$$

3. Доказать, что множество $\mathcal{P}_{fin}(A)$ всех конечных подмножеств счетного множетва A счетно.

4. Доказать, что множество $\mathcal{P}(\mathbf{N})$ несчетно.

Глава 2

Интуиционизм

Аксиоматизация теории множеств, начатая Цермело, служила ответом на вопрос «Что делать?», обычно возникающий в кризисной ситуации. Ответ на другой вопрос «Кто виноват?» также интересовал математиков. Неожиданная попытка ответа на него привела к возникновению интуиционистского направления в математике.

§2.1. Интуиционистская критика классической математики

Парадоксы теории множеств свидетельствуют о неблагополучии классической математики в целом. Еще задолго до их обнаружения высказывались сомнения в обоснованности некоторых методов образования математических понятий и способов рассуждения о них. В частности, обсуждался статус существования в математике. В связи с любым определением возникает вопрос о существовании объекта, удовлетворяющего этому определению. Обычно этот вопрос решается указанием такого объекта. Однако в математике известны «теоремы чистого существования», когда доказывается существование объекта без предъявления способа его построения (например, доказательство существования трансцендентных чисел, основанное на счетности множества всех алгебраических чисел, а также многие доказательства, использующие аксиому выбора). В аксиоматических теориях существование объекта с данным свойством считается доказанным, если предположение о его несуществовании ведет к противоречию. Такие доказательства в классической математике высоко ценились за их остроумие.

Признание построения объекта единственно законным способом доказательства существования является характерной особенностью интуиционизма — направления в математике, признающего единственным критерием правомерности тех или иных методов их интуитивную убедительность. Интуиционистские идеи высказывались еще Л. Кронекером и Ж. А. Пуанкаре, однако тогда они относились к философии математики и не воплощались в конкретные математические построения. Так, Пуанкаре настаивал на «изначальной интуиции» математической индукции, которая является проявлением некоторых свойств нашего разума. Однако он признавал доказательство непротиворечивости доказательством существования. Для Кронекера характерно признание доказательства существования объекта только с помощью построения. При этом он считал, что этот объект существует сам по себе и лишь копируется нами.

Явно и последовательно взгляды интуиционистов были сформулированы в диссертации Л. Э. Я. Брауэра «Об основаниях математики», опубликованной в 1907 г. на голландском языке. Касаясь философии математики, Брауэр заявляет, что чистая математика представляет собой свободное творчество разума и не имеет никакого отношения к опыту. Наблюдение правильно повторяющейся последовательности событий может привести к образованию некоторой математической системы, однако в современной чистой математике, напротив, чаще всего образуются абстрактные математические системы, которыми затем пользуются другие науки для приведения в систему результатов наблюдений с целью достижения большей ясности.

Деятельность Брауэра не ограничилась лишь философскими рассуждениями. Начиная с работы «Основание теории множеств, независимое от логического закона исключенного третьего», опубликованной в 1918 – 1919 гг. (см. [13]), Брауэром велась разработка совершенно нового подхода к обоснованию анализа и теории множеств. Признавая «изначальную интуицию» натурального числа, интуиционизм рассматривает арифметику как основу всей математики. При этом отвергается как интуитивно ясное представление о континууме в виде геометрического пространства, характерное для древнегреческой математики.

Рассмотрим некоторые примеры конкретной реализации идей интуиционизма при построении математических теорий.

§2.2. Элементы интуиционистской математики

Согласно интуиционистской доктрине математические объекты порождаются человеческим сознанием, поэтому истинность суждений о них определяется представлениями об этих объектах того математика, в сознании которого они возникли. В силу некоторых общих свойств человеческого мышления возможно образование в сознании разных людей одинаковых математических понятий. К ним относится изначальная интуиция натурального числа, или построение его по математической индукции. Построение натурального числа n состоит в последовательном построении натуральных чисел от 1 до n. Процесс построения натуральных чисел можно фиксировать в материальной форме. Например, с каждым шагом построения мы можем связывать написание палочки I на бумаге. Тогда слово I будет отождествляться с числом 1, слово II — с числом 2, и т. д. Такой взгляд позволяет пользоваться в доказательствах методом индукции. Пусть $P(x)$ — такое свойство натуральных чисел, что $P(1)$ истинно, и с помощью некоторого рассуждения можно заключить, что из $P(n)$ следует $P(n')$, где n' — число, построенное на следующем шаге после n. Теперь, если m — произвольное натуральное число, мы знаем, что в процессе построения чисел от 1 до m на каждом шаге сохраняется свойство P, следовательно, $P(m)$ истинно.

С точки зрения интуиционизма построение математических объектов и рассуждения о них должны подчиняться критерию интуитивной ясности и убедительности. В конкретных математических конструкциях интуиционизм проявляется в отказе от рассмотрения бесконечной совокупности как данной в завершенном виде. В интуиционистской математике бесконечность рассматривается лишь как *становящаяся*, или *потенциальная*. Так, натуральный ряд в интуиционисткой математике рассматривается не как завершенная совокупность, а лишь как процесс построения натуральных чисел, начиная с 1.

Отправляясь от понятия натурального числа, на основе интуиционистских представлений можно развивать своеобразную математическую теорию. Не представляет труда построение целых и рациональных чисел. Отрицательные целые числа можно отождествлять со словами вида $-n$, где n — натуральное число, 0 можно отождествить с пустым словом. Нетрудно с помощью подходящих алгоритмов над словами определить операции сложения и вычитания целых чисел. Рациональные числа можно отождествить с несократимыми дробями вида m/n, где m — целое, а n — натуральное число. Алгоритмически определяются арифметические операции на рациональных числах. Теперь можно, подражая классической теории, строить интуиционистскую теорию действительных чисел.

§2.3. Свободно становящиеся последовательности

Пусть задано некоторое правило последовательного построения рациональных чисел: на первом шаге строится число r_1, на втором — число r_2, и т. д. В таком случае будем говорить, что дана последовательность r. При этом правило построения r_n может быть произвольным: число r_n может строиться посредством некоторого алгоритма или выбираться случайно. Главная особенность интуиционистского понимания последовательности состоит в том, что гарантирована возможность неограниченного ее продолжения, причем сама последовательность никогда не бывает дана в готовом виде: нам может быть задан только конечный ее отрезок. В этом смысле последовательность является *потенциально бесконечной*. В интуиционистской математике для таких последовательностей используется термин «*свободно становящаяся последовательность*».

Последовательность рациональных чисел r называется фундаментальной, если для каждого натурального числа k мы можем найти натуральное число n_0 такое, что для всех $m, n \geq n_0$ выполняется неравенство $|r_n - r_m| \leq \frac{1}{k}$. Например, последовательность $r_n = \frac{1}{2^n}$ является фундаментальной последовательностью. Действительно, для любого данного k в качестве n_0 можно взять наименьшее число n такое, что $2^n \geq k$. Рассмотрим последовательность q_n, определяемую следующим образом: если n-й знак после запятой в десятичном разложении числа π есть 9 первого вхождения последовательности 0123456789 в это разложение, то $q_n = 1$; в противном случае $q_n = \frac{1}{2^n}$. Очевидно, что последовательность q_n отличается от последовательности r_n не более чем одним членом, но пока мы не знаем, встречается ли последовательность 0123456789 в десятичном разложении числа π, мы не можем найти такое n_0, что для всех $m, n \geq n_0$ выполняется неравенство $|q_n - q_m| \leq \frac{1}{2}$. Следовательно, мы не имеем права утверждать, что последовательность q_n является фундаментальной.

Даже при случайном выборе членов последовательности r_n можно позаботиться, чтобы эта последовательность была фундаментальной. Рассмотрим, например, такую последовательность α. Для построения α_1 следует бросить монету и в качестве α_1 взять середину левой или правой половины отрезка $[0,1]$ в зависимости от того, выпали «орел» или «решка». Таким образом, если выпал «орел», мы полагаем $\alpha_1 = \frac{1}{4}$; если же выпала «решка», полагаем $\alpha_1 = \frac{3}{4}$. На каждом дальнейшем шаге построения последовательности α будем поступать аналогично. А именно, если при построении числа α_n был выбран отрезок $[p,q]$, то для построения числа α_{n+1} следует бросить монету, выбрать левую или правую половину отрезка $[p,q]$ в зависимости от того, выпали «орел» или «решка», и в качестве α_{n+1} взять середину выбранного отрезка. Очевидно, что для любых n и m выполняется $|\alpha_n - \alpha_{n+m}| < \frac{1}{2^n}$, так что последовательность α является фундаментальной.

Фундаментальная последовательность рациональных чисел называется *действительным числовым генератором.* Будем считать, что два действительных числовых генератора $a = a_n$ и $b = b_n$ совпадают, и писать $a = b$, если для любого натурального k мы можем найти такое n_0, что для всех $n \geq n_0$ выполняется неравенство $|a_n - b_n| \leq \frac{1}{k}$. Нетрудно проверить, что отношение совпадения между действительными числовыми генераторами является рефлексивным, симметричным и транзитивным (см. упражнение 1).

Неравенство действительных числовых генераторов a и b означает, что предположение $a = b$ ведет к противоречию, и обозначается $a \neq b$. Более сильное различие между действительными числовыми генераторами выражается в следующем понятии. Говорят, что числовые генераторы a и b отделены, и пишут $a\#b$, если можно найти такие n и k, что для любого $p \geq n$ выполняется неравенство $|a_p - b_p| > \frac{1}{k}$. Условие $a\#b$ влечет $a \neq b$. Обратное, вообще говоря, неверно. Можно привести пример такого числового генератора a, что $a \neq 0$ (здесь 0 — последовательность, все члены которой равны 0), однако утверждение $a\#0$ остается недоказанным. Идея построения этого примера основана на так называемых «исторических аргументах Брауэра», которые он изложил в докладе на 10-м Международном философском конгрессе в Амстердаме в 1948 г. (см [14]). Представим себе, что имеется некий творческий субъект, занимающийся решением математических проблем, идеализированный в том смысле, что он потенциально бессмертен и обладает неограниченными способностями, позволяющими ему рано или поздно решить любую проблему (в качестве такого субъекта можно вообразить все человечество в целом). Зафиксируем некоторую пока что нерешенную математическую проблему Ф и определим числовой генератор a следующим образом. Фиксируем некоторую неограниченно продолжаемую дискретную последовательность моментов времени $0, 1, 2, \ldots$. Например, это может быть отсчет дней, начиная с некоторого фиксированного дня. Значение a_n будет определяться в момент n согласно следующему правилу: если к моменту времени n наш творческий субъект еще не решил проблему Ф, полагаем $a_n = \frac{1}{2^n}$; если же он решил проблему Ф в момент $m \leq n$, полагаем $a_n = \frac{1}{2^m}$. Очевидно, что условие $a = 0$ означало бы, что проблема Ф никогда не будет решена, а это противоречит нашим представлениям о способностях творческого субъекта. Поэтому $a \neq 0$, причем этот факт мы установили уже в начальный момент. С другой стороны, истинность утверждения $a\#0$ означает, что мы можем указать такие n и k, что для любого $p \geq n$ выполняется неравенство $a_p > \frac{1}{k}$. Отсюда следует, что проблема Ф будет решена до момента q такого, что $2^q < k$. Но очевидно, что такое q нам станет известно только тогда, когда проблема Ф будет решена, а в начальный момент мы его указать не можем. Таким образом, в начальный момент утверждение $a \neq 0$ истинно, а $a\#0$ — нет.

Сравнивая понятие действительного числового генератора с классическим понятием действительного числа по Кантору, можно заметить, что каждый действительный числовой генератор является представителем некоторого действительного числа, причем совпадающие генераторы представляют одно и то же число. Приведенный выше пример последовательности α показывает, что в принципе ни одно действительное число из отрезка $[0, 1]$ не может быть исключено из рассмотрения. В этом смысле интуиционистский континуум, представленный действительными числовыми генераторами, ничуть не беднее континуума обычных действительных чисел. Однако важно, что в рассуждениях о действительном числовом генераторе мы должны исходить из того, что нам задан только начальный его фрагмент, и все выводы должны делаться на основе лишь той информации, которая содержится в этом фрагменте, и не зависеть от возможных его продолжений.

Хотелось бы определить интуиционистское действительное число как класс эквивалентности действительных числовых генераторов по отношению совпадения. В связи с этим уместно коснуться интуиционистских взглядов на понятие множества.

§2.4. Потоки и виды

С точки зрения интуиционизма приемлемы следующие два способа определения множества: 1) посредством задания способа порождения его элементов; 2) посредством указания свойства, которое характеризует элементы множества. Первый способ задания множеств уточняется с помощью понятия потока. Говорят, что задан *поток* M, если, во-первых, указан *закон потока* Λ, с помощью которого строятся конечные последовательности натуральных чисел, и, во-вторых, указан *дополнительный закон* Γ, который каждой конечной последовательности, построенной в соответствии с законом Λ, сопоставляет некоторый математический объект. При этом закон потока Λ делит конечные последовательности натуральных чисел на допустимые и недопустимые и должен удовлетворять следующим условиям:

1) для любого натурального числа k этот закон позволяет установить, является ли оно членом допустимой одноэлементной последовательности;

2) если допустима последовательность $a_0, a_1, \ldots, a_n, a_{n+1}$, то допустима и последовательность $a_0, a_1, \ldots, a_n$;

3) если дана допустимая последовательность $a_0, a_1, \ldots, a_n$, то закон Λ позволяет для любого натурального числа k решить, является ли допустимой последовательность $a_0, a_1, \ldots, a_n, k$;

4) для любой допустимой последовательности $a_0, a_1, \ldots, a_n$ можно найти хотя бы одно натуральное число k такое, что последовательность $a_0, a_1, \ldots, a_n, k$ является допустимой.

Свободно становящаяся последовательность называется *допустимой*, если каждый начальный ее фрагмент допустим согласно закону потока Λ.

Пусть a — допустимая свободно становящаяся последовательность, и пусть b_n есть объект, сопоставляемый дополнительным законом Γ конечной последовательности $a_1, \ldots, a_n$. Тогда свободно становящаяся последовательность $b_1, b_2, \ldots$ называется *элементом потока M*.

Поток, элементами которого являются действительные числовые генераторы, можно определить следующим образом. Пусть фиксирован некоторый эффективный пересчет всех рациональных чисел $r_1, r_2, \ldots$. Закон потока Λ зададим так:

1) каждое натуральное число образует допустимую одночленную последовательность;

2) если последовательность $a_1, \ldots, a_n$ допустима, то последовательность $a_1, \ldots, a_n, k$ является допустимой тогда и только тогда, когда $|r_{a_n} - r_k| < \frac{1}{2^n}$.

Дополнительный закон Γ сопоставляет допустимой последовательности $a_1, \ldots, a_n$ рациональное число r_{a_n}. Очевидно, что все элементы этого потока являются действительными числовыми генераторами, и, обратно, для любого действительного числового генератора можно построить элемент этого потока, представляющий то же действительное число.

Если множество определяется посредством указания свойства, характеризующего элементы этого множества, то соответствующее свойство называется *видом*, а всякий объект, обладающий этим свойством, называется *членом* данного вида. Очевидно, можно рассматривать вид, состоящий в совпадении действительного числового генератора с данным действительным числовым генератором. Такой вид называется действительным числом, а всякий его член — представителем этого действительного числа.

§2.5. Интуиционизм и логика

Касаясь вопроса о соотношении интуиционистской математики и логики А. Гейтинг [11] указывает: «Умозаключения интуиционистской математики не производятся по твердо установленным предписаниям, которые можно было бы объединить в логическую систему, наоборот, очевидность всякого отдельного вывода испытывается непосредственно». Таким образом, интуиционистская математика не пользуется какой-либо априорной логической системой. Единственным критерием правильности рассуждения является интуитивная ясность каждого логического шага. Однако это не исключает существования некоторых общих правил, по которым из одних математических утверждений интуитивно ясным путем получаются другие утверждения. Выявление и изучение таких правил составляет предмет *интуиционистской логики*, являющейся важным разделом современной математической логики. Одним из естественных путей построения интуиционистской логики является критический анализ классической логики и выявление тех ее принципов, которые приемлемы интуиционистски.

В 1908 г. появилась работа Л. Э. Я. Брауэра «Недостоверность логических принципов» (на голландском языке). В ней отмечалось, что правила классической логики, дошедшие до нас от Аристотеля (IV век до н. э.), абстрагированы от обращения с конечными совокупностями. Забывая об этом, впоследствии эту логику ошибочно приняли за нечто первичное по отношению к математике и в конце концов стали применять ее без какого-либо оправдания к математике бесконечных множеств. Принципом классической логики, который Брауэр не принимает для бесконечных множеств, является *закон исключенного третьего*: «Для любого высказывания Φ, либо Φ, либо не Φ». Пусть Φ есть высказывание «Существует элемент множества D, обладающий свойством P», причем свойство P таково, что для любого элемента из D мы можем определить, обладает ли он свойством P. Тогда «не Φ» эквивалентно утверждению «Каждый элемент из D не обладает свойством P». Если D — конечное множество, то в принципе можно обследовать по очереди все его элементы и либо найти элемент, обладающий свойством P, либо убедитьсяся, что все элементы не обладают свойством P, так что в этом случае справедлив закон исключенного третьего. Если же D бесконечно, то принципиально невозможно закончить исследование всех его элементов. Для некоторых множеств D и свойств P мы можем найти элемент, обладающий свойством P, или, напротив, доказать посредством математического рассуждения, что каждый элемент множества D не обладает свойством P (как, например, с помощью известного рассуждения доказывается, что не существует таких натуральных чисел m и n, что $m^2 = 2n^2$). Однако нет никакой уверенности в существовании такого решения вопроса об истинности утверждения Φ в общем случае. Правда, можно было бы считать, что всякая проблема разрешима «в принципе», но это означало бы привлечение философских допущений, что в математике делать не принято.

При построении логики несколько иной, чем в традиционной, классической логике, смысл интуиционисты придают исходным логическим понятиям. В традиционной логике высказывание понимается как такое предложение, которое может быть истинным или ложным, так что истинностное значение есть непременный атрибут всякого высказывания. Интуиционистский взгляд на истинность высказывания представляется более соответствующим математической практике. С точки зрения интуиционизма, истинность высказывания связана с возможностью его доказательства. Таким образом, высказывание считается истинным, если имеется его доказательство. Чтобы избежать ассоциаций с доказательствами в формальных теориях, вместо термина «доказательство» мы будем употреблять термин «обоснование».

В контексте такой трактовки истинности высказывания понимаются и традиционные логические операции: *конъюнкция* $\&$, соответствующая союзу «и», *дизъюнкция* $\vee$, соответствующая союзу «или», *импликация* $\supset$, соответствующая обороту «Если ..., то ...». Так, высказывание $\Phi \,\&\, \Psi$ считается истинным тогда и только тогда, когда истинны оба высказывания Φ и Ψ, т. е. мы располагаем обоснованием каждого из этих высказываний. Высказывание $\Phi \vee \Psi$ считается истинным тогда и только тогда, когда истинно хотя бы одно из высказываний Φ и Ψ, т. е. мы располагаем обоснованием высказывания Φ или обоснованием высказывания Ψ. Высказывание $\Phi \supset \Psi$ считается истинным тогда и только тогда, когда имеется некий общий метод, позволяющий любое обоснование высказывания Φ преобразовать в обоснование высказывания Ψ.

Интуиционистская трактовка *квантора существования* $\exists x$, соответствующего обороту «Существует x такой, что ...», и *квантора всеобщности* $\forall x$, соответствующего обороту «Для всех x ...», состоит в следующем. Пусть $\Phi(x)$ — некоторое свойство, которым могут обладать или не обладать объекты подходящим образом заданного множества. Тогда высказывание $\exists x\, \Phi(x)$ считается истинным, если для некоторого конкретного объекта a из рассматриваемого множества мы имеем обоснование высказывания $\Phi(a)$. Высказывание $\forall x\, \Phi(x)$ считается истинным, если имеется общий метод, позволяющий для любого конкретного объекта a из рассматриваемого множества получить обоснование высказывания $\Phi(a)$.

Понятие ложного высказывания не является самостоятельным в интуиционисткой логике: высказывание Φ считается ложным, если нам удалось доказать высказывание $\Phi \supset \perp$, где $\perp$ — некоторое абсурдное высказывание (например, $0 = 1$), заведомо не имеющее обоснования. Высказывание $\Phi \supset \perp$ называется отрицанием высказывания Φ и обозначается $\neg\Phi$. Очевидно, что если высказывание Φ истинно, то его отрицание $\neg\Phi$ не может быть истинным.

Таким образом, в отличие от класической логики, где каждое высказывание либо истинно, либо ложно, в интуиционистской логике высказывания подразделяются на три класса: истинные, ложные и все прочие, или непроверенные, при этом только принадлежность высказывания к одному из первых двух классов является окончательной, а всякое непроверенное высказывание с течением времени в результате исследовательской деятельности человека может перейти в разряд истинных (если удастся доказать его) или в разряд ложных (если удастся его опровергнуть, т. е. доказать истинность отрицания этого высказывания).

Мы видим, что интуиционистское понимание некоторых видов высказываний существенно отличается от классического. Пусть, например, высказывание имеет вид $\Phi \vee \neg\Phi$. Если Φ — истинное высказывание, например, 0=0, то высказывание $\Phi \vee \neg\Phi$ также истинно. Аналогично, высказывание $\Phi\vee\neg\Phi$ истинно, если Φ — ложное высказывание, например, 0=1. Если же Φ — непроверенное высказывание (такое высказывание нетрудно найти в современной научной литературе, где формулируются нерешенные математические проблемы), то мы не можем утверждать, что высказывание $\Phi \vee \neg\Phi$ истинно. Но с классической точки зрения это высказывание истинно, правда, единственным аргументом здесь является сомнительный тезис, что такое высказывание «истинно всегда».

Рассмотрим еще один хрестоматийный пример математического доказательства, которое неприемлемо с интуиционистской точки зрения. Этот пример приводится в книге А. Г. Драгалина [8] со ссылкой на ван Далена [27].

Теорема 1. *Существуют иррациональные числа a и b такие, что число a^b рационально.*

Доказательство. Рассмотрим число $\sqrt{2}^{\sqrt{2}}$. Если оно рационально, то можно взять $a = \sqrt{2}$, $b = \sqrt{2}$. Если же число $\sqrt{2}^{\sqrt{2}}$ иррационально, можно взять $a = \sqrt{2}^{\sqrt{2}}$, $b = \sqrt{2}$. Таким образом, в любом случае нужные a и b существуют. $\square$

Это доказательство является ярким образцом доказательства «чистого существования», и для интуициониста, очевидно, оно неприемлемо. К счастью, для рассматриваемой теоремы имеется и другое, более глубокое доказательство, показывающее, что число $\sqrt{2}^{\sqrt{2}}$ иррационально, так что искомые числа таковы: $a = \sqrt{2}^{\sqrt{2}}$, $b = \sqrt{2}$.

Упражнения

1. Доказать, что отношение совпадения между числовыми генераторами является отношением эквивалентности.

2. Доказать, что если a, b, c — действительные числовые генераторы, и $a\#b$, $b = c$, то $a\#c$.

3. Доказать, что если a, b — действительные числовые генераторы, и $a\#b$, то для любого действительного числового генератора c имеет место $a\#c$ или $b\#c$.

Глава 3

Элементы классической логики

Логика как наука о законах и формах рассуждений возникла в странах Древнего Востока — Китае и Индии. В основе современной классической логики лежит *формальная традиционная логика*, разработка которой была начата древнегреческим ученым Аристотелем в IV веке до н. э. Им была разработана первая формализация рассуждений в виде *силлогизмов*. В XVII веке логика признается как рабочий инструмент всех других наук и практики, поскольку она принуждает к строгим формулировкам мысли. Г. Лейбниц выдвинул идею построения универсального символического языка для записи суждений и формулирования логических принципов в виде правил, позволяющих строить содержательные рассуждения подобно математическим вычислениям. Тогда, по мнению Лейбница, вместо того, чтобы спорить, ученые скажут: «давайте вычислим» (по латыни — «calculemus»). Лейбниц считается основоположником математической логики. В XIX веке появились первые научные работы по алгебраизации традиционной формальной логики. Английский математик и логик Дж. Буль обнаружил аналогии между алгеброй и логикой, в результате чего им были разработаны основы *алгебры логики*, в которой законы арифметики и правила арифметических действий переносятся на логические операции над высказываниями. Независимо от него к сходным идеям пришел шотландский математик и логик О. де Морган. Важным шагом в развитии математической логики явилась аксиоматизация логики и арифметики, предпринятая немецким математиком и логиком Ф. Л. Г. Фреге. Мощным стимулом для формирования современного облика математической логики и ее развития послужили исследования, проводимые в русле осуществления выдвинутой Д. Гильбертом программы обоснования математики с целью спасения последней от парадоксов. Суть этой программы состояла в строгой формализации математических теорий и изучении формальных доказательств.

§3.1. Алфавит, буква, слово

Математическая логика в основном занимается изучением математических рассуждений. В математике рассуждения обычно оформляются в виде математических текстов. Поэтому будет уместно рассмотреть некоторые общие понятия, относящиеся к письменным математическим языкам.

Элементарные знаки, из которых состоит текст, называются *буквами.* При использовании того или иного значка в качестве буквы нас не интересуют части этого значка, а лишь этот знак в целом. При выборе букв необходимо быть уверенным в том, что всякий раз, рассматривая любые две написанные буквы, мы сможем определить, *одинаковы* эти буквы или *различны.*

Алфавит — это конечный список букв. *Слово* в данном алфавите — конечная последовательность букв этого алфавита. Слово XY, полученное приписыванием справа к слову X слова Y, называется *произведением* слов X и Y. Операция произведения слов ассоциативна, но не коммутативна. Слово X называется *началом* слова Y, если существует такое слово Z, что $Y = XZ$. Слово X называется *концом* слова Y, если существует такое слово Z, что $Y = ZX$.

Отметим следующие очевидные факты:

- если X и Y — начала слова Z, то X — начало слова Y или Y — начало слова X;
- если X и Y — концы слова Z, то X — конец слова Y или Y — конец слова X.

Говорят, что слово X *входит* в слово Y, если существуют такие слова U и V, что $Y = UXV$. Слово U называется *левым крылом* данного вхождения слова X в слово Y, а V — *правым крылом* этого вхождения. Различные вхождения слова X в слово Y различаются левыми и правыми крыльями этих вхождений.

Пусть слово X входит в слово Y, и пусть Z — произвольное слово. Зафиксируем некоторое вхождение слова X в Y, т. е. представление слова Y в виде UXV. Тогда слово UZV называется результатом *замены* данного вхождения слова X в слово Y на слово Z.

§3.2. Алгебра высказываний

Высказывания и логические операции. Математическая логика математическими методами изучает математические рассуждения. Всякое рассуждение состоит в последовательном переходе от одного суждения к другому. Материальным выражением суждения является предложение того или иного языка.

Высказывание — это повествовательное предложение, для которого имеет смысл говорить о его истинности или ложности. Этим высказывания отличаются, например, от повелительных или вопросительных предложений. Если высказывание истинно, говорят, что его *истинностное значение* есть *«истина»*, а если высказывание ложно, то его истинностное значение есть *«ложь»*. Истинностные значения «истина» и «ложь» мы будем обозначать числами 1 и 0 соответственно.

Из одних высказываний различными способами можно строить новые, более сложные высказывания. *Логическая операция* — это такой способ построения сложного высказывания из данных высказываний, при котором истинностное значение сложного высказывания полностью определяется истинностными значениями данных высказываний. Для каждой логической операции зависимость истинностного значения полученного с ее помощью сложного высказывания от истинностных значений исходных высказываний можно задать с помощью таблицы. Одноместная операция $\neg$ (*отрицание*), двухместные операции & (*конъюнкция*), $\vee$ (*дизъюнкция*), $\supset$ (*импликация*) задаются следующими таблицами:

A	$\neg A$
0	1
1	0

A	B	$A \,\&\, B$	$A \vee B$	$A \supset B$
0	0	0	0	1
0	1	0	1	1
1	0	0	1	0
1	1	1	1	1

Логические операции $\neg, \&, \vee, \supset$ называются *пропозициональными операциями*, а символы, используемые для их обозначения — *пропозициональными связками.*

$\neg A$ читается как «Неверно, что A», $A \,\&\, B$ — как «A и B», $A \vee B$ — как «A или B», $A \supset B$ — как «Если A, то B».

Пропозициональные формулы. Алфавит *языка логики высказываний* состоит из символов P, $\neg$, &, $\vee$, $\supset$, (,). Слова $(P), (PP), (PPP), \ldots$ будем называть *пропозициональными переменными* и обозначать соответственно $P_1, P_2, P_3, \ldots$. В свою очередь, вместо $P_1, P_2, P_3, \ldots$ будем иногда писать $P, Q, R, \ldots$.

Понятие *пропозициональной формулы* определяется индуктивно следующим образом.

1. Всякая пропозициональная переменная есть формула (такая формула называется *атомом*).

2. Если A — формула, то слово $(\neg A)$ считается формулой.

3. Если A и B — формулы, то слова $(A \lambda B)$, где $\lambda \in \{\&, \vee, \supset\}$, считаются формулами.

Сущность этого определения состоит в том, что слово в алфавите языка логики высказываний считается формулой, если и только если этот факт может быть обоснован с помощью пунктов 1 – 3 приведенного определения. Докажем, например, что слово $(P \supset (\neg Q))$ является формулой. Согласно пункту 1 данного определения переменные P и Q являются формулами. Согласно пункту 2 слово $(\neg Q)$ является формулой. Наконец, согласно пункту 3 слово $(P \supset (\neg Q))$ также является формулой.

Вообще, слово A в алфавите языка логики высказываний является формулой тогда и только тогда, когда существует конечная последовательность слов $A_1, \ldots, A_n$ такая, что для каждого $i = 1, \ldots, n$ слово A_i либо получено по правилу 1, т. е. является пропозициональной переменной, либо получается из одного или двух предшествующих слов по правилу 2 или 3, и при этом A_n совпадает с A. Такую последовательность можно рассматривать как историю построения формулы A в соответствии с правилами 1 – 3. Например, следующая последовательность представляет историю построения формулы $(P \supset (\neg Q))$:

1) P (получено по правилу 1);

2) Q (получено по правилу 1);

3) $(\neg Q)$ (получено по правилу 2 из слова 2));

4) $(P \supset (\neg Q))$ (получено по правилу 3 из слов 1) и 3)).

Индуктивный характер определения формулы позволяет использовать в доказательствах *метод индукции по построению формулы*: если требуется доказать, что все формулы обладают данным свойством, то для этого достаточно установить, что а) каждый атом обладает данным свойством;

б) если слово A обладает данным свойством, то слово $(\neg A)$ обладает данным свойством;

в) если слова A и B обладают данным свойством, то слова $(A \,\&\, B)$, $(A \vee B)$, $(A \supset B)$ обладают данным свойством.

Чтобы доказать, что некоторое слово X не является формулой, достаточно найти такое свойство, которым слово X не обладает, а все формулы им обладают, причем последний факт может быть доказан индукцией по построению формулы. Докажем, например, что слово $((P) \supset \neg(PP))$ не является формулой. Для этого рассмотрим свойство слов в алфавите языка логики высказываний, состоящее в том, что количество левых скобок в слове равно суммарному количеству вхождений переменных и логических связок в это слово. Заметим, что в слове $((P) \supset \neg(PP))$ есть два вхождения переменных и два вхождения логических связок, так что суммарное количество вхождений переменных и логических связок равно четырем, а левых скобок всего три, и это слово не обладает рассматриваемым свойством. Докажем, что любая формула обладает этим свойством. Каждый атом содержит одну левую скобку и одно вхождение переменной, следовательно, обладает рассматриваемым свойством. Пусть слово A обладает рассматриваемым свойством. В слове $(\neg A)$ количество левых скобок на единицу больше, чем в A, количество переменных такое же, как и в слове A, а количество логических связок на единицу больше, чем в A. Следовательно, и в слове $(\neg A)$ количество левых скобок равно суммарному количеству вхождений переменных и логических связок, так что оно обладает рассматриваемым свойством. Аналогично доказывается, что слово вида $(A\lambda B)$, где λ есть $\&$, $\vee$ или $\supset$ обладает рассматриваемым свойством, если слова A и B обладают этим свойством.

В дальнейшем формулу $((A \supset B) \,\&\, (B \supset A))$ будем обозначать $(A \equiv B)$. Будем говорить, что формула A является *подформулой* формулы B, если A входит в B.

Практически, записывая формулы, мы будем опускать некоторые скобки, рассматривая полученные выражения как сокращенные записи исходных формул. В частности, мы не будем писать внешние скобки у формул, а также вместо подформул вида

$(\neg C)$ будем писать $\neg C$. Дальнейшая экономия скобок возможна, если принять соглашение о том, какие логические операции «сильнее» в том смысле, в каком, например, в школьной алгебре операция умножения «сильнее» операции сложения. Для этого расположим логические символы в следующем порядке: $\neg, \&, \vee, \supset, \equiv$, и будем считать, что из всех возможных в первую очередь выполняется та операция, которая в этом списке стоит левее, а из нескольких одинаковых операций выполняется та, которая встречается в выражении раньше. Например, формулу

$$(((P_1 \supset P_2) \,\&\, (P_3 \supset P_4)) \supset ((\neg P_2) \vee P_4))$$

можно сокращенно записать так:

$$(P_1 \supset P_2) \,\&\, (P_3 \supset P_4) \supset \neg P_2 \vee P_4.$$

Если A — пропозициональная формула, не содержащая переменных, отличных от $P_1, \ldots, P_n$, будем обозначать ее $A(P_1, \ldots, P_n)$. Пусть $B_1, \ldots, B_n$ — произвольные формулы. Посредством $A(B_1, \ldots, B_n)$ будем обозначать результат одновременной замены в A всех вхождений переменных $P_1, \ldots, P_n$ на формулы $B_1, \ldots, B_n$ соответственно. Будем говорить, что формула $A(B_1, \ldots, B_n)$ получается *подстановкой* в A формул $B_1, \ldots, B_n$ вместо переменных $P_1, \ldots, P_n$ соответственно.

Истинностные таблицы. Пусть $V = \{P_1, P_2, \ldots\}$ — множество всех пропозициональных переменных. *Оценкой* называется произвольное отображение $g : V \to \{0, 1\}$. Индукцией по построению формулы A определим *значение* $g(A)$ формулы A при оценке g. Для любого атома A значение $g(A)$ задано оценкой g. Положим $g(\neg A) = \neg(g(A))$, $g(A \lambda B) = g(A) \lambda g(B)$, где λ — любой из логических символов $\&, \vee, \supset$, а значения правой части равенств вычисляется в соответствии с приведенными выше таблицами для каждой логической операции.

Нетрудно доказать, что значение формулы A при оценке g зависит только от значений оценки g на переменных, входящих в A. Таким образом, для определения значения формулы A при данной оценке достаточно знать лишь значения этой оценки на переменных, входящих в A. Это позволяет представлять зависимость значения формулы от оценки в виде так называемой истинностной таблицы.

Пусть $Q_1, \ldots, Q_n$ — некоторый список переменных, включающий все переменные, входящие в формулу A. *Истинностной таблицей* формулы A над списком $Q_1, \ldots, Q_n$ называется таблица следующего вида:

Q_1	$\ldots$	Q_n	A
$\ldots$	$\ldots$	$\ldots$	$\ldots$
α_1	$\ldots$	α_n	α
$\ldots$	$\ldots$	$\ldots$	$\ldots$

Кроме заголовка эта таблица содержит 2^n строк, в которых выписаны все различные наборы нулей и единиц $\alpha_1 \ldots \alpha_n$ и значения $\alpha \in \{0, 1\}$ формулы A при оценке, сопоставляющей переменным $Q_1, \ldots, Q_n$ соответственно значения $\alpha_1, \ldots, \alpha_n$.

Общезначимые пропозициональные формулы. *Тавтология* (*общезначимая формула, тождественно истинная формула*) — это пропозициональная формула, значение которой при любой оценке равно 1. Истинностная таблица тавтологии обладает тем свойством, что в ее последнем столбце во всех строках стоит 1. Каждая тавтология является схемой истинных высказываний и в этом смысле выражает некоторый *логический закон*. Вот некоторые логические законы: $P \vee \neg P$ (закон исключенного третьего); $\neg\neg P \equiv P$ (закон двойного отрицания); $(P \supset Q) \equiv (\neg Q \supset \neg P)$ (закон контрапозиции).

Множество всех тавтологий разрешимо в том смысле, что существует алгоритм, позволяющий по произвольной пропозициональной формуле узнать, является ли она тавтологией: алгоритм проверки пропозициональных формул на предмет обладания свойством быть тавтологией состоит в построении истинностной таблицы формулы и изучении столбца ее значений.

Выполнимость и логическое следование. Множество пропозициональных формул Γ называется *выполнимым*, если существует оценка, при которой все формулы из Γ принимают значение 1. Невыполнимое множество формул называется *несовместным*.

Говорят, что пропозициональная формула F *логически следует* из множества пропозициональных формул Γ, и пишут $\Gamma \models F$, если $g(F) = 1$ для любой оценки g, при которой все формулы из Γ принимают значение 1. Если $\Gamma = \{F_1, \ldots, F_n\}$, то вместо $\Gamma \models F$ пишут $F_1, \ldots, F_n \models F$.

Теорема 2. *Каковы бы ни были формулы $F_1, \ldots, F_n, F$, имеет место*

$$F_1, \ldots, F_n \models F \tag{3.1}$$

тогда и только тогда, когда формула

$$F_1 \,\&\, \ldots \,\&\, F_n \supset F \tag{3.2}$$

является тавтологией.

Доказательство. Пусть имеет место (3.1), и g — произвольная оценка. Если при этой оценке хотя бы одна из формул $F_1, \ldots, F_n$ принимает значение 0, то формула (3.2) принимает значение 1. Если же все формулы $F_1, \ldots, F_n$ принимают значение 1, то $g(F) = 1$ в силу (3.1), и формула (3.2) принимает значение 1. Таким образом, при любой оценке формула (3.2) принимает значение 1, т. е. является тавтологией.

Пусть формула (3.2) является тавтологией, и пусть g — такая оценка, при которой все формулы $F_1, \ldots, F_n$ принимают значение 1. Так как при этой оценке формула (3.2) принимает значение 1, то необходимо $g(F) = 1$. Таким образом, $g(F) = 1$ для любой оценки g, при которой все формулы $F_1, \ldots, F_n$ принимают значение 1, т. е. имеет место (3.1). $\square$

Теорема 3. *Каковы бы ни были множество пропозициональных формул Γ и формула F, имеет место $\Gamma \models F$ тогда и только тогда, когда множество $\Gamma \cup \{\neg F\}$ несовместно.*

Доказательство. Пусть $\Gamma \models F$. Если множество $\Gamma \cup \{\neg F\}$ выполнимо, то при некоторой оценке g все формулы из Γ принимают значение 1 и $g(\neg F) = 1$, т. е. $g(F) = 0$, что невозможно. Значит, множество $\Gamma \cup \{\neg F\}$ несовместно.

Пусть множество $\Gamma \cup \{\neg F\}$ несовместно. Докажем $\Gamma \models F$. Пусть g — такая оценка, при которой все формулы из Γ принимают значение 1. Тогда $g(F) = 1$, ибо в противном случае $g(\neg F) = 1$, и множество $\Gamma \cup \{\neg F\}$ выполнимо. Значит, $g(F) = 1$ для любой оценки g, при которой все формулы из Γ принимают значение 1, т. е. $\Gamma \models F$. $\square$

§3.3. Классическое исчисление высказываний

Путем построения истинностной таблицы для пропозициональной формулы можно проверить, является ли эта формула общезначимой. Однако представляет интерес и другой способ описания общезначимых формул — с помощью исчисления. Более того, при рассмотрении неклассических логических систем описание их с помощью исчислений в ряде случаев представляется наиболее естественным и единственно возможным.

Общее понятие исчисления. Пусть Σ — некоторый алфавит, т. е. список символов, называемых буквами. Конечная последовательность букв этого алфавита называется словом в алфавите Σ. *Исчисление* в алфавите Σ задается путем указания *аксиом* — некоторых выделенных слов в алфавите Σ — и *правил вывода*, позволяющих из одного или нескольких слов в алфавите Σ получать новые слова в алфавите Σ. *Вывод* в данном исчислении — это конечная последовательность слов $w_1, \dots, w_n$ в алфавите Σ такая, что для каждого $i = 1, \dots, n$ слово w_i либо является аксиомой, либо получается из каких-нибудь предшествующих слов этой последовательности по одному из правил вывода. Говорят, что слово w в алфавите Σ *выводимо* в данном исчислении, если существует вывод, оканчивающийся словом w.

Вывод из множества слов Γ (так называемого множества *гипотез*) в данном исчислении — это конечная последовательность слов $w_1, \dots, w_n$ в алфавите Σ такая, что для каждого $i = 1, \dots, n$ слово w_i либо является аксиомой, либо является гипотезой (т. е. принадлежит множеству Γ), либо получается из каких-нибудь предшествующих слов этой последовательности по одному из правил вывода. Говорят, что слово w в алфавите Σ *выводимо из множества* Γ в данном исчислении, если существует вывод из Γ, оканчивающийся словом w.

В дальнейшем мы будем рассматривать так называемые *пропозициональные исчисления*. Это исчисления в алфавите логики высказываний, аксиомы которых суть пропозициональные формулы, а правила вывода позволяют из формул получать только формулы. Таким образом, в пропозициональном исчислении могут выводиться только пропозициональные формулы.

Аксиомы классического исчисления высказываний. Аксиомами *классического исчисления высказываний* будем называть пропозициональные формулы любого из следующих видов, где A, B, C — произвольные формулы:

1. $A \supset (B \supset A)$;
2. $(A \supset B) \supset ((A \supset (B \supset C)) \supset (A \supset C))$;
3. $A \,\&\, B \supset A$;
4. $A \,\&\, B \supset B$;
5. $A \supset (B \supset A \,\&\, B)$;
6. $A \supset A \vee B$;
7. $B \supset A \vee B$;
8. $(A \supset C) \supset ((B \supset C) \supset (A \vee B \supset C))$;
9. $(A \supset B) \supset ((A \supset \neg B) \supset \neg A)$;
10. $\neg\neg A \supset A$.

Выражения 1 – 10 называются *схемами аксиом* классического исчисления высказываний. Единственным правилом вывода классического исчисления высказываний является правило *модус поненс* (modus ponens; сокращенно: MP):

$$\frac{A \quad A \supset B}{B}.$$

Это правило позволяет из формул A и $A \supset B$ получить формулу B. Будем говорить, что формула B является *непосредственным следствием* формул A и $A \supset B$.

Выводом в исчислении высказываний считается такая конечная последовательность формул $A_1, \ldots, A_n$, в которой каждая формула является либо аксиомой, либо непосредственным следствием каких-нибудь двух предшествующих формул. Формула A выводима в исчислении высказываний, если существует вывод, оканчивающийся формулой A; в этом случае будем писать $\vdash A$.

Теорема 4. *Какова бы ни была формула A, формула $A \supset A$ выводима в классическом исчислении высказываний.*

Доказательство. Выводом формулы $A \supset A$ является следующая последовательность формул:

1. $(A \supset (A \supset A)) \supset ((A \supset ((A \supset A) \supset A)) \supset (A \supset A))$ (аксиома 2);
2. $A \supset (A \supset A)$ (аксиома 1);
3. $(A \supset ((A \supset A) \supset A)) \supset (A \supset A)$ (получена по правилу MP из формул 1 и 2);
4. $A \supset ((A \supset A) \supset A)$ (аксиома 1);
5. $A \supset A$ (получено по правилу MP из формул 3 и 4). □

Предложение 3. *Если пропозициональное исчисление содержит схемы аксиом 1, 2 и правило MP, то, какова бы ни была формула A, в этом исчислении выводима формула $A \supset A$.*

Доказательство. Построенный при доказательстве теоремы 4 вывод формулы $A \supset A$ в классическом исчислении высказываний будет выводом в любом пропозициональном исчислении, которое содержит схемы аксиом 1, 2 и правило MP. □

Имеет место следующее *правило подстановки*:

Предложение 4. *Если выводима формула $A(P_1, \ldots, P_n)$, то выводима формула $A(B_1, \ldots, B_n)$, каковы бы ни были формулы $B_1, \ldots, B_n$.*

Доказательство. Пусть $A_1, \ldots, A_k$ — вывод формулы $A(P_1, \ldots, P_n)$. Во все формулы из этого вывода подставим формулы $B_1, \ldots, B_n$ вместо переменных $P_1, \ldots, P_n$. Очевидно, что при этом каждая аксиома преобразуется в аксиому же, а непосредственное следствие исходных формул — в непосредственное следствие соответствующих преобразованных формул. Таким образом мы получим вывод формулы $A(B_1, \ldots, B_n)$. □

Пусть Γ — некоторое множество формул (будем называть их гипотезами). Выводом из Γ называется конечная последовательность формул $A_1, \ldots, A_n$, в которой каждая формула либо является аксиомой, либо принадлежит множеству Γ, либо является непосредственным следствием двух предшествующих формул. Говорят, что формула A выводима из Γ и пишут $\Gamma \vdash A$, если существует вывод из Γ, оканчивающийся формулой A. Всякий вывод в исчислении высказываний является выводом из пустого множества гипотез, поэтому $\vdash A$ означает то же, что и $\emptyset \vdash A$.

Отметим некоторые очевидные свойства отношения выводимости $\vdash$ (см. упражнение 1):

монотонность: если $\Gamma \vdash A$ и $\Gamma \subseteq \Delta$, то $\Delta \vdash A$;

транзитивность: если $\Gamma \vdash A$, и $\Delta \vdash B$ для любой формулы $B \in \Gamma$, то $\Delta \vdash A$;

компактность: если $\Gamma \vdash A$, то существует конечное множество $\Delta \subseteq \Gamma$ такое, что $\Delta \vdash A$.

Теорема о дедукции. Следующая теорема называется *теоремой о дедукции.*

Теорема 5. *Каковы бы ни были множество формул* Γ *и формулы* A, B*, имеет место* $\Gamma \cup \{A\} \vdash B \Rightarrow \Gamma \vdash A \supset B$.

Доказательство. Пусть $A_1, \ldots, A_n$ — вывод B из $\Gamma \cup \{A\}$. Индукцией по i докажем, что $\Gamma \vdash A \supset A_i$ для $i = 1, \ldots, n$. Если $i = 1$, то A_i — либо аксиома, либо гипотеза из Γ, либо формула A. Если A_i — аксиома или гипотеза из Γ, то следующая последовательность является выводом $A \supset A_i$ из Γ:

1. $A_i \supset (A \supset A_i)$ (аксиома 1);
2. A_i (аксиома или гипотеза);
3. $A \supset A_i$ (получено по правилу MP из 1 и 2).

Если же A_i совпадает с A, то построенный выше вывод $A \supset A$ является выводом $A \supset A_i$ из Γ. Допустим, что для некоторого $k \leq n$ формулы $A \supset A_i$ $(i = 1, \ldots, k-1)$ выводимы из Γ. Докажем, что формула $A \supset A_k$ выводима из Γ. Если A_k — аксиома или гипотеза из $\Gamma \cup \{A\}$, утверждение доказывается, как в случае $i = 1$. Пусть A_k — непосредственное следствие формулы A_i и формулы A_j (вида $A_i \supset A_k$), где $i, j < k$. По индуктивному предположению,

$$\Gamma \vdash A \supset A_i, \qquad \Gamma \vdash A \supset (A_i \supset A_k). \tag{3.3}$$

Следующая последовательность является выводом $A \supset A_k$ из множества $\{A \supset A_i, A \supset (A_i \supset A_k)\}$:

1. $(A \supset A_i) \supset ((A \supset (A_i \supset A_k)) \supset (A \supset A_k))$ (аксиома 2);
2. $A \supset A_i$ (гипотеза);
3. $(A \supset (A_i \supset A_k)) \supset (A \supset A_k)$ (получено по MP из 1 и 2);
4. $A \supset (A_i \supset A_k)$ (гипотеза):
5. $A \supset A_k$ (получено по правилу MP из 3 и 4).

Таким образом, $\{A \supset A_i, A \supset (A_i \supset A_k)\} \vdash A \supset A_k$. Отсюда и из (3.3) в силу транзитивности вытекает $\Gamma \vdash A \supset A_k$, что и требовалось. Так как A_n есть B, то $\Gamma \vdash A \supset B$. □

Предложение 5. *Если исчисление содержит схемы аксиом 1 и 2, и MP — единственное правило вывода, то для этого исчисления верна теорема о дедукции.*

Доказательство. Если пропозициональное исчисление содержит схемы аксиом 1 и 2 и единственным правилом вывода является MP, то для этого исчисления остается в силе доказательство теоремы 5. □

Множество формул Γ называется *противоречивым*, если существует такая формула B, что $\Gamma \vdash B$ и $\Gamma \vdash \neg B$. В противном случае Γ называется *непротиворечивым.* Если множество Γ противоречиво, то любое его расширение также противоречиво, а любое подмножество непротиворечивого множества непротиворечиво.

Теорема 6 (принцип приведения к абсурду)**.** *Если* $\Gamma \cup \{A\}$ *— противоречивое множество формул, то* $\Gamma \vdash \neg A$.

Доказательство. Пусть $\Gamma \cup \{A\} \vdash B$ и $\Gamma \cup \{A\} \vdash \neg B$. Тогда по теореме 5

$$\Gamma \vdash A \supset B; \qquad \Gamma \vdash A \supset \neg B. \tag{3.4}$$

С помощью аксиомы 9 легко доказать $\{A \supset B, A \supset \neg B\} \vdash \neg A$. Отсюда и из (3.4) в силу транзитивности выводимости вытекает $\Gamma \vdash \neg A$, что и требовалось. □

Предложение 6. *Если исчисление содержит схему аксиом 9 и для этого исчисления верна теорема о дедукции, то для этого исчисления верен принцип приведения к абсурду.*

Доказательство. Если пропозициональное исчисление содержит схему аксиом 9 и для этого исчисления верна теорема о дедукции, то для этого исчисления остается в силе доказательство теоремы 6. $\square$

Производные правила вывода. Теорема о дедукции и принцип приведения к абсурду суть примеры так называемых *производных правил вывода*

$$\frac{\Gamma_1 \vdash A_1 \quad \dots \quad \Gamma_n \vdash A_n}{\Delta \vdash B},$$

утверждающих, что если $\Gamma_1 \vdash A_1, \dots, \Gamma_n \vdash A_n$, то $\Delta \vdash B$. Вот еще одно полезное производное правило вывода — *правило силлогизма*:

$$\frac{\Gamma \vdash A \supset B \quad \Gamma \vdash B \supset C}{\Gamma \vdash A \supset C}.$$

Оно легко обосновывается с помощью теоремы о дедукции.

Теорема 7. *Имеют место следующие производные правила вывода:*

введение конъюнкции $\dfrac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash A \,\&\, B}$ $(\to \&)$*;*

удаление конъюнкции $\dfrac{\Gamma \vdash A \,\&\, B}{\Gamma \vdash A}$, $\dfrac{\Gamma \vdash A \,\&\, B}{\Gamma \vdash B}$ $(\& \to)$*;*

введение дизъюнкции $\dfrac{\Gamma \vdash A}{\Gamma \vdash A \vee B}$, $\dfrac{\Gamma \vdash B}{\Gamma \vdash A \vee B}$ $(\to \vee)$*;*

удаление дизъюнкции $\dfrac{\Gamma, A \vdash C \quad \Gamma, B \vdash C}{\Gamma, A \vee B \vdash C}$ $(\vee \to)$*;*

введение импликации $\dfrac{\Gamma, A \vdash B}{\Gamma \vdash A \supset B}$ $(\to\supset)$*;*

удаление импликации $\dfrac{\Gamma \vdash A \quad \Gamma \vdash A \supset B}{\Gamma \vdash B}$ $(\supset\to)$*;*

введение отрицания $\dfrac{\Gamma, A \vdash B \quad \Gamma, A \vdash \neg B}{\Gamma \vdash \neg A}$ $(\to \neg)$*;*

удаление отрицания $\dfrac{\Gamma, \neg A \vdash B \quad \Gamma, \neg A \vdash \neg B}{\Gamma \vdash A}$ $(\neg \to)$.

Доказательство. Правило $(\to \&)$ обосновывается с помощью аксиомы 5, правила $(\& \to)$ — с помощью аксиом 3 и 4. Правила $(\to \vee)$ обосновываются с помощью аксиом 6 и 7. Правило $(\vee \to)$ называется *правилом доказательства разбором случаев* и обосновываются с помощью аксиомы 8. Правило $(\to\supset)$ — это теорема о дедукции. Правило $(\supset\to)$ по существу есть правило MP. Правило $(\to \neg)$ — это принцип приведения к абсурду. Правило $(\neg \to)$ называется *правилом доказательства от противного* и обосновывается с помощью правила $(\to \neg)$ и аксиомы 10. $\square$

Теорема 8. *Множество пропозициональных формул* Γ *противоречиво тогда и только тогда, когда любая формула выводима из* Γ.

Доказательство. Пусть множество пропозициональных формул Γ противоречиво, и пусть A — произвольная формула. Очевидно, что множество $\Gamma \cup \{\neg A\}$ противоречиво. Тогда в силу правила $(\neg \to)$ имеет место $\Gamma \vdash A$. Обратно, пусть любая формула выводима из Γ. В частности, какова бы ни была формула A, имеет место $\Gamma \vdash A$ и $\Gamma \vdash \neg A$, а это означает, что множество Γ противоречиво. $\square$

Корректность классического исчисления высказываний. Важность рассмотрения и изучения классического исчисления высказываний обусловлена следующей теоремой.

Теорема 9 (теорема о корректности)**.** *Какова бы ни была формула* A*, если* $\vdash A$*, то* A *является тавтологией.*

Доказательство. Каждая аксиома классического исчисления высказываний является тавтологией (см. упражнение 2). Очевидно, что если формулы A и $A \supset B$ — тавтологии, то и B является тавтологией. Поэтому, если дан вывод $A_1, \ldots, A_n$ формулы A в классическом исчислении высказываний, то индукцией по i нетрудно доказать, что каждая формула A_i в этом выводе является тавтологией, в частности, A — последняя формула в этом выводе. $\square$

Таким образом, построение вывода формулы в классическом исчислении высказываний является одним из способов доказательства того факта, что эта формула является тавтологией.

Теорема 10 (обобщенная теорема о корректности)**.** *Каковы бы ни были множество формул* Γ *и формула* A*, если* $\Gamma \vdash A$*, то* $\Gamma \models A$.

Доказательство. Пусть $\Gamma \vdash A$. В силу свойства компактности отношения выводимости существует конечное множество $\Delta \subseteq \Gamma$ такое, что $\Delta \vdash A$. Пусть $\Delta = \{A_1, \ldots, A_n\}$. Применяя n раз теорему о дедукции, получаем $\vdash A_1 \supset (\cdots \supset (A_n \supset A) \ldots)$. В силу теоремы 9 формула

$$A_1 \supset (\cdots \supset (A_n \supset A) \ldots) \tag{3.5}$$

является тавтологией. Докажем, что $\Gamma \models A$. Пусть g — такая оценка, при которой все формулы из Γ принимают значение 1. В частности, $g(A_i) = 1$ $(i = 1, \ldots, n)$. Так как формула (3.5) является тавтологией, то она принимает значение 1 при оценке g. Отсюда и из истинностной таблицы для импликации получаем $g(A) = 1$, что и требовалось доказать. □

Теорема 11. *Всякое выполнимое множество формул непротиворечиво.*

Доказательство. Пусть множество формул Γ выполнимо. Это означает, что существует оценка f, при которой все формулы из Γ принимают значение 1. Допустим, что множество Γ противоречиво, т. е. $\Gamma \vdash B$ и $\Gamma \vdash \neg B$ для некоторой формулы B. Тогда в силу обобщенной теоремы о корректности $\Gamma \models B$ и $\Gamma \models \neg B$. Следовательно, $f(B) = 1$ и $f(\neg B) = 1$, что невозможно. Полученное противоречие показывает, что на самом деле множество Γ непротиворечиво. □

Полнота классического исчисления высказываний. Меожество пропозициональных формул Γ называется *максимальным непротиворечивым* множеством, если Γ непротиворечиво, но всякое собственное расширение $\Delta \supset \Gamma$ противоречиво. Нетрудно доказать, что всякое максимальное непротиворечивое множество Γ обладает следующими свойствами:

Γ замкнуто относительно выводимости: $\Gamma \vdash A \Rightarrow A \in \Gamma$;

Γ полно в том смысле, что для любой формулы A имеет место $A \in \Gamma$ или $(\neg A) \in \Gamma$.

Всякое непротиворечивое множество Γ можно расширить до максимального непротиворечивого множеств. Это делается следующим образом. Множество всех формул счетно. Пусть $A_0, A_1, \ldots$ — пересчет всех формул. Индукцией по n определяется множество Δ_n: $\Delta_0 = \Gamma$;

$$\Delta_{i+1} = \begin{cases} \Delta_i \cup \{A_i\}, & \text{если } \Delta_i \cup \{A_i\} \text{ непротиворечиво;} \\ \Delta_i & \text{в противном случае.} \end{cases}$$

Положим $\Delta = \bigcup\limits_{i=1}^{\infty} \Delta_i$. Нетрудно доказать, что Δ — максимальное непротиворечивое расширение множества Γ.

Любое максимальное непротиворечивое множество Δ выполнимо: если оценка g определена так, что $g(P_i) = 1 \Leftrightarrow P_i \in \Delta$, то индукцией по построению нетрудно доказать, что для любой формулы A выполняется условие $g(A) = 1 \Leftrightarrow A \in \Delta$.

Теорема 12. *Всякое непротиворечивое множество пропозициональных формул выполнимо.*

Доказательство. Пусть Γ — непротиворечивое множество формул. Его можно расширить до максимального непротиворечивого множества формул Δ, которое выполнимо, т. е. существует оценка g, при которой все формулы из Δ принимают значение 1. В частности, при этой оценке g все формулы из Γ принимают значение 1, т. е. множество Γ выполнимо. □

Теорема 13 (обобщенная теорема о полноте)**.** *Каковы бы ни были множество формул* Γ *и формула* A,

$$\Gamma \models A \Rightarrow \Gamma \vdash A.$$

Доказательство. Пусть $\Gamma \models A$. Тогда по теореме 3 множество $\Gamma \cup \{\neg A\}$ несовместно. Отсюда и из теоремы 12 следует, что оно противоречиво. Но тогда по правилу $(\neg \rightarrow)$ $\Gamma \vdash A$. □

Теорема 14 (теорема о полноте)**.** *Всякая тавтология выводима в классическом исчислении высказываний.*

Доказательство. Пусть A — тавтология. Тогда множество $\{\neg A\}$ невыполнимо. По теореме 12 оно противоречиво. Но тогда $\vdash A$ по правилу $(\neg \rightarrow)$, что и требовалось доказать. □

§3.4. Элементарные языки и алгебраические системы

Переменная — это выражение, служащее для обозначения произвольного объекта из фиксированного множества, называемого *областью возможных значений* этой переменной. Область определения переменной v будем обозначать $D(v)$. Если переменная v употребляется так, что допускается подстановка вместо нее *имен* (т. е. обозначений) объектов из $D(v)$, то эта переменная называется *свободной*. Если же по смыслу выражения, содержащего переменную, подстановка вместо нее имен объектов недопустима, то эта переменная называется *связанной*. В одном выражении одна и та же переменная может употребляться одновременно как свободная и как связанная, так что следует говорить о свободных и связанных *вхождениях* переменной.

Выражение, содержащее свободные вхождения переменных и превращающееся в имя некоторого объекта или высказывание при подстановке вместо свободных вхождений каждой переменной v имени какого-либо объекта из $D(v)$, называется *именной формой* или, соответственно, *высказывательной формой*. Переменные, имеющие свободные вхождения в именную или высказывательную форму, называются ее *параметрами*. Именную или высказывательную форму называют n-местной, если она содержит ровно n параметров. В частности, можно говорить и о 0-местных именных и высказывательных формах, понимая под ними соответственно имена и высказывания.

Для k-местной именной или высказывательной формы с параметрами $x_1, \ldots, x_k$ употребляют обозначение $F(x_1, \ldots, x_k)$. Тогда, если $a_1, \ldots, a_k$ — имена объектов из $D(x_1), \ldots, D(x_k)$ соответственно, то через $F(a_1, \ldots, a_k)$ обозначается выражение, полученное из $F(x_1, \ldots, x_k)$ подстановкой $a_1, \ldots, a_k$ соответственно вместо свободных вхождений $x_1, \ldots, x_k$.

Над высказывательными формами можно совершать логические операции. Абсолютно ясен смысл высказывательных форм $\neg A$, $A \,\&\, B$, $A \vee B$, $A \supset B$, если A и B — высказывательные формы. Наряду с этими операциями в математической логике рассматриваются *кванторы*, позволяющие из данной высказывательной формы получать высказывательную форму с меньшим числом параметров, в частности, из одноместной высказывательной формы — высказывание. *Квантор всеобщности* позволяет из высказывательной формы $A(x)$ с единственным параметром x получить высказывание «Для всех x верно, что $A(x)$», обозначаемое $\forall x\, A(x)$. Высказывание $\forall x\, A(x)$ считается истинным тогда и только тогда, когда $A(a)$ истинно для любого $a \in D(x)$. *Квантор существования* позволяет из высказывательной формы $A(x)$ с единственным параметром x получить высказывание «Существует такой x, что $A(x)$», обозначаемое $\exists x\, A(x)$. Высказывание $\exists x\, A(x)$ считается истинным тогда и только тогда, когда найдется такой объект $a \in D(x)$, что истинно $A(a)$. Кванторы $\forall x$ и $\exists x$ можно применять и к высказывательным формам вида $A(x, y, \dots)$, содержащим наряду с x параметры $y, \dots$, в результате чего получается высказывательная форма с параметрами $y, \dots$.

В грамматике используются понятия субъекта и предиката. *Субъект* — это то, о чем говорится в предложении, а *предикат* выражает то, что говорится о субъекте. В математической логике используется более широкая трактовка субъектно-предикатной структуры предложения. Прежде всего, в качестве субъектов данного предложения мы можем выделить одно или несколько имен каких-либо предметов, входящих в это предложение. Заменив затем выделенные имена на переменные, мы получим высказывательную форму, «в чистом виде» выражающую то, что говорится о субъекте или субъектах. Эту высказывательную форму тоже называют предикатом.

Со всякой высказывательной формой $A(x_1, \dots, x_n)$ связана функция, которая значениям $a_1, \dots, a_n$ параметров $x_1, \dots, x_n$ сопоставляет высказывание $A(a_1, \dots, a_n)$. Так мы приходим к представлению о предикате как о функции, значениями которой являются высказывания. Наконец, если не различать высказывания, имеющие одно и то же истинностное значение, то получаем следующее определение предиката: *k-местным предикатом* на множестве M называется произвольная функция $P : M^k \to \{0, 1\}$.

Чтобы сделать математические утверждения точными математическими объектами, в математической логике используются искусственные языки. Мы будем рассматривать *элементарные языки*. Элементарный язык задается *сигнатурой* — набором $\Omega = \langle Cn, Fn, Pr \rangle$, где Cn — множество *констант*, Fn — множество *функциональных символов*, Pr — множество *предикатных символов*. При этом с каждым функциональным и предикатным символом связано натуральное число — количество аргументов (или *валентность*) этого символа. Валентность любого функционального символа положительна, а предикатный символ может иметь и нулевую валентность. Функциональный или предикатный символ валентности k называют k-местным. Во всяком элементарном языке имеется счетный набор *переменных* $x_0, x_1, x_2, \ldots$. Элементарный язык с сигнатурой Ω будем называть языком Ω.

Из переменных, констант, функциональных и предикатных символов с помощью скобок (,), запятых и *логических символов* $\neg$, $\&$, $\vee$, $\supset$, $\forall$, $\exists$ строятся термы и формулы. Определение *терма* носит индуктивный характер:

1) каждая переменная есть терм;

2) каждая константа есть терм;

3) если f есть k-местный функциональный символ, а $t_1, \ldots, t_k$ — термы, то выражение $f(t_1, \ldots, t_k)$ есть терм.

Атомные формулы (или *атомы*) — это выражения вида $P(t_1, \ldots, t_k)$, где P есть k-местный предикатный символ ($k \geq 1$), а $t_1, \ldots, t_k$ — термы. *Формулы* определяются индуктивно:

1) каждый атом есть формула;

2) если Φ — формула, то $\neg\Phi$ — формула;

3) если Φ и Ψ — формулы, то $(\Phi \,\&\, \Psi)$, $(\Phi \vee \Psi)$, $(\Phi \supset \Psi)$ — формулы;

4) если Φ — формула, x — переменная, то $\forall x\, \Phi$ и $\exists x\, \Phi$ — формулы.

Символы $\neg, \&, \vee, \supset$ называются *логическими связками*, а $\exists$ и $\forall$ — *кванторами*. В формулах вида $\exists x\, \Phi$ и $\forall x\, \Phi$ выражение $\forall x$ или $\exists x$ называется *кванторной приставкой*, а формула Φ — *областью действия* соответствующей кванторной приставки. Выражение $\Phi \equiv \Psi$ будет использоваться как сокращенное обозначение формулы $(\Phi \supset \Psi) \,\&\, (\Psi \supset \Phi)$. *Логической длиной* формулы назовем общее количество входящих в нее логических связок и кванторов.

Вхождение переменной x в формулу Φ называется *связанным*, если оно входит в кванторную приставку $\forall x$ или $\exists x$ или в область действия такой кванторной приставки. Вхождение переменной, не являющееся связанным, называется *свободным*. Если переменная v имеет свободные вхождения в формулу Φ, будем говорить, что v — *параметр* формулы Φ. Формула, не имеющая параметров, называется *замкнутой формулой* или *высказыванием*. Пусть $v_1, \ldots, v_n$ — все параметры формулы Φ. В этом случае высказывание $\forall v_1 \ldots \forall v_n\, \Phi$ будем называть *универсальным замыканием* формулы Φ.

Индуктивное определение формулы дает возможность использовать в доказательствах принцип индукции по построению формулы.

Пусть даны различные переменные $x_1, \ldots, x_k$ и (не обязательно различные) термы $t_1, \ldots, t_k$. Через $\Phi[t_1/x_1, \ldots, t_n/x_n]$ будем обозначать результат одновременной подстановки в формулу Φ термов $t_1, \ldots, t_k$ вместо свободных вхождений переменных $x_1, \ldots, x_k$ соответственно. Нетрудно заметить, что если Φ не содержит свободных вхождений переменных $x_1, \ldots, x_k$ (в частности, если она замкнута), то $\Phi[t_1/x_1, \ldots, t_n/x_n]$ совпадает с Φ.

Имея в виду дальнейшую подстановку термов $t_1, \ldots, t_k$ вместо $x_1, \ldots, x_k$ в формулу Φ, иногда для этой формулы употребляют обозначение $\Phi(x_1, \ldots, x_k)$, а для $\Phi[t_1/x_1, \ldots, t_n/x_n]$ — обозначение $\Phi(t_1, \ldots, t_k)$.

Обычно при записи формул опускают внешние скобки. Дальнейшая экономия скобок возможна, если принять соглашение о том, какие логические операции «сильнее». Для этого расположим логические символы в следующем порядке: $\forall, \exists, \neg, \&, \vee, \supset$ и будем считать, что из всех возможных в первую очередь выполняется та операция, которая в этом списке стоит раньше. Например, формулу

$$\forall x\, ((\neg P(x)) \supset (\exists y\, Q(x, y) \vee (R(x) \,\&\, P(y))))$$

можно сокращенно записать так:

$$\forall x\, (\neg P(x) \supset \exists y\, Q(x, y) \vee R(x) \,\&\, P(y)),$$

а выражение

$$\forall x\, \neg P(x) \supset \exists y\, Q(x, y) \vee R(x) \,\&\, P(y))$$

является сокращенной записью формулы

$$(\forall x\,(\neg P(x)) \supset (\exists y\,Q(x,y) \vee (R(x)\,\&\,P(y)))).$$

При построении логико-математического языка обычно подразумевается некоторый смысл составляющих его символов, однако мы вправе рассматривать и другие интерпретации этого языка. Чтобы задать *интерпретацию* языка $\Omega = \langle Cn, Fn, Pr\rangle$, нужно

1) зафиксировать непустое множество M — *основное множеством* или *носитель интерпретации*;

2) каждой константе $c \in Cn$ сопоставить некоторый элемент $\bar{c} \in M$ — значение константы c в данной интерпретации;

3) каждому (k-местному) функциональному символу $f \in Fn$ сопоставить некоторую (k-местную) функцию $\bar{f} : M^k \to M$ — значение функционального символа f в данной интерпретации;

4) каждому (k-местному) предикатному символу $P \in Pr$ сопоставить некоторый (k-местный) предикат $\bar{P} : M^k \to \{0,1\}$ — значение предикатного символа P в данной интерпретации. Если P есть 0-местный предикатный символ, то ему сопоставляется значение 0 или 1.

Непустое множество M, рассматриваемое вместе с интерпретацией на нем всех символов сигнатуры Ω, называется *алгебраической системой сигнатуры* Ω и обозначается $\langle M, \Omega\rangle$. Множество M называют носителем алгебраической системы $\langle M, \Omega\rangle$. *Мощностью* алгебраической системы называется мощность ее носителя.

§3.5. Классическая логика предикатов

Пусть фиксирована алгебраическая система $\mathfrak{M} = \langle M, \Omega\rangle$. Наряду с сигнатурой $\Omega = \langle Cn, Fn, Pr\rangle$ рассмотрим сигнатуру Ω', полученную добавлением к множеству Cn имен всех элементов множества M. Индукцией по построению терма t сигнатуры Ω', не содержащего переменных, определим значение $[t] \in M$ терма t в $\mathfrak{M}$:

1) если t — константа $c \in Cn$, то $[t] \rightleftharpoons \bar{c}$;
2) если t — константа $m \in M$, то $[t] \rightleftharpoons m$;
3) если t имеет вид $f(t_1, \ldots, t_n)$, то $[t] \rightleftharpoons \bar{f}([t_1], \ldots, [t_n])$.

Индукцией по логической длине высказывания Φ сигнатуры Ω' определяется его *истинностное значение* $[\Phi] \in \{0,1\}$ в $\mathfrak{M}$. Если Φ — атом $P(t_1,\ldots,t_n)$, то $[\Phi] \rightleftharpoons \bar{P}([t_1],\ldots,[t_n])$. Если Φ имеет вид $\neg\Psi$ или $(\Psi_1\lambda\Psi_2)$, где $\lambda \in \{\&,\vee,\supset\}$, то $[\Phi]$ определяется в соответствии с истинностной таблицей для $\neg$ и λ. Если Φ имеет вид $\exists x\,\Psi(x)$, то для любого $m \in M$ определено значение $[\Psi(m)]$ высказывания $\Psi(m)$. Тогда

$$[\Phi] = 1 \leftrightharpoons (\exists m \in M)\,[\Psi(m)] = 1.$$

Аналогично, если Φ имеет вид $\forall x\,\Psi$, то

$$[\Phi] = 1 \leftrightharpoons (\forall m \in M)\,[\Psi(m)] = 1.$$

Поскольку любое высказывание Φ языка Ω является высказыванием языка Ω', то определено его истинностное значение в $\mathfrak{M}$. Будем говорить, что высказывание Φ *истинно* в $\mathfrak{M}$ и писать $\mathfrak{M} \models \Phi$, если $[\Phi] = 1$. В противном случае будем говорить, что Φ *ложно* в $\mathfrak{M}$ и писать $\mathfrak{M} \not\models \Phi$.

Высказывание Φ называется *выполнимым*, если существует такая алгебраическая система $\mathfrak{M}$, что $\mathfrak{M} \models \Phi$; в этом случае $\mathfrak{M}$ называется *моделью* высказывания Φ. Множество высказываний Γ называется выполнимым, если существует такая алгебраическая система $\mathfrak{M}$, что $(\forall\Phi \in \Gamma)\,\mathfrak{M} \models \Phi$; в этом случае алгебраическую систему $\mathfrak{M}$ называют *моделью множества* Γ и пишут $\mathfrak{M} \models \Gamma$.

Высказывание Φ языка Ω называется *общезначимым*, если $\mathfrak{M} \models \Phi$ для любой системы $\mathfrak{M}$ сигнатуры Ω. Формула $\Phi(x_1,\ldots,x_n)$, содержащая лишь свободные переменные $x_1,\ldots,x_n$, называется общезначимой, если для любой алгебраической системы $\mathfrak{M} = \langle M,\Omega\rangle$ и любых $m_1,\ldots,m_n \in M$ имеет место $\mathfrak{M} \models \Phi(m_1,\ldots,m_n)$. Очевидно, что формула $\Phi(x_1,\ldots,x_n)$ общезначима тогда и только тогда, когда общезначимо ее универсальное замыкание.

Элементарной теорией называется произвольное множество высказываний некоторого элементарного языка. Высказывания, составляющие теорию, называются ее *аксиомами*. Теория называется *совместной*, если она имеет модель. В противном случае теория называется *несовместной*.

Говорят, что высказывание Φ языка Ω *логически следует* из множества высказываний T языка Ω, и пишут $T \models \Phi$, если Φ

истинно во всякой модели множества T. В этом случае высказывание Φ называется *логическим следствием* множества высказываний T. *Теоремами* элементарной теории T в языке Ω называются высказывания языка Ω, которые логически следуют из T. Таким образом, теорема данной теории T — это высказывание, истинное во всех моделях теории T. Нетрудно доказать, что высказывание Φ является теоремой теории T тогда и только тогда, когда при добавлении аксиомы $\neg\Phi$ к теории T получается несовместная теория.

§3.6. Классическое исчисление предикатов

Обычно установление факта, что данное утверждение логически следует из аксиом теории, достигается путем некоторого рассуждения. Такое рассуждение называют *доказательством*, а полученное с его помощью следствие из аксиом — *теоремой*. В случае элементарных теорий методы доказательства можно полностью обозреть и систематизировать. Это делается с помощью *исчисления предикатов*.

Аксиомы и правила вывода классического исчисления предикатов. Пусть фиксирован элементарный язык Ω. Классическое исчисление предикатов в языке Ω задается следующим набором *схем аксиом*:

1. $A \supset (B \supset A)$;
2. $(A \supset B) \supset ((A \supset (B \supset C)) \supset (A \supset C))$;
3. $A \,\&\, B \supset A$;
4. $A \,\&\, B \supset B$;
5. $A \supset (B \supset A \,\&\, B)$;
6. $A \supset A \vee B$;
7. $B \supset A \vee B$;
8. $(A \supset C) \supset ((B \supset C) \supset (A \vee B \supset C))$;
9. $(A \supset B) \supset ((A \supset \neg B) \supset \neg A)$;
10. $\neg\neg A \supset A$;
11. $\forall v\, A(v) \supset A(t)$;
12. $A(t) \supset \exists v\, A(v)$.

В схемах $1-10$ A, B, C — произвольные формулы языка Ω. В схемах 11 и 12 $A(v)$ — формула языка Ω, v — переменная, t — терм языка Ω, *свободный для v в $A(v)$*, т. е. никакое свободное вхождение v в $A(v)$ не находится в области действия квантора по переменной, входящей в t.

Правила вывода классического исчисления предикатов:

(I) $\dfrac{A, A \supset B}{B}$ (*modus ponens* или MP);

(II) $\dfrac{A \supset B}{\exists v\, A \supset B}$ (*удаление квантора существования*);

(III) $\dfrac{B \supset A}{B \supset \forall v\, A}$ (*введение квантора всеобщности*).

Правила (II) и (III) называют *правилами Бернайса.* В этих правилах A и B — формулы языка Ω, v — переменная, не имеющая свободных вхождений в B. Условимся говорить, что применение этих правил *связывает* переменную v.

Выводом в исчислении предикатов называется конечная последовательность формул $\Phi_1, \ldots, \Phi_n$ такая, что для каждого $i = 1, \ldots, n$ формула Φ_i либо есть аксиома, либо получается из одной или двух предыдущих формул по одному из правил вывода. Говорят, что формула Φ *выводима* в исчислении предикатов и пишут $\vdash \Phi$, если существует вывод, оканчивающийся формулой Φ.

Пусть Γ — некоторое множество формул языка Ω, которые условно будем называть *гипотезами. Квазивыводом* из Γ называется конечная последовательность формул $\Phi_1, \ldots, \Phi_n$ такая, что для каждого $i = 1, \ldots, n$ формула Φ_i либо есть аксиома, либо есть гипотеза, либо получается из одной или двух предыдущих формул по одному из правил вывода. Для квазивывода $\Phi_1, \ldots, \Phi_n$ и для каждого $i = 1, \ldots, n$ определим по индукции множество $\Delta(\Phi_i) \subseteq \Gamma$:

1) если Φ_i — аксиома, то $\Delta(\Phi_i) = \emptyset$;

2) если Φ_i — гипотеза, то $\Delta(\Phi_i) = \{\Phi_i\}$;

3) если Φ_i получена по правилу MP из Φ_k и Φ_l, то

$$\Delta(\Phi_i) = \Delta(\Phi_k) \cup \Delta(\Phi_l);$$

4) если Φ_i получена по правилу (II) или (III) из Φ_k, то

$$\Delta(\Phi_i) = \Delta(\Phi_k).$$

Если гипотеза Φ принадлежит множеству $\Delta(\Phi_i)$, будем говорить, что в данном квазивыводе формула Φ_i *зависит* от Φ.

Выводом из Γ называется квазивывод из Γ, в котором всякое применение правила (II) или (III) к формуле Φ_i связывает переменную, не входящую свободно ни в одну из формул из множества $\Delta(\Phi_i)$. Говорят, что формула Φ *выводима из* Γ и пишут $\Gamma \vdash \Phi$, если существует вывод из Γ, оканчивающийся формулой Φ.

Нетрудно проверить, что каждая аксиома классического исчисления предикатов общезначима, и при применении правил вывода к общезначимым формулам получается общезначимая формула. Поэтому имеет место следующая *теорема о корректности* классического исчисления предикатов:

Теорема 15. *Всякая формула, выводимая в классическом исчислении предикатов, общезначима.*

Теорема о дедукции. Следующая теорема называется *теоремой о дедукции* для исчисления предикатов.

Теорема 16. *Каковы бы ни были множество формул* Γ *и формулы* Φ, Ψ, *если* $\Gamma \cup \{\Phi\} \vdash \Psi$, *то* $\Gamma \vdash \Phi \supset \Psi$.

Доказательство. Сначала отметим одно свойство выводимости. Пусть имеется вывод $\Phi_1, \ldots, \Phi_n$ формулы Ψ из множества Γ, в котором Ψ не зависит от гипотезы $\Phi \in \Gamma$. Вычеркнем из этого вывода все формулы Φ_i, для которых $\Phi \in \Delta(\Phi_i)$. Нетрудно проверить, что получившаяся последовательность формул является выводом формулы Ψ из множества $\Gamma \setminus \{\Phi\}$, причем в этом выводе каждая формула зависит от тех же гипотез, что и в исходном выводе.

Приступим к доказательству теоремы. Пусть $\Phi_1, \ldots, \Phi_n$ — вывод формулы Ψ из $\Gamma \cup \{\Phi\}$. Положим $\Delta'(\Phi_i) = \Delta(\Phi_i) \cap \Gamma$. По индукции докажем, что для любого $i = 1, \ldots, n$ существует вывод из Γ формулы $\Phi \supset \Phi_i$, в котором $\Phi \supset \Phi_i$ не зависит от гипотез, не входящих в $\Delta'(\Phi_i)$. Сначала рассмотрим случай, когда в выводе $\Phi_1, \ldots, \Phi_n$ формула Φ_i не зависит от Φ. Тогда, как мы только что заметили, существует вывод формулы Φ_i из Γ, в котором Φ_i зависит от тех же гипотез, что и в исходном выводе. Продолжим этот вывод до вывода формулы $\Phi \supset \Phi_i$ из Γ: …, Φ_i (зависит от $\Delta(\Phi_i)$); $\Phi_i \supset (\Phi \supset \Phi_i)$ (аксиома 1); $\Phi \supset \Phi_i$ (получено по правилу MP, зависит от $\Delta(\Phi_i)$).

Если Φ_i есть формула Φ, то, как и в доказательстве теоремы 4, строится вывод формулы $\Phi \supset \Phi$, который является также выводом из Γ.

Перейдем к общему случаю. Если $i = 1$, то Φ_i либо является аксиомой или принадлежит множеству Γ, либо совпадает с Φ. Во всех случаях утверждение доказано выше.

Пусть $i = k+1$, и для каждого $j \leq k$ существует вывод из Γ формулы $\Phi \supset \Phi_j$, в котором эта формула не зависит от гипотез, не входящих в $\Delta'(\Phi_j)$. В случаях, когда формула Φ_i является аксиомой или гипотезой из $\Gamma \cup \{\Phi\}$, утверждение уже доказано. Рассмотрим случай, когда в исходном выводе формулы Ψ из $\Gamma \cup \{\Phi\}$ формула Φ_i получена по одному из правил вывода.

Случай, когда Φ_i получена по правилу MP из Φ_j и Φ_l, причем $j, l \leq k$ и Φ_l имеет вид $\Phi_j \supset \Phi_i$, рассматривается точно так же, как в доказательстве теоремы о дедукции для исчисления высказываний (теорема 5).

Пусть формула Φ_i получена по правилу (II) из формулы Φ_j ($j \leq k$). В этом случае Φ_j имеет вид $\Phi' \supset \Psi$, а Φ_i имеет вид $\exists v\, \Phi' \supset \Psi$, где Φ' и Ψ — формулы языка Ω, v — переменная, не имеющая свободных вхождений в Ψ. При этом $\Delta(\Phi_i) = \Delta(\Phi_j)$. Случай, когда Φ_i не зависит от Φ, уже рассмотрен, поэтому будем считать, что Φ_i зависит от Φ. Следовательно, Φ_j также зависит от Φ. Отсюда и из определения вывода из гипотез вытекает, что Φ и все формулы из множества $\Delta'(\Phi_j)$ не содержат свободных вхождений v. По индуктивному предположению существует вывод из Γ формулы $\Phi \supset \Phi_j$ (т. е. $\Phi \supset (\Phi' \supset \Psi)$), в котором $\Phi \supset \Phi_j$ не зависит от гипотез, не входящих в $\Delta'(\Phi_j)$. Продолжим его до вывода из Γ формулы $\Phi \supset \Phi_i$ (т. е. $\Phi \supset (\exists v \Phi' \supset \Psi)$), в котором $\Phi \supset \Phi_i$ не зависит от гипотез, не входящих в $\Delta'(\Phi_i)$:

$\ldots$, $\Phi \supset (\Phi' \supset \Psi)$ (зависит только от $\Delta'(\Phi_j)$); $\ldots$ [вывод формулы $\Phi' \supset (\Phi \supset \Psi)$ из формулы $\Phi \supset (\Phi' \supset \Psi)$ средствами исчисления высказываний]; $\Phi' \supset (\Phi \supset \Psi)$ (зависит только от $\Delta'(\Phi_j)$); $\exists v\, \Phi' \supset (\Phi \supset \Psi)$ (получено по правилу (II), зависит только от $\Delta'(\Phi_j)$); $\ldots$ [вывод $\Phi \supset (\exists v\, \Phi' \supset \Psi)$ из формулы $\exists v\, \Phi' \supset (\Phi \supset \Psi)$ средствами исчисления высказываний]; $\Phi \supset (\exists v \Phi' \supset \Psi)$ (зависит только от $\Delta'(\Phi_j) = \Delta'(\Phi_i)$).

Таким образом, случай, когда формула Φ_i получена по правилу (II), полностью рассмотрен.

Пусть формула Φ_i получена по правилу (III) из формулы Φ_j ($j \leq k$). В этом случае Φ_j имеет вид $\Psi \supset \Phi'$, а Φ_i имеет вид

$\Psi \supset \forall v\,\Phi'$, где Φ' и Ψ — формулы языка Ω, v — переменная, не имеющая свободных вхождений в Ψ. При этом $\Delta(\Phi_i) = \Delta(\Phi_j)$. Случай, когда Φ_i не зависит от Φ, уже рассмотрен, поэтому будем считать, что Φ_i зависит от Φ. Следовательно, Φ_j также зависит от Φ. Отсюда и из определения вывода из гипотез вытекает, что Φ и все формулы из $\Delta'(\Phi_j)$ не содержат свободных вхождений v. По индуктивному предположению существует вывод из Γ формулы $\Phi \supset \Phi_j$ (т. е. формулы $\Phi \supset (\Psi \supset \Phi')$), в котором $\Phi \supset \Phi_j$ не зависит от гипотез, не входящих в $\Delta'(\Phi_j)$. Продолжим его до вывода из Γ формулы $\Phi \supset \Phi_i$ (т. е. формулы $\Phi \supset (\Psi \supset \forall v\Phi')$), в котором $\Phi \supset \Phi_i$ не зависит от гипотез, не входящих в $\Delta'(\Phi_i)$:
$\ldots$ [вывод из Γ формулы $\Phi \supset (\Psi \supset \Phi')$]; $\Phi \supset (\Psi \supset \Phi')$ (зависит только от $\Delta'(\Phi_j)$); $\ldots$ [вывод формулы $\Phi \,\&\, \Psi \supset \Phi'$ из формулы $\Phi \supset (\Psi \supset \Phi')$ средствами исчисления высказываний]; $\Phi \,\&\, \Psi \supset \Phi'$ (зависит только от $\Delta'(\Phi_j)$); $\Phi \,\&\, \Psi \supset \forall v\,\Phi'$ (получено по правилу (III), зависит только от $\Delta'(\Phi_j)$); $\ldots$ [вывод $\Phi \supset (\Psi \supset \forall v\,\Phi')$ из формулы $\Phi \,\&\, \Psi \supset \forall v\,\Phi'$ средствами исчисления высказываний]; $\Phi \supset (\Psi \supset \forall v\Phi')$ (зависит только от $\Delta'(\Phi_j) = \Delta'(\Phi_i)$).
Таким образом, случай, когда формула Φ_i получена по правилу (III), также полностью рассмотрен. $\square$

Рассмотрим одно применение теоремы о дедукции.

Теорема 17 (обобщенная теорема от корректности)**.** *Каковы бы ни были множество высказываний* Γ *и высказывание* Φ*, если* $\Gamma \vdash \Phi$*, то* $\Gamma \models \Phi$*.*

Доказательство. Пусть $\Gamma \vdash \Phi$. Тогда существует конечное множество $\Delta = \{\Phi_1, \ldots, \Phi_n\} \subseteq \Gamma$ такое, что $\Delta \vdash \Phi$. Применяя n раз теорему о дедукции, получаем $\vdash \Phi_1 \supset (\ldots \supset (\Phi_n \supset \Phi)\ldots)$. В силу теоремы о корректности исчисления предикатов (теорема 15) формула

$$\Phi_1 \supset (\ldots \supset (\Phi_n \supset \Phi)\ldots) \tag{3.6}$$

общезначима. Докажем, что $\Gamma \models \Phi$. Пусть $\mathfrak{M}$ — модель множества Γ. Тогда все формулы $\Phi_1, \ldots, \Phi_n$ истинны в алгебраической системе $\mathfrak{M}$. Так как кроме того общезначимая формула (3.6) истинна в $\mathfrak{M}$, то, очевидно, формула Φ также истинна в $\mathfrak{M}$. $\square$

§3.7. Теорема Гёделя о полноте классического исчисления предикатов

Расширения непротиворечивых теорий. Множество формул Γ называется *противоречивым*, если существует такая формула Φ, что $\Gamma \vdash \Phi$ и $\Gamma \vdash \neg\Phi$. В противном случае Γ называется *непротиворечивым.* Нетрудно доказать, что Γ противоречиво тогда и только тогда, когда $\forall\Psi\,[\Gamma \vdash \Psi]$. Зафиксируем замкнутую формулу Φ и через $\perp$ обозначим формулу $\Phi \,\&\, \neg\Phi$. Очевидно, что множество Γ противоречиво тогда и только тогда, когда $\Gamma \vdash \perp$. Таким образом, вместо «множество Γ противоречиво» можно писать $\Gamma \vdash \perp$. Нетрудно доказать (см. упражнение 4), что для классического исчисления предикатов имеет место *правило доказательства от противного*

$$\Gamma \cup \{\neg\Psi\} \vdash \perp \Leftrightarrow \Gamma \vdash \Psi.$$

Теорема 18. *Пусть $\Gamma_0, \Gamma_1, \Gamma_2, \ldots$ — непротиворечивые множества высказываний языка Ω, причем*

$$\Gamma_0 \subseteq \Gamma_1 \subseteq \Gamma_2 \subseteq \ldots \subseteq \Gamma_n \subseteq \Gamma_{n+1} \subseteq \ldots.$$

Тогда множество $\Gamma = \bigcup\limits_{n=1}^{\infty} \Gamma_n$ непротиворечиво.

Доказательство. Пусть множество Γ противоречиво. Тогда противоречиво некоторое конечное его подмножество $\Delta \subseteq \Gamma$. Очевидно, что $\Delta \subseteq \Gamma_n$ для некоторого n. Следовательно, множество Γ_n противоречиво, что невозможно по условию. Значит, на самом деле множество Γ непротиворечиво. $\square$

Множество высказываний Γ языка Ω будем называть *максимальным непротиворечивым множеством*, если Γ непротиворечиво, но любое собственное его расширение противоречиво. Нетрудно доказать, что всякое максимальное непротиворечивое множество высказываний Γ обладает следующими свойствами:

1) Γ полно в том смысле, что для любого высказывание Φ языка Ω имеет место либо $\Phi \in \Gamma$, либо $(\neg\Phi) \in \Gamma$;

2) Γ замкнуто относительно выводимости в том смысле, что каково бы ни было высказывание Φ языка Ω, если $\Gamma \vdash \Phi$, то $\Phi \in \Gamma$.

Теорема 19. *Если множество высказываний* Γ *языка* Ω *непротиворечиво, то существует максимальное непротиворечивое множество высказываний* Γ' *языка* Ω *такое, что* $\Gamma \subseteq \Gamma'$.

Доказательство. Будем считать, что сигнатура Ω не более чем счетна. Тогда множество всех высказываний языка Ω счетно. Зафиксируем пересчет $\Phi_0, \Phi_1, \Phi_2, \ldots$ этого множества. Определим последовательность непротиворечивых множеств высказываний $\Gamma_0, \Gamma_1, \Gamma_2, \ldots$. Положим $\Gamma_0 = \Gamma$. Пусть непротиворечивое множество высказываний Γ_n уже определено. Если $\Gamma_n \nvdash \neg\Phi_n$, положим $\Gamma_{n+1} = \Gamma_n \cup \{\Phi_n\}$; в противном случае $\Gamma_{n+1} = \Gamma_n$. Нетрудно доказать, что в любом случае множество Γ_{n+1} непротиворечиво. Таким образом, мы получили последовательность непротиворечивых множеств высказываний $\Gamma_0, \Gamma_1, \Gamma_2, \ldots$, причем $\Gamma_0 \subseteq \Gamma_1 \subseteq \Gamma_2 \subseteq \ldots \subseteq \Gamma_n \subseteq \Gamma_{n+1} \subseteq \ldots$. По теореме 18 множество $\Gamma' = \bigcup\limits_{n=1}^{\infty} \Gamma_n$ непротиворечиво. Из построения множеств Γ_n видно, что Γ' является максимальным непротиворечивым множеством. □

Множество высказываний Γ языка Ω будем называть *насыщенным*, если всякий раз, когда формула вида $\exists v \Phi(v)$ выводима из Γ, имеет место $\Gamma \vdash \Phi(c)$ для некоторой константы c из Ω.

Теорема 20. *Пусть* Γ — *непротиворечивое множество высказываний языка* Ω, *а сигнатура* Ω' *получена добавлением к* Ω *счетного множества дополнительных констант. Тогда существует максимальное непротиворечивое насыщенное множество высказываний* Γ' *языка* Ω' *такое, что* $\Gamma \subseteq \Gamma'$.

Доказательство. Пусть сигнатура Ω' получена добавлением к Ω множества дополнительных констант $M = \{c_0, c_1, c_2, \ldots\}$. Множество высказываний вида $\exists v \Phi$ языка Ω' счетно. Зафиксируем некоторый пересчет таких высказываний:

$$\exists v_0 \Phi_0, \exists v_1 \Phi_1, \exists v_2 \Phi_2, \ldots. \tag{3.7}$$

Определим последовательность множеств $\Gamma_0, \Gamma_1, \Gamma_2, \ldots$, причем Γ_n $(n = 0, 1, 2, \ldots)$ будет максимальным множеством высказываний в синатуре Ω_n, полученной добавлением к Ω лишь конечного числа констант из M. При этом в ходе построения последовательности $\Gamma_0, \Gamma_1, \Gamma_2, \ldots$ некоторые формулы из последовательности (3.7) будут вычеркиваться. Положим $\Omega_0 = \Omega$, Γ_0 — максимальное непротиворечивое расширение множества Γ в языке Ω_0, существующее в силу теоремы 19. Пусть максимальное непротиворечивое множество высказываний Γ_n в языке Ω_n построено, и $\exists v \Phi(v)$ — первая еще не вычеркнутая формула языка Ω_n из последовательности (3.7) такая, что $\Gamma_n \vdash \exists v \Phi(v)$. Пусть c — первая константа из M, не встречающаяся в Γ_n и в $\Phi(v)$. Пусть Ω_{n+1} — сигнатура, полученная добавлением к Ω_n константы c. Нетрудно доказать, что множество высказываний $\Gamma_n \cup \{\Phi(c)\}$ в языке Ω_{n+1} непротиворечиво. В качестве Γ_{n+1} возьмем максимальное непротиворечивое расширение множества $\Gamma_n \cup \{\Phi(c)\}$ в языке Ω_{n+1}, существующее в силу теоремы 19. Последовательность $\Gamma_0, \Gamma_1, \Gamma_2, \ldots$ построена. Положим $\Omega' = \bigcup\limits_{n=1}^{\infty} \Omega_n$, $\Gamma' = \bigcup\limits_{n=1}^{\infty} \Gamma_n$. Нетрудно доказать, что Γ' — максимальное непротиворечивое насыщенное множество. $\square$

Совместность непротиворечивых теорий. Докажем, что любая непротиворечивая элементарная теория имеет модель.

Теорема 21. *Для любого максимального непротиворечивого насыщенного множества высказываний существует модель.*

Доказательство. Пусть Γ — максимальное непротиворечивое насыщенное множество высказываний языка $\Omega = \langle Cn, Fn, Pr \rangle$. Определим интерпретацию $\mathfrak{M}$. Ее носитель — множество M всех термов языка Ω, не содержащих переменных. Для $c \in Cn$, $f \in Fn$, $P \in Pr$ и $t_1, \ldots, t_n \in M$ положим

$$\bar{c} \leftrightharpoons c; \ \bar{f}(t_1, \ldots, t_n) \leftrightharpoons f(t_1, \ldots, t_n);$$

$$\bar{P}(t_1, \ldots, t_n) = 1 \leftrightharpoons P(t_1, \ldots, t_n) \in \Gamma.$$

Индукцией по логической длине высказывания Φ языка Ω нетрудно доказать, что $\mathfrak{M} \models \Phi \Leftrightarrow \Phi \in \Gamma$. Следовательно, $\mathfrak{M}$ является моделью множества Γ. $\square$

Теорема 22. *Любое непротиворечивое множество высказываний имеет модель.*

Доказательство. Пусть Γ — непротиворечивое множество высказываний языка Ω. В силу теоремы 20 существует такое максимальное непротиворечивое насыщенное множество высказываний Γ' сигнатуры Ω', полученной добавлением к Ω счетного множества дополнительных констант, что $\Gamma \subseteq \Gamma'$. По теореме 21 существует модель $\mathfrak{M}'$ множества Γ'. Это интерпретация языка Ω'. Рассмотрим интерпретацию $\mathfrak{M}$ языка Ω с тем же носителем, что и $\mathfrak{M}'$, в котором символы из Ω интерпретируются точно так же, как и в $\mathfrak{M}'$. Иными словами, $\mathfrak{M}$ — это по сути та же интерпретация $\mathfrak{M}'$, в которой нас не интересуют значения символов, не входящих в сигнатуру Ω. Можно доказать, что всякое высказывание языка Ω истинно в интерпретации $\mathfrak{M}$ тогда и только тогда, когда оно истинно в интерпретации $\mathfrak{M}'$. Так как все высказывания из Γ истинны в $\mathfrak{M}'$, то они истинны и в $\mathfrak{M}$. Значит, $\mathfrak{M}$ — модель множества Γ. $\square$

Теорема 23 (теорема Гёделя о полноте)**.** *Любая общезначимая формула выводима в исчислении предикатов.*

Доказательство. Пусть Φ — общезначимая формула. Если в ней есть свободные переменные $v_1, \ldots, v_n$, то замкнутая формула $\forall v_1 \ldots \forall v_n \Phi$, которую мы обозначим через Ψ, также общезначима. Докажем $\vdash \Psi$. Допустим противное, т. е. что $\nvdash \Psi$. Тогда в силу правила доказательства от противного множество $\{\neg\Psi\}$ непротиворечиво. По теореме 22 оно имеет модель. В этой модели формула Ψ ложна, что противоречит ее общезначимости. Значит, $\vdash \forall v_1 \ldots \forall v_n \Phi$, а тогда $\vdash \Phi$. $\square$

Теорема 24. *В исчислении предикатов выводимы все общезначимые формулы и только они.*

Доказательство. Это утверждение вытекает из теоремы 23 и теоремы о корректности исчисления предикатов (теорема 15). $\square$

Теорема 25 (обобщенная теорема Гёделя о полноте)**.** *Пусть Γ — произвольное множество высказываний языка Ω, Φ — высказывание языка Ω, причем $\Gamma \models \Phi$. Тогда $\Gamma \vdash \Phi$.*

Доказательство. Пусть $\Gamma \models \Phi$. Допустим, что $\Gamma \nvdash \Phi$. Тогда в силу правила доказательства от противного множество $\Gamma \cup \{\neg\Phi\}$ непротиворечиво. По теореме 22 оно имеет модель $\mathfrak{M}$, так что $\mathfrak{M} \models \Gamma$ и $\mathfrak{M} \models \neg\Phi$. С другой стороны, если $\mathfrak{M} \models \Gamma$, то $\mathfrak{M} \models \Phi$, ибо $\Gamma \models \Phi$. Полученное противоречие показывает, что на самом деле $\Gamma \vdash \Phi$. □

Теорема 26. *Высказывание* Φ *логически следует из множества высказываний* Γ *тогда и только тогда, когда* Φ *выводится из* Γ.

Доказательство. Это утверждение вытекает из теоремы 25 и обобщенной теоремы о корректности исчисления предикатов (теорема 17). □

Упражнения

1. Доказать, что соответствие $\Gamma \vdash A$ обладает свойствами монотонности, транзитивности и компактности.

2. Доказать, что каждая аксиома классического исчисления высказываний является тавтологией.

3. Доказать теорему о корректности классического исчисления предикатов.

4. Доказать, что для классического исчисления предикатов справедливо правило доказательства от противного.

5. Построить выводы в классическом исчислении предикатов формул $P(y) \supset Q(y)$ и $\forall x\, P(x) \supset \forall x\, Q(x)$ из множества гипотез $\{\forall x\, (P(x) \supset Q(x))\}$.

6. Доказать *локальную теорему Мальцева*: если любое конечное подмножество множества высказываний Γ выполнимо, то Γ выполнимо.

7. Доказать *теорему Мальцева о компактности*: каковы бы ни были множество высказываний Γ и высказывание Φ, если $\Gamma \models \Phi$, то $\Delta \models \Phi$ для некоторого конечного подмножества $\Delta \subseteq \Gamma$.

Глава 4

Интуиционистское исчисление высказываний (ИИВ)

§4.1. Исчисление Колмогорова

Первая попытка построения системы аксиом интуиционистской логики была предпринята А. Н. Колмогоровым [5]. Он исходил из предложенной Д. Гильбертом [21] системы классической логики высказываний, состоящей из следующих схем аксиом:

Г1. $A \supset (B \supset A)$;
Г2. $(A \supset (A \supset B)) \supset (A \supset B)$;
Г3. $(A \supset (B \supset C)) \supset (B \supset (A \supset C))$;
Г4. $(B \supset C) \supset ((A \supset B) \supset (A \supset C))$;
Г5. $A \supset (\neg A \supset B)$;
Г6. $(A \supset B) \supset ((\neg A \supset B) \supset B)$.

Другие законы классической логики высказываний могут быть получены из аксиом с помощью правила MP. Исчисление, задаваемое схемами аксиом Г1 – Г6 вместе с правилом MP, будем называть *исчислением Гильберта.* Подвергая эту систему аксиом критическому анализу с интуиционистской точки зрения, А. Н. Колмогоров приходит к системе аксиом интуиционистской логики, состоящей из схем аксиом Г1 – Г4 исчисления Гильберта, а также следующей схемы аксиом:

$$(A \supset B) \supset ((A \supset \neg B) \supset \neg A).$$

Таким образом, *исчисление Колмогорова* имеет следующие схемы аксиом:

К1. $A \supset (B \supset A)$;
К2. $(A \supset (A \supset B)) \supset (A \supset B)$;
К3. $(A \supset (B \supset C)) \supset (B \supset (A \supset C))$;
К4. $(B \supset C) \supset ((A \supset B) \supset (A \supset C))$;
К5. $(A \supset B) \supset ((A \supset \neg B) \supset \neg A)$.

Единственным правилом вывода является MP.

Аксиомы исчисления Колмогорова являются схемами интуиционистски истинных высказываний. Рассмотрим, например, схему К1. Покажем, что для любых A и B высказывание $A \supset (B \supset A)$ интуиционистски истинно, т. е. существует общий метод получения обоснования для $B \supset A$, если дано обоснование для A. Пусть дано обоснование a для A. Обоснованием для $B \supset A$ может служить операция, которая любое обоснование для B преобразует в имеющееся у нас обоснование a для A. Аналогичными рассуждениями нетрудно показать, что схемы К2 – К5 приемлемы с интуиционистской точки зрения.

Правило МР сохраняет интуиционистскую истинность: если высказывания A и $A \supset B$ истинны, т. е. даны обоснование для A и общий метод, позволяющий получить обоснование для B из любого обоснования для A, то истинно и высказывание B. Поэтому все формулы, выводимые в исчислении Колмогорова, являются схемами интуиционистски истинных высказываний.

По поводу аксиомы Г5 А. Н. Колмогоров пишет, что хотя критика Бруаэра не коснулась ее, тем не менее она «не имеет и не может иметь интуитивных оснований как утверждающая нечто о последствиях невозможного: мы обязаны признать B, если признали ложным истинное суждение A» [5, II, §4]. Аксиома Г6 по существу выражает закон исключенного третьего: каково бы ни было высказывание A, если в качестве B взять $A \vee \neg A$, то очевидно, что из интуиционистской истинности высказывания Г5 вытекает интуиционистская истинность высказывания $A \vee \neg A$, что, как мы знаем, имеет место не для всех высказываний A. Позже мы строго докажем, что аксиомы Г5 и Г6 невыводимы в исчислении Колмогорова.

Можно доказать, что для исчислений Гильберта и Колмогорова имеет место теорема о дедукции: если $\Gamma \cup \{A\} \vdash B$, то $\Gamma \vdash A \supset B$. Для этих исчислений верен также принцип приведения к абсурду: если множество $\Gamma \cup \{A\}$ противоречиво, то $\Gamma \vdash \neg A$. Нетрудно доказать, что всякая формула, выводимая в исчислении Колмогорова, выводима и в исчислении Гильберта. Очевидно, что для этого достаточно доказать выводимость аксиомы К5 в исчислении Гильберта (см. упражнение 1).

§4.2. Интуиционистское, минимальное и позитивное исчисления

Исчисление Колмогорова явилось первой аксиоматизацией интуиционистской логики высказываний. Позднее другие системы аксиом были предложены В. И. Гливенко [17], А. Гейтингом [20], Г. Генценом [16], [6, §77]. Они эквивалентны между собой в том смысле, что из них выводимы одни и те же формулы, и эквивалентны системе Гейтинга:

И1. $A \supset (B \supset A)$;
И2. $(A \supset B) \supset ((A \supset (B \supset C)) \supset (A \supset C))$;
И3. $A \,\&\, B \supset A$;
И4. $A \,\&\, B \supset B$;
И5. $A \supset (B \supset A \,\&\, B)$;
И6. $A \supset A \vee B$;
И7. $B \supset A \vee B$;
И8. $(A \supset C) \supset ((B \supset C) \supset (A \vee B \supset C))$;
И9. $(A \supset B) \supset ((A \supset \neg B) \supset \neg A)$;
И10. $A \supset (\neg A \supset B)$.

Эти схемы аксиом вместе с правилом MP задают *интуиционистское исчисление высказываний* (ИИВ).

Мы видим, что схема аксиом И10 — это отвергнутая Колмогоровым схема аксиом Г5 исчисления Гильберта. Все же она включена в систему постулатов исчисления, называемого интуиционистским. В пользу этого можно привести такое расуждение. Пусть дано обоснование для высказывания A. Тогда в качестве обоснования для высказывания $\neg A \supset B$ можно взять произвольное общее правило, поскольку оно должно применяться только в случае, когда дано обоснование для высказывания $\neg A$, однако, имея обоснование для высказывания A, мы можем быть уверены, что наше обоснование для высказывания $\neg A \supset B$ никогда не будет использовано. Те, кого такое обоснование удовлетворяет, могут пользоваться ИИВ. Остальные должны довольствоваться *минимальным исчислением*, введенным И. Юхансоном [23]. Оно задается схемами аксиом И1 – И9. Если из минимального исчисления исключить схему аксиом И9, то получится *позитивное исчисление*, рассмотренное Д. Гильбертом и П. Бернайсом [4].

Для рассматриваемых исчислений имеет место *правило подстановки* (предложение 4). Так как в интуиционистском, минимальном и позитивном исчислениях есть схемы аксиом И1 и И2, а единственное правило вывода — МР, то в силу предложения 5 для этих исчислений верна *теорема о дедукции*. Присутствие схемы аксмиом И9 в интуиционистском и минимальном исчислениях позволяет утверждать в силу предложения 6, что для этих исчислений верен *принцип приведения к абсурду*. Более того, для ИИВ верны все производные правила вывода, сформулированные в теореме 7, за исключением правила удаления отрицания ($\neg \to$).

Формулы A и B назовем *эквивалентными* в данном исчислении, если выводима формула $A \equiv B$. Для рассматриваемых исчислений имеет место *теорема об эквивалентной замене*: если формула B получена заменой в формуле A некоторого вхождения подформулы C на эквивалентную ей формулу D, то A и B эквивалентны (см. упражнение 2). Очевидно, что эквивалентные формулы одновременно выводимы или невыводимы.

Соотношение между исчислением Колмогорова и минимальным исчислением выражается следующими двумя фактами: 1) всякая формула, выводимая в исчислении Колмогорова, выводима и в минимальном исчислении; 2) всякая формула, содержащая только логические связки $\supset$ и $\neg$ и выводимая в минимальном исчислении, выводима и в исчислении Колмогорова. Таким образом, исчисление Колмогорова — это импликативно-негативный фрагмент минимального исчисления (см. [10]).

Рассмотрим соотношение между минимальным и позитивным исчислением. Пусть A — пропозициональная формула, $\perp$ — переменная, не входящая в A. Через $A_\perp$ обозначим результат последовательной замены в A подформул вида $\neg B$ на $B \supset \perp$. Формулу $A_\perp$ назовем $\perp$-*образом* формулы A.

Предложение 7. *Формула A выводима в минимальном исчислении тогда и только тогда, когда ее $\perp$ -образ $A_\perp$ выводим в позитивном исчислении.*

Доказательство. Тот факт, что если формула A выводима в минимальном исчислении, то ее $\perp$ -образ $A_\perp$ выводим в позитивном исчислении, доказывается индукцией по длине вывода формулы A в минимальном исчислении с учетом следующих замечаний. Во-первых, $\perp$-образ всякой аксиомы минимального исчисления является аксиомой позитивного исчисления. Действительно, $\perp$-образ любой из аксиом И1 – И8 имеет ту же логическую форму и является аксиомой позитивного исчисления. $\perp$-образ аксиомы И9 имеет вид

$$(A_\perp \supset B_\perp) \supset ((A_\perp \supset (B_\perp \supset \perp)) \supset (A_\perp \supset \perp)),$$

т. е. получается по схеме аксиом И2. Во-вторых, если формула B получена по правилу MP из формул A и $A \supset B$, то $B_\perp$ получается по правилу MP из формул $A_\perp$ и $(A \supset B)_\perp$, имеющей вид $A_\perp \supset B_\perp$. Отсюда следует, что если в выводе формулы A в минимальном исчислении каждую формулу заменить на ее $\perp$-образ, то получится вывод формулы $A_\perp$ в позитивном исчислении.

Докажем теперь, что если формула $A_\perp$ выводима в позитивном исчислении, то формула A выводима в минимальном исчислении. Для этого заметим, что если формула $A_\perp$ выводима в позитивном исчислении, то она выводима и в минимальном исчислении. Поскольку для рассматриваемых исчислений имеет место правило подстановки, то в минимальном исчислении выводима и формула $A_{\neg(\perp\supset\perp)}$, полученная подстановкой в $A_\perp$ формулы $\neg(\perp \supset \perp)$ вместо переменной $\perp$. Нетрудно доказать, что какова бы ни была формула B, формулы $B \supset \neg(\perp \supset \perp)$ и $\neg B$ эквивалентны в минимальном исчислении. Следовательно в силу теоремы об эквивалентной замене формулы $A_{\neg(\perp\supset\perp)}$ эквивалентны в минимальном исчислении, поэтому, если в минимальном исчислении выводима формула $A_{\neg(\perp\supset\perp)}$, то выводима и формула A. □

Предложение 8. *Формула $P \supset (\neg P \supset Q)$ невыводима в минимальном исчислении.*

Доказательство. $\perp$-образ рассматриваемой формулы есть формула $P \supset ((P \supset \perp) \supset Q)$, очевидно, не являющаяся тавтологией классической логики. Но в позитивном исчислении выводятся только тавтологии. Следовательно, $\perp$-образ формулы $P \supset (\neg P \supset Q)$ невыводим в позитивном исчислении, и в силу предложения 7 сама эта формула невыводима в минимальном исчислении. □

§4.3. Исчисление задач по Колмогорову

ИИВ возникло в результате пересмотра классической логики с интуиционистской точки зрения. Попытка дать истолкование интуиционистской логики в рамках обычных математических понятий была предпринята А. Н. Колмогоровым [25]. Он предложил рассматривать пропозициональные формулы как схемы типов задач. При этом понятия «задачи» и «решения задачи» считаются общеизвестными и никак не уточняются. Пропозициональные переменные интерпретируются как переменные по задачам, а логические операции — как способы получения новых задач из уже имеющихся: задача $A \,\&\, B$ состоит в том, чтобы решить обе задачи A и B; задача $A \vee B$ состоит в том, чтобы решить хотя бы одну из задач A и B; задача $A \supset B$ состоит в том, чтобы свести задачу B к задаче A; задача $\neg A$ состоит в том, чтобы, предположив, что дано решение задачи A, прийти к противоречию.

Всякая пропозициональная формула $F(P_1, \ldots, P_n)$ является схемой типов задач, которая превращается в конкретную задачу, коль скоро переменные $P_1, \ldots, P_n$ интерпретируются как конкретные задачи. Общезначимость пропозициональной формулы понимается как существование общего метода решения задач данного типа. Таким образом, закон исключенного третьего $P \vee \neg P$ не является законом логики задач: общезначимость этой формулы означала бы существование общего метода, позволяющего для любой конкретной задачи либо найти ее решение, либо привести к противоречию предположение о существовании ее решения. Поскольку такой метод вряд ли возможен, формулу $P \vee \neg P$ нельзя признать общезначимой. В то же время формулы, выводимые в ИИВ, оказываются общезначимыми. Тем самым получена интерпретация этого исчисления как логики задач.

Найденная интерпретация интуиционистской логики высказываний имела важное методологическое значение. В рамках хотя и не вполне точных, но все же понятных любому математику понятий «задачи» и «решения задачи» была обоснована необходимость рассмотрения логических систем, не содержащих закона исключенного третьего.

§4.4. Простые импликации

Простой конъюнкцией называется конъюнкция формул вида i) P; ii) $\neg P$; iii) $P \supset Q$; iv) $P \supset Q \vee R$; v) $P \& Q \supset R$; vi) $(P \supset Q) \supset R$, где P, Q, R — пропозициональные переменные. *Простой импликацией* называется формула вида $K \supset Z$, где K — простая конъюнкция, Z — переменная.

Посредством ИИВ+$A(P_1, \ldots, P_n)$ обозначим исчисление, аксиомами которого являются аксиомы ИИВ, а также формулы вида $A(B_1, \ldots, B_n)$, полученные подстановкой в $A(P_1, \ldots, P_n)$ любых формул $B_1, \ldots, B_n$ вместо переменных $P_1, \ldots, P_n$. Будем говорить, что формулы F и G *дедуктивно эквивалентны* в ИИВ, если ИИВ+$F \vdash G$ и ИИВ+$G \vdash F$. Очевидно, что если F и G дедуктивно эквивалентны, то ИИВ$\vdash F \Leftrightarrow$ИИВ$\vdash G$.

Теорема 27. *Всякая пропозициональная формула дедуктивно эквивалентна в ИИВ некоторой простой импликации.*

Доказательство. Всем подформулам G формулы F сопоставим различные переменные P_G, при этом пусть P_G совпадает с G, если G — переменная. Индукцией по построению G определим формулы $K^+(G)$ и $K^-(G)$. Если G — атом, то $K^+(G)$ и $K^-(G)$ есть $G \supset G$. Пусть G имеет вид $A \lambda B$, где λ есть & или $\vee$, и формулы $K^+(A)$, $K^-(A)$, $K^+(B)$, $K^-(B)$ уже определены. Тогда

$$K^+(G) \leftrightharpoons K^+(A) \& K^+(B) \& (P_A \lambda P_B \supset P_G),$$

$$K^-(G) \leftrightharpoons K^-(A) \& K^-(B) \& (P_G \supset P_A \lambda P_B).$$

Если G имеет вид $A \supset B$, то

$$K^+(G) \leftrightharpoons K^-(A) \& K^+(B) \& ((P_A \supset P_B) \supset P_G),$$

$$K^-(G) \leftrightharpoons K^+(A) \& K^-(B) \& (P_G \supset (P_A \supset P_B)).$$

Наконец, если G имеет вид $\neg A$, то

$$K^+(G) \leftrightharpoons K^-(A) \& (\neg P_A \supset P_G),$$

$$K^-(G) \leftrightharpoons K^+(A) \& (P_G \supset \neg P_A).$$

Лемма 1. *Какова бы ни была подформула G формулы F,*
1) $K^+(G) \vdash G \supset P_G$; 2) $K^-(G) \vdash P_G \supset G$.

Доказательство. Утверждения 1) и 2) доказываются одновременно индукцией по построению подформулы G. Если G — переменная, то утверждения 1) и 2) очевидны. Пусть G имеет вид $A \supset B$, причем $K^{+}(A) \vdash A \supset P_A$, $K^{-}(A) \vdash P_A \supset A$, $K^{+}(B) \vdash B \supset P_B$, $K^{-}(B) \vdash P_B \supset B$. Тогда утверждение 1) имеет вид $K^{-}(A) \,\&\, K^{+}(B) \,\&\, ((P_A \supset P_B) \supset P_G) \vdash (A \supset B) \supset P_G$. В силу теоремы о дедукции для его доказательства достаточно показать, что из множества

$$\Gamma = \{K^{-}(A) \,\&\, K^{+}(B) \,\&\, ((P_A \supset P_B) \supset P_G), A \supset B\}$$

выводится P_G. Для этого достаточно доказать $\Gamma \vdash P_A \supset P_B$. В силу теоремы о дедукции для этого достаточно из множества $\Delta = \{K^{-}(A) \,\&\, K^{+}(B) \,\&\, ((P_A \supset P_B) \supset P_G), A \supset B, P_A\}$ вывести P_B. Так как по предположению $K^{+}(B) \vdash B \supset P_B$, то достаточно показать, что $\Delta \vdash B$, для чего достаточно проверить, что $\Delta \vdash A$. Так как по предположению $K^{-}(A) \vdash P_A \supset A$, то достаточно убедиться, что $\Delta \vdash P_A$, что очевидно. Аналогично доказывается утверждение 2), а также рассматриваются случаи, когда G имеет вид $A \lambda B$, где λ есть $\&$ или $\vee$, или $\neg A$. $\square$

Следствие 1. $K^{+}(F) \vdash F \supset P_F$.

Доказательство. Это утверждение немедленно вытекает из леммы 1, когда G есть F. $\square$

Лемма 2. *ИИВ*+$(K^{+}(F) \supset P_F) \vdash F$.

Доказательство. Аксиомой исчисления ИИВ+$(K^{+}(F) \supset P_F)$ является формула, полученная подстановкой в $K^{+}(F) \supset P_F$ вместо каждой переменной P_G подформулы G формулы F. При такой подстановке $K^{+}(F)$ превращается в конъюнкцию формул вида $H \supset H$, а P_F превращается в F. Теперь очевидно, что F выводима в рассматриваемом исчислении. $\square$

Из следствия 1 и леммы 2 вытекает, что F дедуктивно эквивалентна формуле $K^{+}(F) \supset P_F$. Осталось доказать, что последняя дедуктивно эквивалентна в ИИВ простой импликации. Заметим, что $K^{+}(F)$ есть конъюнкция формул вида 1) $P \supset P$; 2) $P \supset \neg Q$; 3) $\neg P \supset Q$; 4) $P \,\&\, Q \supset R$; 5) $P \supset Q \,\&\, R$; 6) $P \supset Q \vee R$; 7) $P \vee Q \supset R$; 8) $(P \supset Q) \supset R$; 9) $P \supset (Q \supset R)$, где P, Q, R — переменные. Каждая формула вида 5) эквивалентна в ИИВ $(P \supset Q) \mathbin{\&} (P \supset R)$. Каждая формула вида 7) эквивалентна формуле $(P \supset R) \mathbin{\&} (Q \supset R)$. Каждая формула вида 9) эквивалентна в ИИВ формуле $P \mathbin{\&} Q \supset R$. Заменим в $K^{+}(F)$ конъюнктивные члены вида 5), 7), 9) на только что указанные эквивалентные им формулы. Получим формулу вида $K'(F)$, эквивалентную формуле $K^{+}(F)$. Очевидно, что формула $K'(F) \supset P_F$ дедуктивно эквивалентна F.

Пусть $\perp$ — пропозициональная переменная, не входящая в $K'(F)$. Заменим в $K'(F)$ каждый конъюнктивный член вида 2) на $P \mathbin{\&} Q \supset \perp$ и каждый конъюнктивный член вида 3) на формулу $(P \supset \perp) \supset Q$; кроме того добавим в $K'(F)$ конъюнктивный член $\neg\perp$. Полученная формула $K''(F)$ является простой конъюнкцией, а формула $K''(F) \supset P_F$ — простой импликацией. Докажем, что $K'(F) \supset P_F$ и $K''(F) \supset P_F$ дедуктивно эквивалентны.

Докажем, что ИИВ$+K''(F) \supset P_F \vdash K'(F) \supset P_F$. Подставим $\neg(P \supset P)$ вместо $\perp$ в $K''(F) \supset P_F$. Получим аксиому рассматриваемого исчисления. При этом каждая формула вида $P \mathbin{\&} Q \supset \perp$ перейдет в формулу $P \mathbin{\&} Q \supset \neg(P \supset P)$, эквивалентную формуле $P \supset \neg Q$, а каждая формула вида $(P \supset \perp) \supset Q$ перейдет в формулу $(P \supset \neg(P \supset P)) \supset Q$, эквивалентную формуле $\neg P \supset Q$; наконец, формула $\neg\perp$ перейдет в выводимую формулу $\neg\neg(P \supset P)$. $\square$

Упражнения

1. Доказать, что аксиома К5 исчисления Колмогорова выводима в исчислении Гильберта.

2. Доказать, что для ИИВ имеет место теорема об эквивалентной замене.

3. Доказать, что каковы бы ни были пропозициональные формулы A и B, следующие формулы выводимы в ИИВ: $A \supset \neg\neg A$; $\neg\neg(\neg\neg A \supset A)$; $\neg\neg\neg A \supset \neg A$; $\neg(A \mathbin{\&} \neg A)$; $(\neg A \vee B) \supset (A \supset B)$; $\neg(A \vee B) \supset (\neg A \mathbin{\&} \neg B)$;
   $(\neg A \mathbin{\&} \neg B) \supset \neg(A \vee B)$; $(\neg A \vee \neg B) \supset \neg(A \mathbin{\&} B)$;
   $(A \supset B) \supset (\neg B \supset \neg A)$; $(A \supset \neg B) \supset (B \supset \neg A)$.

Глава 5

Псевдобулевы алгебры

§5.1. Логические матрицы и оценки

Логической матрицей назовем набор

$$\mathbf{M} = \langle M, 1, \cdot, +, \to, \sim \rangle,$$

где M — непустое множество (*носитель* матрицы $\mathbf{M}$), $1 \in M$, $\sim$ — одноместная, а $\cdot$, $+$, $\to$ — двухместные операции на M, причем для любых элементов $x, y \in M$ выполняются условия:

1) если $1 \to x = 1$, то $x = 1$;

2) если $x \to y = y \to x = 1$, то $x = y$.

В дальнейшем элементы множества M будем называть *элементами логической матрицы* $\mathbf{M}$ и иногда будем писать $x \in \mathbf{M}$ вместо $x \in M$.

Оценкой в логической матрице $\mathbf{M}$ называется произвольная функция, которая каждой пропозициональной переменной сопоставляет некоторый элемент множества M. Всякую оценку f можно продолжить на множество всех пропозициональных формул, положив

$$f(A \,\&\, B) = f(A) \cdot f(B);$$

$$f(A \vee B) = f(A) + f(B);$$

$$f(A \supset B) = f(A) \to f(B);$$

$$f(\neg A) =\sim f(A).$$

Будем говорить, что формула A *истинна* в логической матрице $\mathbf{M}$, если $f(A) = 1$, какова бы ни была оценка f в $\mathbf{M}$. Если же для некоторой оценки f имеет место $f(A) \neq 1$, то говорят, что формула A *опровергается* в матрице $\mathbf{M}$, а матрица $\mathbf{M}$ называется *контрмоделью* для этой формулы.

Логическая матрица $\mathbf{M}$ называется *моделью* данного пропозиционального исчисления, если все формулы, выводимые в этом исчислении, истинны в матрице $\mathbf{M}$. Логическая матрица называется *точной моделью* данного исчисления, если в этом исчислении выводимы те и только те формулы, которые истинны в этой матрице.

Теорема 28. *Пусть пропозициональное исчисление таково, что его единственным правилом вывода является МР. Тогда логическая матрица* $\mathbf{M}$ *является моделью этого исчисления, если и только если все его аксиомы истинны в* $\mathbf{M}$.

Доказательство. Пусть логическая матрица $\mathbf{M}$ является моделью данного пропозиционального исчисления. Поскольку все аксиомы этого исчисления выводимы в нем, они истинны в $\mathbf{M}$ по определению модели. Обратно, пусть в логической матрице $\mathbf{M}$ истинны все аксиомы пропозиционального исчисления, в котором единственным правилом вывода является МР, и пусть $A_1, \ldots, A_n$ — некоторый вывод в этом исчислении. Индукцией по i докажем, что для любого $i = 1, \ldots, n$ формула A_i истинна в матрице $\mathbf{M}$. При $i = 1$ формула A_i является аксиомой и истинна в $\mathbf{M}$ по условию. Пусть для некоторого $k \le n$ каждая из формул A_i при $i < k$ истинна в $\mathbf{M}$. Докажем, что формула A_k также истинна в $\mathbf{M}$. Если формула A_k является аксиомой, то она истинна в $\mathbf{M}$ по условию. Если же A_k получена по правилу МР из формул A_l и A_m, где $l, m < k$, причем A_m имеет вид $A_l \supset A_k$, то по индуктивному предположению для любой оценки f имеет место $f(A_l) = 1$ и $f(A_m) = f(A_l) \to f(A_k) = 1 \to f(A_k) = 1$. Отсюда и из определения логической матрицы следует, что $f(A_k) = 1$ для любой оценки f, т. е. формула A_k истинна в матрице $\mathbf{M}$. Таким образом, любая формула, выводимая в данном исчислении, истинна в матрице $\mathbf{M}$. Значит, $\mathbf{M}$ является моделью этого исчисления. $\square$

Моделью ИИВ является, например, логическая матрица

$$\mathbf{M}_1 = \left\langle \left\{0, \frac{1}{2}, 1\right\}, \cdot, +, \to, \sim \right\rangle,$$

где

$$x \cdot y = \min(x, y);\ x + y = \max(x, y);$$

$$x \to y = \begin{cases} 1, & \text{если } x \le y, \\ y, & \text{если } x > y; \end{cases} \quad \sim x = x \to 0 = \begin{cases} 1, & \text{если } x = 0, \\ 0, & \text{если } x \ne 0. \end{cases}$$

Предложение 9. *Формула* $(P \supset Q) \supset ((\neg P \supset Q) \supset Q)$ *невыводима в ИИВ.*

Доказательство. Рассмотрим такую оценку f в $\mathbf{M}_1$, что

$$f(P) = f(Q) = \frac{1}{2}.$$

Вычисления показывают (см. упражнение 1), что значение рассматриваемой формулы при этой оценке равно $\frac{1}{2}$, следовательно, эта формула не истинна в модели $\mathbf{M}_1$ ИИВ и потому невыводима в этом исчислении. $\square$

Следствие 2. *Формула* $(P \supset Q) \supset ((\neg P \supset Q) \supset Q)$ *невыводима в исчислении Колмогорова.*

Доказательство. Утверждение следует из предложения 9 и того факта, что всякая формула, выводимая в исчислении Колмогорова, выводима и в ИИВ. $\square$

Таким образом, аксиома Г6 исчисления Гильберта невыводима в исчислении Колмогорова.

Заметим также, что при любой такой оценке f в $\mathbf{M}_1$, что $f(P) = \frac{1}{2}$, $f(Q) = 1$, формула

$$(\neg P \supset \neg Q) \supset (Q \supset P)$$

принимает значение $\frac{1}{2}$; при таких оценках формулы $P \vee \neg P$ и $\neg\neg P \supset P$ также принимают значение $\frac{1}{2}$. Значит, все эти формулы также невыводимы в итуиционистском исчислении высказываний.

Вот еще один пример модели ИИВ:

$$\mathbf{M}_2 = \langle \{0,1\}^2 \cup \{1\}, 1, \cdot, +, \rightarrow, \sim \rangle,$$

где

$$1 \cdot a = a \cdot 1 = a;\ 1 + a = a + 1 = 1;\ 1 \rightarrow a = a;\ a \rightarrow 1 = 1;\ \sim 1 = \langle 0, 0 \rangle$$

(здесь a — произвольный элемент матрицы $\mathbf{M}_2$), а операции над элементами вида $\langle a, b \rangle$, где $a, b \in \{0,1\}$, определяются так:

$$\langle a_1, b_1 \rangle \cdot \langle a_2, b_2 \rangle = \langle \min(a_1, a_2), \min(b_1, b_2) \rangle;$$

$$\langle a_1, b_1 \rangle + \langle a_2, b_2 \rangle = \langle \max(a_1, a_2), \max(b_1, b_2) \rangle;$$

$$\sim \langle a,b\rangle = \begin{cases} 1, \text{ если } a=b=0; \\ \langle 1-a, 1-b\rangle, \text{ если } a\neq 0 \text{ или } b\neq 0 \end{cases}$$

$$\langle a_1,b_1\rangle \to \langle a_2,b_2\rangle = \gamma(\sim \langle a_1,b_1\rangle + \langle a_2,b_2\rangle),$$

где $\gamma(x) = \begin{cases} 1, \text{ если } x = \langle 1,1\rangle, \\ x, \text{ если } x \neq \langle 1,1\rangle. \end{cases}$

Нетрудно проверить, например, что если $f(P) = \langle 0,1\rangle$, то при такой оценке f формула $\neg P \vee \neg\neg P$ принимает значение $\langle 1,1\rangle$. Значит, она не истинна в модели $\mathbf{M}_2$ ИИВ и невыводима в этом исчислении.

§5.2. Решетки и псевдобулевы алгебры

Пусть на непустом множестве M задан частичный порядок $\leq$. Это означает, что выполняются следующие аксиомы:

A1. $\forall a\,[a \leq a]$ (*рефлексивность*);

A2. $\forall a,b\,[a \leq b \,\&\, b \leq a \Rightarrow a = b]$ (*антисимметричность*);

A3. $\forall a,b,c\,[a \leq b \,\&\, b \leq c \Rightarrow a \leq c]$ (*транзитивность*).

Пусть A — непустое подмножество частично упорядоченного множества M. Элемент $a \in A$ называется *наибольшим* элементом множества A, если $(\forall x \in A)\, x \leq a$. Элемент $a \in A$ называется *наименьшим* элементом множества A, если $(\forall x \in A)\, a \leq x$. Нетрудно доказать, что в любом непустом множестве содержится не более чем один наибольший элемент и не более чем один наименьший элемент (см. упражнение 2).

Верхней гранью пары элементов a, b частично упорядоченного множества M называется всякий такой элемент c, что $a \leq c$ и $b \leq c$. Если множество всех верхних граней пары элементов a, b непусто и содержит наименьший элемент, то этот элемент называется *точной верхней гранью* пары a, b и обозначается $a + b$. *Нижней гранью* пары элементов a, b частично упорядоченного множества M называется всякий такой элемент c, что $c \leq a$ и $c \leq b$. Если множество всех нижних граней пары элементов a, b непусто и содержит наибольший элемент, то этот элемент называется *точной нижней гранью* пары a, b и обозначается $a \cdot b$.

Частично упорядоченное множество M, в котором для любой пары элементов a, b существуют их точная верхняя грань $a + b$ и точная нижняя грань $a \cdot b$, называется *решеткой*. Таким образом, в каждой решетке определены двухместные операции $+$ и $\cdot$, причем выполняются условия A1 – A3, а также следующие аксиомы:

A4. $\forall a, b\,[a \leq a + b]$;
A5. $\forall a, b\,[b \leq a + b]$;
A6. $\forall a, b, c\,[a \leq c \,\&\, b \leq c \Rightarrow a + b \leq c]$;
A7. $\forall a, b\,[a \cdot b \leq a]$;
A8. $\forall a, b\,[a \cdot b \leq b]$;
A9. $\forall a, b, c\,[c \leq a \,\&\, c \leq b \Rightarrow c \leq a \cdot b]$.

Предложение 10. *В каждой решетке для любых элементов a, b, c, d выполняются следующие условия:*

1. *$a+b = b+a$; $a \cdot b = b \cdot a$; $a+(b+c) = (a+b)+c$; $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ (коммутативность и ассоциативность операций $+$ и $\cdot$);*

2. *если $a \leq b$ и $c \leq d$, то $a + c \leq b + d$ и $a \cdot c \leq b \cdot d$ (монотонность операций $+$ и $\cdot$);*

3. *$a \cdot (a + b) = a$; $(a \cdot b) + b = b$ (законы поглощения).*

Доказательство. Докажем коммутативность операции $+$. В силу A5 $a \leq b + a$, в силу A4 $b \leq b + a$. Отсюда и из A6 получаем

$$a + b \leq b + a. \tag{5.1}$$

В силу A5 $b \leq a + b$, в силу A4 $a \leq a + b$. Отсюда и из A6 получаем

$$b + a \leq a + b. \tag{5.2}$$

Из (5.1), (5.2) и A2 получаем $a + b = b + a$.

Докажем коммутативность операции $\cdot$. В силу A8 $a \cdot b \leq b$, в силу A7 $a \cdot b \leq a$. Отсюда и из A9 получаем

$$a \cdot b \leq b \cdot a. \tag{5.3}$$

Совершенно аналогично доказывается

$$b \cdot a \leq a \cdot b. \tag{5.4}$$

Из (5.3), (5.4) и A2 получаем $a \cdot b = b \cdot a$.

Докажем ассоциативность оперции $+$. В силу А4

$$a \leq a + b$$

и

$$a + b \leq (a + b) + c.$$

Отсюда и из А3 получаем

$$a \leq (a + b) + c. \tag{5.5}$$

В силу А5 $b \leq a + b$, а так как $a + b \leq (a + b) + c$, то из А3 получаем

$$b \leq (a + b) + c. \tag{5.6}$$

В силу А5 $c \leq (a + b) + c$. Отсюда и из (5.6) и А6 получаем $b + c \leq (a + b) + c$. Наконец, из этого равенства и (5.5) в силу А6 получаем

$$a + (b + c) \leq (a + b) + c. \tag{5.7}$$

Аналогично доказывается, что $(a + b) + c \leq a + (b + c)$. Отсюда и из (5.7) в силу А2 получается $(a + b) + c = a + (b + c)$.

Ассоциативность операции $\cdot$ доказывается аналогично. Таким образом, утверждение 1) можно считать доказанным.

Докажем монотонность операции $+$. Пусть $a \leq b$, $c \leq d$. Так как в силу А4 и А5 $b \leq b + d$ и $d \leq b + d$, то по свойству транзитивности $a \leq b + d$ и $c \leq b + d$. Отсюда в силу А6 получаем $a + c \leq b + d$.

Аналогично доказывается монотонность операции $\cdot$ (см. упражнение 3). Утверждение 2) также можно считать доказанным.

Докажем закон поглощения $a \cdot (a + b) = a$. В силу А7

$$a \cdot (a + b) \leq a. \tag{5.8}$$

В силу А1 $a \leq a$, а в силу А4 $a \leq a + b$. Отсюда и из А9 вытекает

$$a \leq a \cdot (a + b). \tag{5.9}$$

Из 5.8 и 5.9 в силу А2 вытекает $a \cdot (a + b) = a$.

Аналогично доказывается закон поглощения $(a \cdot b) + b = b$. Таким образом, и утверждение 3) можно считать доказанным. $\square$

Решетка называется *дистрибутивной*, если для любых ее элементов a, b, c выполняется условие $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$.

Предложение 11. *В каждой дистрибутивной решетке для любых элементов a, b, c выполняется условие*

$$a + (b \cdot c) = (a + b) \cdot (a + c).$$

Доказательство. В силу дистрибутивности имеем

$$(a + b) \cdot (a + c) = ((a + b) \cdot a) + ((a + b) \cdot c)). \tag{5.10}$$

В силу закона поглощения и дистрибутивности

$$((a + b) \cdot a) + ((a + b) \cdot c)) = a + ((a \cdot c) + (b \cdot c)). \tag{5.11}$$

В силу ассоциативности

$$a + ((a \cdot c) + (b \cdot c)) = (a + (a \cdot c)) + (b \cdot c). \tag{5.12}$$

Наконец, в силу закона поглощения

$$(a + (a \cdot c)) + (b \cdot c) = a + (b \cdot c). \tag{5.13}$$

Из равенств (5.10)–(5.13) вытекает доказываемое утверждение. $\square$

Псевдодополнением элемента a относительно элемента b в данной решетке называется наибольший элемент в множестве $\{c \mid a \cdot c \leq b\}$. Псевдодополнение элемента a относительно b, если оно существует, обозначается $a \to b$. Решетка, в которой для любых элементов a и b существует элемент $a \to b$, называется *импликативной решеткой*. Таким образом, в каждой импликативной решетке определена двухместная операция $\to$, выполняются условия A1 – A9, а также следующие аксиомы:

A10. $\forall a, b\, [a \cdot (a \to b) \leq b]$;

A11. $\forall a, b, c\, [a \cdot c \leq b \Rightarrow c \leq a \to b]$.

Предложение 12. *В каждой импликативной решетке есть наибольший элемент.*

Доказательство. Пусть a — произвольный элемент данной импликативной решетки. Докажем, что $a \to a$ — наибольший элемент в данной решетке. Пусть b — произвольный элемент решетки. Тогда в силу A8 $b \cdot a \leq a$. Отсюда и из A11 получаем $b \leq (a \to a)$, что и требовалось доказать. $\square$

Через 1 обозначим наибольший элемент импликативной решетки.

Теорема 29. *Каждая импликативная решетка является дистрибутивной решеткой.*

Доказательство. Пусть a, b, c — произвольные элементы данной импликативной решетки. Докажем, что

$$a \cdot (b + c) = a \cdot b + a \cdot c. \tag{5.14}$$

Пусть $d = a \cdot b + a \cdot c$. Тогда $a \cdot b \leq d$ в силу A4. Отсюда следует $b \leq a \to d$ в силу A11. Аналогично доказываются неравенства $a \cdot c \leq d$ и $c \leq a \to d$. Тогда $b + c \leq a \to d$ в силу A6. Отсюда и из A1 получаем в силу утверждения 2 из предложения 4, что

$$a \cdot (b + c) \leq a \cdot (a \to d),$$

и далее в силу A10 $a \cdot (a \to d) \leq d$. Отсюда в силу транзитивности отношения $\leq$ получаем

$$a \cdot (b + c) \leq d. \tag{5.15}$$

Далее, так как $b \leq b + c$, то $a \cdot b \leq a \cdot (b + c)$, а так как $c \leq b + c$, то $a \cdot c \leq a \cdot (b + c)$. Отсюда получаем в силу A6

$$d = a \cdot b + a \cdot c \leq a \cdot (b + c). \tag{5.16}$$

Из (5.15) и (5.16) получаем (5.14). □

Предложение 13. *В каждой импликативной решетке выполняются следующие условия:*

1. $\forall a, b, c\, [a \leq b \Rightarrow b \to c \leq a \to c]$;
2. $\forall a, b, c\, [a \leq b \Rightarrow c \to a \leq c \to b]$;
3. $\forall a, b, c\, [a \leq b \to c \Rightarrow a \cdot b \leq c]$;
4. $\forall a, b\, [a \to b = 1 \Leftrightarrow a \leq b]$;
5. $\forall a, b\, [b \leq a \to b]$;
6. $\forall a, b, c\, [a \to b \leq ((a \to (b \to c)) \to (a \to c)]$;
7. $\forall a, b\, [a \leq b \to a \cdot b]$;
8. $\forall a, b, c\, [a \to c \leq (b \to c) \to (a + b \to c)]$.

Доказательство. 1. Пусть a, b, c — произвольные элементы данной импликативной решетки, причем $a \leq b$. Тогда в силу монотонности операции $\cdot$ и A10 имеем $a \cdot (b \to c) \leq b \cdot (b \to c) \leq c$, а значит $(b \to c) \cdot a \leq c$, откуда получаем $b \to c \leq a \to c$ в силу A11.

2. Пусть a, b, c — произвольные элементы данной импликативной решетки, причем $a \leq b$. Тогда в силу A10 имеем $(c \to a) \cdot c \leq a \leq b$, откуда получаем $c \to a \leq c \to b$ в силу A11.

3. Пусть a, b, c — произвольные элементы данной импликативной решетки. Если $a \leq b \to c$, то в силу монотонности операции $\cdot$ и аксиомы A10 имеем $a \cdot b \leq b \cdot (b \to c) \leq c$, т. е. $a \cdot b \leq c$. Обратно, если $a \cdot b \leq c$, то $a \leq b \to c$ в силу A11.

4. Пусть a, b — произвольные элементы данной импликативной решетки. Тогда, если $a \to b = 1$, то $a \cdot 1 \leq b$ в силу A10, т. е. $a \leq b$. Обратно, если $a \leq b$, то $a \cdot 1 \leq b$, и в силу A11 получаем $1 \leq a \to b$, откуда следует $a \to b = 1$, ибо 1 — наибольший элемент.

5. Пусть a, b — произвольные элементы. Так как $b \cdot a \leq b$, то в силу A11 получаем $b \leq a \to b$.

6. Пусть a, b, c — произвольные элементы. В силу A11 достаточно доказать, что

$$(a \to b) \cdot (a \to (b \to c)) \leq a \to c,$$

а для этого достаточно доказать $(a \to b) \cdot (a \to (b \to c)) \cdot a \leq c$. Последнее утверждение вытекает из следующих неравенств:

$$(a \to b) \cdot (a \to (b \to c)) \cdot a \leq (a \to b) \cdot a \leq b \tag{5.17}$$

в силу коммутативности операции $\cdot$, а также аксиом A7 и A10;

$$(a \to b) \cdot (a \to (b \to c)) \cdot a \leq (a \to (b \to c)) \cdot a \leq b \to c \tag{5.18}$$

в силу аксиом A8 и A10;

$$(a \to b) \cdot (a \to (b \to c)) \cdot a \leq b \cdot (b \to c) \leq c \tag{5.19}$$

в силу аксиом A9 и A10.

7. Пусть a, b — произвольные элементы. Так как $a \cdot b \leq a \cdot b$, то в силу A11 получаем $a \leq b \to a \cdot b$, что и требовалось.

8. Пусть a, b, c — произвольные элементы. Очевидны следующие неравенства:

$$a \cdot (a \to c) \cdot (b \to c) \leq a \cdot (a \to c) \leq c \tag{5.20}$$

в силу в аксиом A7 и A10;

$$b \cdot (a \to c) \cdot (b \to c) \le b \cdot (b \to c) \le c \tag{5.21}$$

в силу коммутативности операции $\cdot$ и аксиом A8 и A10. Из (5.20) и (5.21) в силу коммутативности операции $\cdot$ и A11 вытекают неравенства

$$a \le (a \to c) \cdot (b \to c) \to c \tag{5.22}$$

и

$$b \le (a \to c) \cdot (b \to c) \to c. \tag{5.23}$$

Из (5.22) и (5.23) в силу аксиомы A6 получаем

$$a + b \le (a \to c) \cdot (b \to c) \to c,$$

откуда в силу 3 имеем

$$(a + b) \cdot (a \to c) \cdot (b \to c) \le c$$

и далее в силу 3

$$(a \to c) \cdot (b \to c) \le a + b \to c$$

и

$$(a \to c) \le (b \to c) \to (a + b \to c),$$

что и требовалось. □

Импликативная решетка называется *псевдобулевой алгеброй* или *алгеброй Гейтинга*, если в ней есть наименьший элемент, который мы будем обозначать 0. *Псевдодополнением* элемента a данной псевдобулевой алгебры называется элемент $a \to 0$, обозначаемый $\sim a$. Таким образом, в каждой псевдобулевой алгебре есть элемент 0 и определена одноместная операция $\sim$, причем выполняются условия A1 – A11, а также следующие аксиомы:

A12. $\forall a\, [0 \le a]$;

A13. $\forall a\, [\sim a = a \to 0]$.

Заметим, что в любой псевдобулевой алгебре $\sim a = 1$ тогда и только тогда, когда $a = 0$. Действительно, из аксиомы A13 получаем, что ~ 0 есть элемент $0 \to 0$, который, как мы установили ранее, равен 1. Обратно, пусть $\sim a = 1$, т. е. $a \to 0 = 1$. Но тогда из аксиомы A10 следует, что $a \le 0$, т. е. $a = 0$.

Если в псевдобулевой алгебре выполняется условие

$$\forall a\, [a + \sim a = 1],$$

то такая алгебра называется *булевой алгеброй*.

§5.3. Операции над псевдобулевыми алгебрами

Рассмотрим некоторые способы построения новых псевдобулевых алгебр из уже имеющихся.

Прямые произведения псевдобулевых алгебр. Пусть A и B — непустые множества с заданными на них частичными порядками $\le_A$ и $\le_B$ соответственно. На прямом произведении $A \times B$ этих множеств определим бинарное отношение $\le$, для произвольных пар $\langle a_1, b_1\rangle$ и $\langle a_2, b_2\rangle$ из $A \times B$ положив

$$[\langle a_1, b_1\rangle \le \langle a_2, b_2\rangle] \leftrightharpoons [a_1 \le_A a_2 \,\&\, b_1 \le_B b_2].$$

Множество $A \times B$ с таким отношением $\le$ назовем *прямым произведением* частично упорядоченных множеств A и B.

Теорема 30. *Если частично упорядоченные множества A и B являются псевдобулевыми алгебрами, то их прямое произведение также является псевдобулевой алгеброй.*

Доказательство. Проверим, что $\le$ — частичный порядок.

Пусть $\langle a, b\rangle \in A \times B$. Так как для A и B выполнена аксиома A1, то $a \le_A a$ и $b \le_B b$. Отсюда следует $\langle a, b\rangle \le \langle a, b\rangle$ в силу определения $\le$. Таким образом, аксиома A1 выполнена.

Пусть $\langle a_1, b_1\rangle$ и $\langle a_2, b_2\rangle$ — элементы из $A \times B$, причем $\langle a_1, b_1\rangle \le \langle a_2, b_2\rangle$, т. е. $a_1 \le_A a_2$ и $b_1 \le_B b_2$, и $\langle a_2, b_2\rangle \le \langle a_1, b_1\rangle$, т. е. $a_2 \le_A a_1$ и $b_2 \le_B b_1$. Так как для A и B выполнена аксиома A2, то отсюда следует $a_1 = a_2$, $b_1 = b_2$, т. е. $\langle a_1, b_1\rangle = \langle a_2, b_2\rangle$. Таким образом, аксиома A2 выполнена.

Пусть $\langle a_1, b_1\rangle$, $\langle a_2, b_2\rangle$ и $\langle a_3, b_3\rangle$ — элементы из $A \times B$, причем $\langle a_1, b_1\rangle \le \langle a_2, b_2\rangle$, т. е. $a_1 \le_A a_2$ и $b_1 \le_B b_2$, и $\langle a_2, b_2\rangle \le \langle a_3, b_3\rangle$, т. е. $a_2 \le_A a_3$ и $b_2 \le_B b_3$. Так как для A и B выполнена аксиома A3, то отсюда следует $a_1 \le_A a_3$, $b_1 \le_B b_3$, т. е. $\langle a_1, b_1\rangle \le \langle a_3, b_3\rangle$. Таким образом, аксиома A3 выполнена.

Покажем, что $A \times B$ является решеткой. Так как A и B — решетки, в них определены операции $+$ и $\cdot$, удовлетворяющие аксиомам A4 – A9. Для произвольных элементов $\langle a_1, b_1\rangle$ и $\langle a_2, b_2\rangle$ множества $A \times B$ положим $\langle a_1, b_1\rangle + \langle a_2, b_2\rangle = \langle a_1 + a_2, b_1 + b_2\rangle$; $\langle a_1, b_1\rangle \cdot \langle a_2, b_2\rangle = \langle a_1 \cdot a_2, b_1 \cdot b_2\rangle$. Проверим, что для таких операций $+$ и $\cdot$ выполняются аксиомы A4 – A9.

Пусть $\langle a_1, b_1\rangle$ и $\langle a_2, b_2\rangle$ — элементы из $A\times B$. Так как для A и B выполнена аксиома A4, то $a_1 \leq_A a_1 + a_2$, $b_1 \leq_B b_1 + b_2$, т. е. $\langle a_1, b_1\rangle \leq \langle a_1 + a_2, b_1 + b_2\rangle = \langle a_1, b_1\rangle + \langle a_2, b_2\rangle$. Таким образом, аксиома A4 выполнена.

Аналогично доказывается, что выполняется аксиома A5.

Пусть $\langle a_1, b_1\rangle$, $\langle a_2, b_2\rangle$ и $\langle a_3, b_3\rangle$ — произвольные элементы из $A \times B$, причем $\langle a_1, b_1\rangle \leq \langle a_3, b_3\rangle$, т. е. $a_1 \leq_A a_3$ и $b_1 \leq_B b_3$, и $\langle a_2, b_2\rangle \leq \langle a_3, b_3\rangle$, т. е. $a_2 \leq_A a_3$ и $b_2 \leq_B b_3$. Так как для A и B выполнена аксиома A6, то отсюда следует $a_1 + a_2 \leq_A a_3$, $b_1 + b_2 \leq_B b_3$, т. е. $\langle a_1, b_1\rangle + \langle a_2, b_2\rangle = \langle a_1 + a_2, b_1 + b_2\rangle \leq \langle a_3, b_3\rangle$. Таким образом, аксиома A6 выполнена.

Пусть $\langle a_1, b_1\rangle$ и $\langle a_2, b_2\rangle$ — элементы из $A \times B$. Так как для A и B выполнена аксиома A7, то $a_1 \cdot a_2 \leq_A a_1$, $b_1 \cdot b_2 \leq_B b_2$, т. е. $\langle a_1, b_1\rangle \cdot \langle a_2, b_2\rangle = \langle a_1 \cdot a_2, b_1 \cdot b_2\rangle \leq \langle a_1, b_1\rangle$. Таким образом, аксиома A7 выполнена.

Аналогично доказывается, что выполняется аксиома A8.

Пусть $\langle a_1, b_1\rangle$, $\langle a_2, b_2\rangle$ и $\langle a_3, b_3\rangle$ — элементы из $A\times B$, причем $\langle a_3, b_3\rangle \leq \langle a_1, b_1\rangle$, т. е. $a_3 \leq_A a_1$ и $b_3 \leq_B b_1$, и $\langle a_3, b_3\rangle \leq \langle a_2, b_2\rangle$, т. е. $a_3 \leq_A a_2$ и $b_3 \leq_B b_2$. Так как для A и B выполнена аксиома A9, то отсюда следует $a_3 \leq_A a_1 \cdot a_2$, $b_3 \leq_B b_1 \cdot b_2$, т. е.

$$\langle a_3, b_3\rangle \leq \langle a_1 \cdot a_2, b_1 \cdot b_2\rangle = \langle a_1, b_1\rangle \cdot \langle a_2, b_2\rangle.$$

Таким образом, аксиома A9 выполнена.

Покажем, что $A\times B$ является импликативной решеткой. Так как A и B — импликативные решетки, в них определена операция $\to$, удовлетворяющая аксиомам A10 и A11. Для произвольных элементов $\langle a_1, b_1\rangle$ и $\langle a_2, b_2\rangle$ из — множества $A\times B$ положим $\langle a_1, b_1\rangle \to \langle a_2, b_2\rangle = \langle a_1 \to a_2, b_1 \to b_2\rangle$. Проверим, что для такой операции $\to$ выполняются аксиомы A10 и A11.

Пусть $\langle a_1, b_1\rangle$ и $\langle a_2, b_2\rangle$ — произвольные элементы множества $A \times B$. Так как для множеств A и B выполнена аксиома A10, то $a_1 \cdot (a_1 \to a_2) \leq_A a_2$, $b_1 \cdot (b_1 \to b_2) \leq_B b_2$. Отсюда следует

$$\langle a_1, b_1\rangle \cdot (\langle a_1, b_1\rangle \to \langle a_2, b_2\rangle) =$$

$$= \langle a_1 \cdot (a_1 \to a_2), b_1 \cdot (b_1 \to b_2)\rangle \leq \langle a_2, b_2\rangle.$$

Таким образом, аксиома A10 выполнена.

Пусть $\langle a_1, b_1\rangle$, $\langle a_2, b_2\rangle$ и $\langle a_3, b_3\rangle$ — элементы множества $A\times B$, причем $\langle a_1, b_1\rangle \cdot \langle a_3, b_3\rangle \leq \langle a_2, b_2\rangle$, т. е. $a_1 \cdot a_3 \leq_A a_2$, $b_1 \cdot b_3 \leq_B b_2$.

Так как для A и B выполнена аксиома А11, то отсюда следует $a_3 \leq_A a_1 \to a_2$, $b_3 \leq_B b_1 \to b_2$, т. е.

$$\langle a_3, b_3 \rangle \leq \langle a_1 \to a_2, b_1 \to b_2 \rangle = \langle a_1, b_1 \rangle \to \langle a_2, b_2 \rangle.$$

Таким образом, аксиома А11 выполнена.

Покажем, что $A \times B$ является псевдобулевой алгеброй. Так как A и B — псевдобулевы алгебры, в них есть наименьшие элементы 0_A и 0_B и определена операция $\sim$, так что выполняются аксиомы А12 и А13. Пусть $0 = \langle 0_A, 0_B \rangle$ и $\sim \langle a, b \rangle = \langle \sim_A a, \sim_B b \rangle$ для любого $\langle a, b \rangle \in A \times B$. Проверим, что для элемента 0 и операции $\sim$ выполняются аксиомы А12 и А13.

Пусть $\langle a, b \rangle \in A \times B$. Так как для A и B выполнена аксиома А12, то $0_A \leq_A a$, $0_B \leq_B b$, т. е. $0 = \langle 0_A, 0_B \rangle \leq \langle a, b \rangle$. Таким образом, аксиома А12 выполнена.

Пусть $\langle a, b \rangle \in A \times B$. Так как для A и B выполнена аксиома А13, то $\sim_A a = a \to 0_A$ и $\sim_B b = b \to 0_B$, т. е.

$$\sim \langle a, b \rangle = \langle \sim_A a, \sim_B b \rangle = \langle a \to 0_A, b \to 0_B \rangle =$$

$$= \langle a, b \rangle \to \langle 0_A, 0_B \rangle = \langle a, b \rangle \to 0.$$

Таким образом, аксиома А13 выполнена. □

Прямое произведение $A_1 \times \ldots \times A_n$ любого конечного числа псевдобулевых алгебр $A_1, \ldots, A_n$ определяется аналогично и оказывается псевдобулевой алгеброй. В частности, для любой псевдобулевой алгебры A и любого натурального $n \geq 2$ можно построить псевдобулеву алгебру A^n как алгебру $A_1 \times \ldots \times A_n$, где $A_1 = \ldots = A_n = A$.

Операция Г. Пусть множество A с отношением $\leq_A$ является псевдобулевой алгеброй, и пусть $\omega \notin A$. На множестве $A \cup \{\omega\}$ определим отношение $\leq$, положив для любых $a, b \in A$: $a \leq \omega$, если $a \neq 1$; $a \leq b \rightleftharpoons a \leq_A b$; $\omega \leq 1$.

Очевидно, что так определенное отношение $\leq$ является частичным порядком, при этом 1 — наибольший элемент, а если $|A| > 1$, то 0 — наименьший элемент.

Для каждого $a \in A$ положим $\gamma(a) = a$, если $a \neq 1$, и $\gamma(a) = \omega$, если $a = 1$. Зададим на множестве $B = A \cup \{\omega\}$ операции $+$, $\cdot$, $\to$, $\sim$ следующими таблицами:

$x \to y$	$y = 1$	$y = \gamma(v)$
$x = 1$	1	$\gamma(x \to_A v)$
$x = \gamma(u)$	1	$u \to_A v$

$x \cdot y$	$y = 1$	$y = \gamma(v)$
$x = 1$	1	$\gamma(x \cdot_A v)$
$x = \gamma(u)$	$\gamma(u \cdot_A y)$	$\gamma(u \cdot_A v)$

$x + y$	$y = 1$	$y = \gamma(v)$
$x = 1$	1	1
$x = \gamma(u)$	1	$\gamma(u +_A v)$

$$\sim x = \begin{cases} \gamma(\sim_A x), & \text{для } x = 1, \\ \sim_A u, & \text{для } x = \gamma(u). \end{cases}$$

Множество $A \cup \{\omega\}$ с операциями $+$, $\cdot$, $\to$, $\sim$ является псевдобулевой алгеброй. Обозначим ее $\Gamma(A)$. Заметим, что в ней

$$\forall a, b\, [a + b = 1 \Rightarrow (a = 1 \vee b = 1)]. \tag{5.24}$$

Алгебры, в которых выполняется это условие, играют существенную роль при доказательстве следующего факта, впервые сформулированного К. Гёделем [18]: дизъюнкция $A \vee B$ выводима в ИИВ тогда и только тогда, когда одна из формул A и B выводима в ИИВ (это будет доказано в § 6.6). Следуя В. А. Янкову [7], псевдобулеву алгебру, удовлетворяющую условию (5.24), будем называть *гёделевой*. Заметим, что если в псевдобулевой алгебре существует элемент, наибольший среди элементов, отличных от 1 (такой элемент будем называть *гёделевым*), то эта алгебра является гёделевой. Если гёделев элемент существует, то он единственный. Таким образом, всякая алгебра вида $\Gamma(A)$ является гёделевой, причем ω — ее гёделев элемент. Нетрудно доказать, что в любой конечной гёделевой псевдобулевой алгебре существует гёделев элемент.

Определим последовательность псевдобулевых алгебр J_n следующим образом. Пусть $J_0 = \{0, 1\}$ — двухэлементная псевдобулева алгебра. Если алгебра J_{n-1} уже определена, положим $J_n = \Gamma(J_{n-1}^n)$. При этом в качестве гёделева элемента алгебры J_n возьмем число $n + 1$. Таким образом, J_1 — это трехэлементная псевдобулева алгебра с элементами $0 \leq 2 \leq 1$, а алгебра J_2 содержит 10 элементов: (0,0), (0,2), (0,1), (2,0), (2,2), (2,1), (1,0), (1,2), (1,1), 3, причем элемент (1,1) является наибольшим, а элемент 3 — наибольший среди всех отличных от (1,1) элементов. Алгебры из последовательности J_n были введены С. Яськовским [22] и называются *алгебрами Яськовского*.

§5.4. Гомоморфизмы псевдобулевых алгебр

Пусть A и B — псевдобулевы алгебры. Отображение
$$\varphi : A \to B$$
называется *гомоморфизмом* из A в B, если для любых $a, b \in A$ выполняются условия: $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$; $\varphi(a+b) = \varphi(a)+\varphi(b)$; $\varphi(a \to b) = \varphi(a) \to \varphi(b)$; $\varphi(\sim a) =\sim \varphi(a)$. Если при этом φ — взаимно-однозначное отображение, то φ называется *изоморфизмом* алгебр A и B.

Заметим, что если φ — гомоморфизм, то $\varphi(1_A) = 1_B$. Действительно, $\varphi(1_A) = \varphi(a \to a) = \varphi(a) \to \varphi(a) = 1_B$. Отсюда следует, что для любых $a, b \in A$ выполняется условие
$$a \leq b \Rightarrow \varphi(a) \leq \varphi(b).$$
Действительно, если $a \leq b$, то $a \to b = 1_A$. Тогда
$$\varphi(a) \to \varphi(b) = \varphi(a \to b) = \varphi(1_A) = 1_B,$$
значит, $\varphi(a) \leq \varphi(b)$.

Пусть φ — гомоморфизм алгебры A *на* алгебру B. В этом случае будем говорить, что B — *гомоморфный образ* алгебры A. Пусть f — оценка в алгебре B. Тогда можно задать такую оценку g в алгебре A, что $\varphi(g(P_i)) = f(P_i)$ для любой переменной P_i. Будем говорить, что оценка g *согласована* с f и φ.

Предложение 14. *Пусть φ — гомоморфизм псевдобулевой алгебры A на псевдобулеву алгебру B, f — оценка в B, а g — оценка в A, согласованная с f и φ. Тогда $\varphi(g(F)) = f(F)$ для любой формулы F.*

Доказательство. Индукция по построению F. Если F — переменная, то доказываемое равенство вытекает из согласованности g с f и φ.

Пусть F имеет вид $\neg G$, причем для G доказываемое равенство верно, т. е. $\varphi(g(G)) = f(G)$. Тогда
$$\varphi(g(F)) = \varphi(g(\neg G)) = \varphi(\sim g(G)) =$$
$$=\sim \varphi(g(G)) =\sim f(G) = f(\neg G) = f(F),$$
т. е. доказываемое равенство верно и для F. Пусть F имеет вид $G \,\&\, H$, причем $\varphi(g(G)) = f(G)$, $\varphi(g(H)) = f(H)$. Тогда
$$\varphi(g(F)) = \varphi(g(G \,\&\, H)) = \varphi(g(G) \cdot g(H)) =$$

$$= \varphi(g(G)) \cdot \varphi(g(H)) = f(G) \cdot f(H) = f(G \,\&\, H) = f(F),$$

что и требовалось доказать. Аналогично рассматриваются случаи, когда F имеет вид $G \vee H$ или $G \supset H$. □

Предложение 15. *Если алгебра B — гомоморфный образ алгебры A, и пропозициональная формула F истинна в алгебре A, то F истинна в алгебре B.*

Доказательство. Пусть φ — гомоморфизм алгебры A на алгебру B, и пусть формула F истинна в A. Докажем, что F истинна в B. Пусть f — оценка в B. Докажем, что $f(F) = 1_B$. Рассмотрим оценку g в A, согласованную с f и φ. Тогда в силу предложения 14 выполняется равенство $\varphi(g(F)) = f(F)$. Но $g(F) = 1_A$, следовательно, $f(F) = 1_B$, что и требовалось доказать. □

Пусть A — псевдобулева алгебра. Определим отображение φ алгебры $\Gamma(A)$ на алгебру A так: $\varphi(a) = a$, если $a \in A$; $\varphi(\omega) = 1$. Рутинная проверка показывает, что φ — гомоморфизм $\Gamma(A)$ на A. Из предложения 15 следует, что всякая формула, истинная в $\Gamma(A)$, истинна и в A. Следовательно, если формула F опровергается в A, то она опровергается и в $\Gamma(A)$. Пусть f — такая оценка в A, что $f(F) \neq 1$. Так как $A \subseteq \Gamma(A)$, то f может рассматриваться как оценка g в $\Gamma(A)$. Очевидно, что оценка g согласована с f и φ. В силу предожения 14 $\varphi(g(F)) = f(F)$. Отсюда следует $g(F) \neq 1$. Мы доказали следующее утверждение.

Предложение 16. *Каковы бы ни были псевдобулева алгебра A и пропозициональная формула F, если F опровергается в A оценкой f, то F опровергается в $\Gamma(A)$ той же оценкой.*

Упражнения

1. Найти значение аксиомы Г6 исчисления Гильберта в логической матрице $\mathbf{M}_1$ при оценке $f(P) = f(Q) = \frac{1}{2}$.

2. Доказать, что в любом непустом множестве содержится не более чем один наибольший элемент и не более чем один наименьший элемент.

3. Доказать, что в любой решетке операция $\cdot$ монотонна: если $a \leq b$ и $c \leq d$, то $a \cdot c \leq b \cdot d$.

Глава 6

Исследование ИИВ с помощью псевдобулевых алгебр

§6.1. Псевдобулевы алгебры как модели ИИВ

Предложение 17. *Всякая псевдобулева алгебра является логической матрицей.*

Доказательство. В любой псевдобулевой алгебре есть наибольший элемент 1 и определены двухместные операции $\cdot, +, \to$ и одноместная операция $\sim$. Проверим, что для любых ее элементов x, y выполнены следующие условия из определения логической матрицы:

1) если $1 \to x = 1$, то $x = 1$;

2) если $x \to y = y \to x = 1$, то $x = y$.

Пусть x — элемент данной алгебры, причем $1 \to x = 1$. Тогда в силу аксиомы A10 имеем $1 = 1 \cdot (1 \to x) \leq x$, т. е. $1 \leq x$, а значит, $x = 1$. Условие 1) доказано.

Пусть x, y таковы, что $x \to y = y \to x = 1$. Тогда в силу утверждения 4 из предложения 13 имеем $x \leq y$ и $y \leq x$, что дает $x = y$ в силу аксиомы A2. Таким образом, условие 2) выполнено. □

Следующее утверждение называется *теоремой о корректности* ИИВ относительно псевдобулевых алгебр.

Теорема 31. *Всякая псевдобулева алгебра является моделью ИИВ.*

Доказательство. В силу теоремы 28 достаточно доказать, что все аксиомы ИИВ истинны в любой псевдобулевой алгебре. Пусть A, B, C — произвольные формулы, f — произвольная оценка в некоторой псевдобулевой алгебре M, причем

$$f(A) = a,\ f(B) = b,\ f(C) = c.$$

Тогда имеем:

$$f(A \supset (B \supset A)) = a \to (b \to a) = 1$$

в силу утверждений 5 и 4 из предложения 13, и аксиома И1 истинна в M;

$$f((A \supset B) \supset ((A \supset (B \supset C)) \supset (A \supset C))) =$$
$$= (a \to b) \to ((a \to (b \to c)) \to (a \to c)) = 1$$

в силу утверждений 6 и 4 из предложения 13, и аксиома И2 истинна в M;

$$f(A \,\&\, B \supset A) = a \cdot b \to a = 1$$

в силу аксиомы А7 и утверждения 4 из предложения 13, и аксиома И3 истинна в M;

$$f(A \,\&\, B \supset B) = a \cdot b \to b = 1$$

в силу аксиомы А8 и утверждения 4 из предложения 13, и аксиома И4 истинна в M;

$$f(A \supset (B \supset A \,\&\, B)) = a \to (b \to a \cdot b) = 1$$

в силу утверждений 7 и 4 из предложения 13, и аксиома И5 истинна в M;

$$f(A \supset A \vee B) = a \to a + b = 1$$

в силу аксиомы А4 и утверждения 4 из предложения 13, и аксиома И6 истинна в M;

$$f(B \supset A \vee B) = b \to a + b = 1$$

в силу аксиомы А5 и утверждения 4 из предложения 13, и аксиома И7 истинна в M;

$$f((A \supset C) \supset ((B \supset C) \supset (A \vee B \supset C))) =$$
$$= (a \to c) \to (b \to c) \to (a + b \to c) = 1$$

в силу утверждений 4 и 8 из предложения 13, и аксиома И8 истинна в M;

$$f((A \supset B) \supset ((A \supset \neg B) \supset \neg A) =$$

$$= (a \to b) \to ((a \to (b \to 0)) \to (a \to 0)) = 1$$

в силу утверждений 6 и 4 из предложения 13, и аксиома И9 истинна в M;

$$f(A \supset (\neg A \supset B)) = a \to ((a \to 0) \to b) = 1$$

в силу утверждения 4 из предложения 13, так как в силу А10 и А12 $a \cdot (a \to 0) \leq 0 \leq b$, и аксиома И10 истинна в M. $\square$

Теорема 32. *Пусть* $\mathbf{M} = \langle M, 1, \cdot, +, \to, \sim \rangle$ *— логическая матрица. Определим на множестве* M *бинарное отношение* $\leq$, *положив*

$$x \leq y \rightleftharpoons x \to y = 1.$$

Если логическая матрица $\mathbf{M}$ *— модель интуиционистского исчисления высказываний, то* $\langle M, \leq, \cdot, +, \to, \sim \rangle$ *— псевдобулева алгебра.*

Доказательство. Проверим, что отношение $\leq$ и операции $\cdot, +, \to, \sim$ удовлетворяют аксиомам псевдобулевой алгебры А1 – А13.

А1. Докажем, что для любого элемента $a \in M$ имеет место $a \leq a$, т. е. $a \to a = 1$. Для этого заметим, что формула $P \supset P$ выводима в интуиционистском исчислении высказываний. Следовательно, она истинна в $\mathbf{M}$ при оценке f такой, что $f(P) = a$. Тогда $f(P \supset P) = a \to a = 1$, что и требовалось доказать.

А2. Докажем, что для любых $a, b \in M$ выполнено условие: если $a \leq b$ (т. е. $a \to b = 1$) и $b \leq a$ (т. е. $b \to a = 1$), то $a = b$. Но это следует из определения логической матрицы.

А3. Докажем, что для любых $a, b, c \in M$ выполнено условие: если $a \leq b$ (т. е. $a \to b = 1$) и $b \leq c$ (т. е. $b \to c = 1$), то $a \leq c$ (т. е. $a \to c = 1$). Для этого заметим, что формула

$$(P \supset Q) \supset ((Q \supset R) \supset (P \supset R))$$

выводима в интуиционистском исчислении высказываний. Следовательно, она истинна в **M** при оценке f такой, что $f(P) = a$, $f(Q) = b$, $f(R) = c$. Тогда

$$f((P \supset Q) \supset ((Q \supset R) \supset (P \supset R))) =$$
$$= (a \to b) \to ((b \to c) \to (a \to c)) = 1.$$

Так как $a \to b = 1$, то из определения логической матрицы следует $(b \to c) \to (a \to c) = 1$, а так как $b \to c = 1$, то из того же определения следует $a \to c = 1$, что и требовалось доказать.

А4. Докажем, что для любых $a, b \in M$ имеет место $a \leq a + b$, т. е. $a \to a + b = 1$. Для этого заметим, что формула $P \supset P \vee Q$ выводима в интуиционистском исчислении высказываний. Следовательно, она истинна в **M** при оценке f такой, что $f(P) = a$, $f(Q) = b$. Тогда

$$f(P \supset P \vee Q) = a \to a + b = 1,$$

что и требовалось доказать.

А5. Тот факт, что для любых $a, b \in M$ имеет место $b \leq a + b$, т. е. $b \to a + b = 1$, доказывается теми же рассуждениями, что применялись при рассмотрении аксиомы А4, только теперь следует взять формулу $Q \supset P \vee Q$.

А6. Докажем, что для любых $a, b, c \in M$ выполнено условие: если $a \leq c$ (т. е. $a \to c = 1$) и $b \leq c$ (т. е. $b \to c = 1$), то $a + b \leq c$ (т. е. $a + b \to c = 1$). Для этого заметим, что формула

$$(P \supset R) \supset ((Q \supset R) \supset (P \vee Q \supset R))$$

выводима в интуиционистском исчислении высказываний. Следовательно, она истинна в **M** при оценке f такой, что $f(P) = a$, $f(Q) = b$, $f(R) = c$. Тогда

$$f((P \supset R) \supset ((Q \supset R) \supset (P \vee Q \supset R))) =$$
$$= (a \to c) \to ((b \to c) \to (a + b \to c)) = 1.$$

Так как $a \to c = 1$, то из определения логической матрицы следует $(b \to c) \to (a + b \to c) = 1$, а так как $b \to c = 1$, то из того же определения следует $a + b \to c = 1$, что и требовалось доказать.

А7. Докажем, что для любых $a, b \in M$ имеет место $a \cdot b \leq a$, т. е. $a \cdot b \to a = 1$. Для этого заметим, что формула $P \,\&\, Q \supset P$

выводима в интуиционистском исчислении высказываний. Следовательно, она истинна в $\mathbf{M}$ при оценке f такой, что $f(P) = a$, $f(Q) = b$. Тогда

$$f(P \,\&\, Q \supset P) = a \cdot b \to a = 1,$$

что и требовалось доказать.

A8. Тот факт, что для любых $a, b \in M$ имеет место $a \cdot b \leq b$, т. е.

$$a \cdot b \to b = 1,$$

доказывается теми же рассуждениями, что применялись при рассмотрении аксиомы A7, только теперь следует взять формулу $P \,\&\, Q \supset Q$.

A9. Докажем, что для любых $a, b, c \in M$ выполнено условие: если $c \leq a$ (т. е. $c \to a = 1$) и $c \leq b$ (т. е. $c \to b = 1$), то $c \leq a \cdot b$ (т. е. $c \to a \cdot b = 1$). Для этого заметим, что формула

$$(R \supset P) \supset ((R \supset Q) \supset (R \supset P \,\&\, Q))$$

выводима в интуиционистском исчислении высказываний. Следовательно, она истинна в $\mathbf{M}$ при оценке f такой, что $f(P) = a$, $f(Q) = b$, $f(R) = c$. Тогда

$$f((R \supset P) \supset ((R \supset Q) \supset (R \supset P \,\&\, Q))) =$$
$$= (c \to a) \to ((c \to b) \to (c \to a \cdot b)) = 1.$$

Так как $c \to a = 1$, то из определения логической матрицы следует $(c \to b) \to (c \to a \cdot b) = 1$, а так как $c \to b = 1$, то из того же определения следует $c \to a \cdot b = 1$, что и требовалось доказать.

A10. Тот факт, что для любых $a, b \in M$ имеет место

$$a \cdot (a \to b) \leq b,$$

т. е. $a \cdot (a \to b) \to b = 1$, доказывается теми же рассуждениями, что применялись при рассмотрении аксиомы A4, только теперь следует взять формулу $P \,\&\, (P \supset Q) \supset Q$ (см. упражнение 1).

A11. Докажем, что для любых $a, b, c \in M$ выполнено условие: если

$$a \cdot c \leq b$$

(т. е. $a \cdot c \to b = 1$), то $c \leq a \to b$ (т. е. $c \to (a \to b) = 1$). Для этого заметим, что формула $(P \,\&\, R \supset Q) \supset (R \supset (P \supset Q))$ выводима в интуиционистском исчислении высказываний. Следовательно, она истинна в $\mathbf{M}$ при оценке f такой, что $f(P) = a$, $f(Q) = b$, $f(R) = c$. Тогда

$$f((P \,\&\, R \supset Q) \supset (R \supset (P \supset Q))) =$$
$$= (a \cdot c \to b) \to (c \to (a \to b)) = 1.$$

Так как $a \cdot c \to b = 1$, то из определения логической матрицы следует $c \to (a \to b) = 1$, что и требовалось доказать.

А12. Докажем, что в импликативной решетке $\langle M, \leq, \cdot, +, \to \rangle$ есть наименьший элемент. Пусть $b \in M$. Положим

$$0 = b \cdot \sim b$$

и покажем, что 0 — наименьший элемент. Последнее означает, что для любого $a \in M$ имеет место $0 \leq a$, т. е. $(b \cdot \sim b) \to a = 1$. Заметим, что формула $Q \,\&\, \neg Q \supset P$ выводима в интуиционистском исчислении высказываний. Следовательно, она истинна в $\mathbf{M}$ при оценке f такой, что $f(P) = a$, $f(Q) = b$. Тогда $f(Q \,\&\, \neg Q \supset P) = (b \cdot \sim b) \to a = 1$, что и требовалось доказать.

А13. Докажем, что для любого $a \in M$ имеет место

$$\sim a = a \to 0,$$

т. е. $\sim a = a \to (b \cdot \sim b)$. Заметим, что формула

$$\neg P \supset (P \supset Q \,\&\, \neg Q)$$

выводима в интуиционистском исчислении высказываний. Следовательно, она истинна в $\mathbf{M}$ при оценке f такой, что $f(P) = a$, $f(Q) = b$. Тогда

$$f(\neg P \supset (P \supset Q \,\&\, \neg Q)) = \sim a \to (a \to (b \cdot \sim b)) = 1,$$

откуда следует

$$\sim a \leq a \to (b \cdot \sim b). \tag{6.1}$$

Анадогично, принимая во внимание выводимость формулы

$$(P \supset Q \,\&\, \neg Q) \supset \neg P,$$

получаем $a \to (b \cdot \sim b) \leq \sim a$. Отсюда и из (6.1), в силу аксиомы А2, следует $\sim a = a \to (b \cdot \sim b)$, т. е. $\sim a = a \to 0$, что и требовалось доказать. □

§6.2. Нетабличность ИИВ

Пропозициональное исчисление называется *табличным*, если существует конечная точная модель этого исчисления, т. е. такая конечная логическая матрица, в которой истинны те и только те пропозициональные формулы, которые выводимы в этом исчислении. Примером табличного исчисления является классическое исчисление высказываний: его точная модель — двухэлементная алгебра Яськовского $J_0 = \{0, 1\}$ с отношением порядка $0 \leq 1$ (см. упражнение 2).

Теорема 33. *ИИВ не является табличным.*

Доказательство. Приведем доказательство этой теоремы, предложенное К. Гёделем [19]. Последовательность алгебр L_n определим так: $L_0 = J_0$; если алгебра L_{n-1} уже определена, то $L_n = \Gamma(L_{n-1})$ получается добавлением к L_{n-1} гёделева элемента ω_n. Таким образом, L_n — линейно упорядоченное множество $\{0, \omega_1, \ldots, \omega_n, 1\}$, причем элементы перечислены здесь в порядке отношения $\leq$. Рассмотрим формулу

$$F_n = \bigvee_{0 \leq j < i \leq n+1} (P_i \supset P_j),$$

построенную из переменных $P_0, P_1, \ldots, P_n, P_{n+1}$. Пусть f — оценка в L_n такая, что $f(P_0) = 0$; $f(P_i) = \omega_i$ $(1 \leq i \leq n)$; $f(P_{n+1}) = 1$. Очевидно, что если $j < i$, то

$$f(P_i \supset P_j) = f(P_i) \to f(P_j) = f(P_j) \neq 1.$$

Но тогда $f(F_n) = \omega_n \neq 1$. Значит, формула F_n опровергается в псевдобулевой алгебре L_n и потому невыводима в ИИВ.

Допустим, что существует логическая матрица M, являющаяся точной моделью ИИВ. В силу теоремы 32 можно считать M псевдобулевой алгеброй. Пусть в ней $n+1$ элементов $(n \geq 1)$. Тогда для произвольной оценки f в алгебре M найдутся такие i и j, что $0 \leq j < i \leq n+1$ и $f(P_i) = f(P_j) = a$ для некоторого $a \in M$. Тогда $f(P_i \supset P_j) = f(P_i) \to f(P_j) = a \to a = 1$. Следовательно, один из дизъюнктивных членов в F_n принимает значение 1 при оценке f. Но тогда и $f(F_n) = 1$, т. е. F_n истинна в M. Поскольку M — точная модель ИИВ, то F_n выводима, но это невозможно, как было показано выше. Таким образом, не существует конечной точной модели ИИВ. $\square$

§6.3. Теорема Гливенко

Всякая формула, выводимая в ИИВ, выводима и в классическом исчислении высказываний. Обратное неверно: формулы $P \vee \neg P$ и $\neg\neg P \supset P$ выводимы в классическом исчислении высказываний, но не выводимы в ИИВ. Следующая теорема устанавливает связь между выводимостью в классическом и интуиционистском исчислениях высказываний.

Теорема 34 (теорема Гливенко)**.** *Если пропозициональная формула F выводима в классическом исчислении высказываний, то формула $\neg\neg F$ выводима в ИИВ.*

Доказательство. Заметим, что если формула F выводима в ИИВ, то $\neg\neg F$ также выводима. Отсюда следует, что если F — аксиома классического исчисления высказываний, полученная по одной из схем 1 – 9, то $\neg\neg F$ выводима в ИИВ. Пусть F получена по схеме 10 классического исчисления высказываний, т. е. имеет вид $\neg\neg G \supset G$. Докажем, что $\neg\neg(\neg\neg G \supset G)$ выводима в ИИВ. В силу принципа приведения к абсурду достаточно доказать выводимость противоречия из $\neg(\neg\neg G \supset G)$. В качестве противоречия можно выбрать $\neg G$ и $\neg\neg G$. Доказательство выводимости обеих этих формул из гипотезы $\neg(\neg\neg G \supset G)$ является несложным упражнением. Таким образом, если F — аксиома классического исчисления высказываний, то формула $\neg\neg F$ выводима в ИИВ.

Лемма 3. *Если формулы $\neg\neg(G \supset H)$ и $\neg\neg G$ выводимы в ИИВ, то формула $\neg\neg H$ также выводима в ИИВ.*

Доказательство. Покажем, что

$$\{\neg\neg(G \supset H), \neg\neg G\} \vdash \neg\neg H.$$

Для этого достаточно убедиться, что в ИИВ выводимо противоречие из гипотез

$$\neg\neg(G \supset H), \neg\neg G, \neg H.$$

Очевидно, что из этих гипотез выводима формула $\neg\neg(G \supset H)$. Покажем, что из этих гипотез выводима также и формула

$\neg(G \supset H)$. Для этого в силу принципа приведения к абсурду достаточно проверить, что выводится противоречие из гипотез $\neg\neg(G \supset H), \neg\neg G, \neg H, G \supset H$. Очевидно, что из этого множества выводима формула $\neg H$. С другой стороны, дважды применяя правило контрапозиции, из формулы $G \supset H$ можно вывести $\neg\neg G \supset \neg\neg H$, а из нее и гипотезы $\neg\neg G$ — формулу $\neg\neg H$. □

Теперь теорема Гливенко легко доказывается индукцией по длине вывода формулы F в классическом исчислении высказываний (см. упражнение 3). □

Следующая теорема, доказанная В. А. Янковым [7], дает необходимое и достаточное условие того, что при добавлении к ИИВ новой схемы аксиом получается классическое исчисление высказываний.

Теорема 35. *Какова бы ни была формула F, исчисление ИИВ+F эквивалентно классическому исчислению высказываний тогда и только тогда, когда выполнены следующие условия:*

1) формула F выводима в классическом исчислении высказываний;

2) формула F опровергается в алгебре Яськовского J_1.

Доказательство. Пусть исчисление ИИВ+F эквивалентно классическому исчислению высказываний. Тогда, в частности, формула F выводима в классическом исчислении высказываний, так что условие 1) выполнено. С другой стороны, если бы формула F была истинна в алгебре J_1, то и все формулы, выводимые в классическом исчислении высказываний, были бы истинны в этой алгебре, что неверно, так как, например, формула $P \vee \neg P$ опровергается в алгебре J_1. Таким образом, условие 2) также выполнено.

Пусть для формулы $F(P_1, \ldots, P_n)$, не содержащей переменных, отличных от $P_1, \ldots, P_n$, выполнены условия 1) и 2), т. е. эта формула выводима в классическом исчислении высказываний, но опровергается в алгебре J_1, т. е. для некоторой оценки f в алгебре J_1 имеет место $f(F(P_1, \ldots, P_n)) \neq 1$. Очевидно, что $f(F(P_1, \ldots, P_n)) \neq 0$, ибо иначе $f(\neg\neg F(P_1, \ldots, P_n)) = 0$, что невозможно, так как в силу теоремы Гливенко (теорема 34) формула $\neg\neg F(P_1, \ldots, P_n)$ выводима в ИИВ, а потому истинна в алгебре J_1. Докажем, что исчисление ИИВ+F эквивалентно классическому исчислению высказываний. Для этого достаточно доказать, что в этом исчислении выводима формула $\neg\neg P \supset P$.

Алгебра J_1 состоит из элементов 0,2,1, перечисленных в том порядке, как они упорядочены в алгебре J_1. Каждому элементу $a \in J_1$ сопоставим формулу F_a: пусть F_0 есть $\bot$, F_1 есть $\top$ и F_2 есть P, где $\bot$ обозначает формулу $\neg(P \supset P)$, а $\top$ — формулу $P \supset P$.

Лемма 4. *Каковы бы ни были $a, b \in J_1$, в ИИВ из гипотезы $\neg\neg P$ выводимы формулы $\neg F_a \equiv F_{\sim a}$, $F_a \circ F_b \equiv F_{a*b}$, где $\circ$ — любая из логических связок $\&, \vee, \supset$, а $*$ — соответствующая ей операция псевдобулевой алгебры $\cdot, +, \to$.*

Доказательство. Требуется доказать, что из гипотезы $\neg\neg P$ выводимы следующие формулы:

1) $\neg\bot \equiv \top$; 2) $\neg\top \equiv \bot$; 3) $\neg P \equiv \bot$; 4) $\bot \,\&\, \bot \equiv \bot$;
5) $\bot \,\&\, \top \equiv \bot$; 6) $\bot \,\&\, P \equiv \bot$; 7) $\top \,\&\, \bot \equiv \bot$; 8) $\top \,\&\, \top \equiv \top$;
9) $\top \,\&\, P \equiv P$; 10) $P \,\&\, \bot \equiv \bot$; 11) $P \,\&\, \top \equiv P$; 12) $P \,\&\, P \equiv P$;
13) $\bot \vee \bot \equiv \bot$; 14) $\bot \vee \top \equiv \top$; 15) $\bot \vee P \equiv P$; 16) $\top \vee \bot \equiv \top$;
17) $\top \vee \top \equiv \top$; 18) $\top \vee P \equiv \top$; 19) $P \vee \bot \equiv P$; 20) $P \vee \top \equiv \top$;
21) $P \vee P \equiv P$; 22) $\bot \supset \bot \equiv \top$; 23) $\bot \supset \top \equiv \top$;
24) $\bot \supset P \equiv \top$; 25) $\top \supset \bot \equiv \neg\bot$; 26) $\top \supset \top \equiv \top$;
27) $\top \supset P \equiv P$; 28) $P \supset \bot \equiv \bot$; 29) $P \supset \top \equiv \top$;
30) $P \supset P \equiv \top$.

Все эти формулы, кроме 3) и 28), выводятся без использования гипотезы $\neg\neg P$ (см. упражнение 4). Докажем выводимость формулы 3). Сначала докажем, что $\neg\neg P \vdash \neg P \supset \bot$. В силу теоремы о дедукции достаточно убедиться, что $\neg\neg P, \neg P \vdash \bot$, что само по себе очевидно. Очевидно также, что $\neg\neg P \vdash \bot \supset \neg P$. Докажем выводимость формулы 28). Сначала докажем, что $\neg\neg P \vdash (P \supset \bot) \supset \bot$. В силу теоремы о дедукции достаточно убедиться, что $\neg\neg P, P \supset \bot \vdash \bot$. Для этого заметим, что дважды применив к формуле $P \supset \bot$ правило контрапозиции, получим формулу $\neg\neg P \supset \neg\neg\bot$, которая эквивалентна формуле

$\neg\neg P \supset \bot$. Теперь $\bot$ получается из этой формулы и гипотезы $\neg\neg P$ по правилу MP. $\square$

Вернемся к доказательству теоремы. С помощью леммы 4 индукцией по построению формулы $F(P_1, \ldots, P_n)$ доказывается выводимость $\neg\neg P \vdash F(F_{a_1}, \ldots, F_{a_n}) \equiv F_a$, где $a_i = f(P_i)$ $(i = 1, \ldots, n)$, $a = f(F(P_1, \ldots, P_n))$. Отсюда следует, что $F(F_{a_1}, \ldots, F_{a_n}) \vdash \neg\neg P \supset F_a$. Формула $F(F_{a_1}, \ldots, F_{a_n})$ является аксиомой исчисления ИИВ$+F$, а F_a есть P. Таким образом, мы получаем, что в указанном исчислении выводима формула $\neg\neg P \supset P$, что и требовалось доказать. $\square$

§6.4. Характеристические формулы

Пусть A — конечная гёделева псевдобулева алгебра. Это значит, что в ней есть гёделев элемент ω. Каждому элементу $a \in A$ сопоставим пропозициональную переменную P_a. Посредством $K(A)$ обозначим формулу

$$\bigwedge_{a\in A}(\neg P_a \equiv P_{\sim a})\,\&\,\bigwedge_{a,b\in A}(P_a \,\&\, P_b \equiv P_{a\cdot b})\,\&$$
$$\&\,\bigwedge_{a,b\in A}(P_a \vee P_b \equiv P_{a+b})\,\&\,\bigwedge_{a,b\in A}(P_a \supset P_b \equiv P_{a\to b}).$$

Предложение 18. *Пусть F — пропозициональная формула, f — оценка в алгебре A, и пусть $f(F) = d$. Пусть F_f — формула, полученная подстановкой в F переменной P_a вместо каждой переменной P, где $a = f(P)$. Тогда $K(A) \vdash (F_f \equiv P_d)$.*

Доказательство. Индукция по построению F. Пусть F есть P, причем $f(P) = a$. Тогда F_f есть P_a, и доказываемое утверждение очевидно. Пусть F имеет вид $\neg G$, причем для G доказываемое утверждение верно, т. е. из $K(A) \vdash (G_f \equiv P_{f(G)})$. Очевидно, что F_f есть $\neg G_f$, и $f(F) =\sim f(G)$. В силу теоремы об эквивалентной замене $K(A) \vdash \neg G_f \equiv \neg P_{f(G)}$, т. е. $K(A) \vdash F_f \equiv \neg P_{f(G)}$. С другой стороны, в $K(A)$ есть конъюнктивный член $\neg P_{f(G)} \equiv P_{\sim f(G)}$, т. е. $\neg P_{f(G)} \equiv P_{f(F)}$, так что $K(A) \vdash F_f \equiv P_{f(F)}$, что и требовалось доказать. Совершенно аналогично рассматривается случай, когда F имеет вид $G\lambda H$, где G и H — формулы, $\lambda \in \{\&, \vee, \supset\}$. $\square$

Формула $K(A) \supset P_\omega$, которую мы обозначим $\chi(A)$, называется *характеристической формулой* для алгебры A. Это понятие ввел В. А. Янков [7]. Он же доказал следующую теорему.

Теорема 36. *Какова бы ни была конечная гёделева псевдобулева алгебра A, 1) формула $\chi(A)$ опровергается в A; 2) если формула F опровергается в A, то ИИВ+$F \vdash \chi(A)$.*

Доказательство. 1) Рассмотрим такую оценку f в A, что $f(P_a) = a$ для любого $a \in A$. Очевидно, что $f(\chi(A)) = \omega$. Следовательно, $\chi(A)$ опровергается в A.

2) Пусть формула F опровергается в A, т. е. существует такая оценка f в A, что $f(F) = d \neq 1$. Формула F_f является аксиомой исчисления ИИВ+F. В силу предложения 18 $K(A) \vdash F_f \equiv P_d$. Отсюда вытекает, что $K(A), F_f \vdash P_d$. Так как $d \neq 1$, то $d \leq \omega$, и $d \to \omega = 1$. Это означает, что в $K(A)$ есть конъюнктивный член $P_d \supset P_\omega \equiv P_1$. Но в $K(A)$ есть также конъюнктивный член $P_1 \supset P_1 \equiv P_1$, так что $\{K(A), F_f\} \vdash P_1$, а значит $\{K(A), F_f\} \vdash (P_d \supset P_\omega)$. Отсюда следует $K(A), F_f \vdash P_\omega$, и далее по теореме о дедукции $F_f \vdash K(A) \supset P_\omega$, что и требовалось доказать. □

Теорема 36 имеет следующее применение. Свойство пропозициональных формул будем называть *интуиционистским*, если множество формул, обладающих этим свойством, замкнуто относительно правила подстановки и выводимости в ИИВ.

Теорема 37. *Пусть A — конечная гёделева псевдобулева алгебра. Если существует формула, опровержимая в алгебре A, которая обладает данным интуиционистским свойством, то этим интуиционистским свойством обладает формула $\chi(A)$.*

Доказательство. Пусть A — конечная гёделева псевдобулева алгебра. Допустим, что некоторая формула F обладает этим свойством и опровержима в алгебре A. Тогда по определению интуиционистского свойства всякая формула, выводимая в исчислении ИИВ+F, также обладает данным свойством. В частности, в силу теоремы 36 формула $\chi(A)$ обладает данным интуиционистским свойством. □

§6.5. Алгебра Линденбаума

Пусть $\mathcal{I}$ — произвольное пропозициональное исчисление. Будем предполагать только, что множество выводимых в этом исчислении формул замкнуто относительно правила MP. Для произвольных формул F и G будем писать $F \leq G$, если формула $F \supset G$ выводима в исчислении $\mathcal{I}$.

Предложение 19. *Если в исчислении $\mathcal{I}$ выводимы все формулы вида*

$$A \supset A$$

и

$$(A \supset B) \supset ((B \supset C) \supset (A \supset C)),$$

то отношение $\leq$ является отношением предпорядка на множестве всех пропозициональных формул.

Доказательство. Из выводимости формулы $A \supset A$ следует, что $A \leq A$ для любой формулы A, так что отношение $\leq$ рефлексивно. Если $A \leq B$ и $B \leq C$, то формулы $A \supset B$ и $B \supset C$ выводимы в исчислении $\mathcal{I}$. Отсюда и из выводимости формулы

$$(A \supset B) \supset ((B \supset C) \supset (A \supset C))$$

следует, что выводима формула $A \supset C$, т. е. $A \leq C$, так что отношение $\leq$ транзитивно. $\square$

По определению, формулы F и G *эквивалентны* в исчислении $\mathcal{I}$ ($F \sim_{\mathcal{I}} G$), если в $\mathcal{I}$ выводимы формулы $F \supset G$ и $G \supset F$. Так как $\leq$ — предпорядок, то в силу предложения 2 отношение $\sim_{\mathcal{I}}$ является отношением эквивалентности на множестве всех пропозициональных формул. Следовательно, множество всех формул разбивается на классы эквивалентности. Через $[F]$ будем обозначать класс эквивалентности, которому принадлежит F, а множество всех классов эквивалентности обозначим $L(\mathcal{I})$. Положим $[F] \leq_{\mathcal{I}} [G]$, если $F \leq G$, т. е. формула $F \supset G$ выводима в исчислении $\mathcal{I}$. В силу предложения 2 так определенное отношение $\leq$ является отношением частичного порядка на множестве $L(\mathcal{I})$.

Следуя [2], множество $L(\mathcal{I})$, рассматриваемое вместе с отношением $\leq_{\mathcal{I}}$ будем называть *алгеброй Линденбаума* для исчисления $\mathcal{I}$. Мы займемся изучением алгебры $L = L(\mathcal{I})$, когда $\mathcal{I}$ — это ИИВ. В этом случае вместо $\leq_{\mathcal{I}}$ будем писать просто $\leq$.

Теорема 38. *Множество L с отношением $\leq$ является псевдобулевой алгеброй, причем*

$$[F]\cdot[G]=[F\,\&\,G];\ [F]+[G]=[F\vee G];\ [F]\to[G]=[F\supset G];$$

$$\sim[F]=[\neg F];\ 0=[P\,\&\,\neg P].$$

Доказательство. Проверим, что для $\leq$, $\cdot$, $+$, $\to$, $\sim$, 0 выполнены аксиомы псевдобулевой алгебры. Мы уже установили, что $\leq$ — частичный порядок, так что аксиомы A1 – A3 выполнены. Проверим другие аксиомы.

A4. Пусть $a, b \in L$. Тогда $a = [F]$, $b = [G]$ для некоторых формул F, G, и $a \leq a + b$ означает $\vdash F \supset F \vee G$, что, очевидно, имеет место. Таким образом, и аксиома A4 выполнена.

Выполнимость аксиомы A5 доказывается аналогично с использованием выводимости формулы $G \supset F \vee G$.

A6. Пусть $a, b, c \in L$. Тогда $a = [F]$, $b = [G]$, $c = [H]$ для некоторых формул F, G и H. Пусть $a \leq c$, т. е. $\vdash F \supset H$, и $b \leq c$, т. е. $\vdash G \supset H$. Используя аксиому И8, нетрудно показать, что в этом случае формула $F \vee G \supset H$ выводима в ИИВ, а тогда

$$a+b=[F\vee G]\leq[H]=c.$$

Таким образом, аксиома A6 также выполнена.

A7. Пусть $a, b \in L$. Тогда $a = [F]$, $b = [G]$ для некоторых формул F, G, и $a \cdot b \leq a$ означает $\vdash F\,\&\,G \supset F$, что, очевидно, имеет место. Таким образом, и аксиома A7 выполнена.

Выполнимость аксиомы A8 доказывается аналогично с использованием выводимости формулы $F\,\&\,G \supset G$.

A9. Пусть $a, b, c \in L$. Тогда $a = [F]$, $b = [G]$, $c = [H]$ для некоторых F, G и H. Пусть $c \leq a$, т. е. $\vdash H \supset F$, и $c \leq b$, т. е. $\vdash H \supset G$. Используя аксиому И5, нетрудно показать, что в этом случае из гипотезы H выводима формула $F\,\&\,G$, откуда в силу теоремы дедукции следует, что выводима формула $H \supset F\,\&\,G$, т. е. $c = [H] \leq [F\,\&\,G] = a \cdot b$. Таким образом, аксиома A9 также выполнена.

A10. Пусть $a, b \in L$. Тогда $a = [F]$, $b = [G]$ для некоторых F, G, и $a \cdot (a \to b) \leq b$ означает

$$\vdash F \,\&\, (F \supset G) \supset G,$$

что очевидно имеет место. Таким образом, и аксиома A10 выполнена.

A11. Пусть $a, b, c \in L$. Тогда $a = [F]$, $b = [G]$, $c = [H]$ для некоторых F, G и H. Пусть $a \cdot c \leq b$, т. е. $\vdash F \,\&\, H \supset G$. В этом случае, очевидно, $\vdash H \supset (F \supset G)$, что означает $c \leq (a \to b)$. Таким образом, аксиома A11 также выполнена.

A12. Пусть $a \in L$, причем $a = [F]$. Тогда $0 \leq a$ означает выводимость формулы $P \,\&\neg P \supset F$, что очевидно имеет место. Таким образом, аксиома A12 выполнена.

A13. Пусть $a \in L$. Тогда $a = [F]$ для некоторой формулы $[F]$, и $\sim a = a \to 0$ означает, что $\neg F \sim F \supset P \,\&\neg P$, т. е. $\vdash \neg F \supset (F \supset P \,\&\neg P)$ и $\vdash (F \supset P \,\&\neg P) \supset \neg F$, что очевидно имеет место. Таким образом, для любого элемента $a \in L$ имеет место $\sim a = a \to 0$, и аксиома A13 выполнена. □

Заметим, что наибольшим элементом 1_L алгебры L является класс $[P \supset P]$, состоящий из всех формул, выводимых в ИИВ. Действительно, все выводимые формулы, очевидно, эквивалентны друг другу и потому образуют один класс эквивалентности $[P \supset P]$. Кроме того, какова бы ни была формула F, формула $F \supset (P \supset P)$ выводима, следовательно, $[F] \leq [P \supset P]$.

Канонической оценкой в алгебре L назовем такую оценку, которая каждой переменной P_i сопоставляет класс эквивалентности $[P_i]$.

Предложение 20. *Пусть f_0 — каноническая оценка в алгебре Линденбаума L. Тогда для любой пропозициональной формулы F выполняется равенство $f_0(F) = [F]$.*

Доказательство. Индукция по построению формулы F. Если F есть переменная, то доказываемое равенство выполняется в силу определения канонической оценки. Пусть формула F имеет вид $\neg G$, и допустим, что для формулы G доказываемое равенство верно, т. е. $f_0(G) = [G]$. Тогда

$$f_0(F) = f_0(\neg G) = \sim (f_0(G)) = \sim [G] = [\neg G] = [F],$$

т. е. доказываемое равенство верно и для формулы F. Пусть формула F имеет вид $G \mathbin{\&} H$, причем $f_0(G) = [G]$, $f_0(H) = [H]$. Тогда

$$f_0(F) = f_0(G \mathbin{\&} H) = f_0(G) \cdot f_0(H) = [G] \cdot [H] = [G \mathbin{\&} H] = [F],$$

что и требовалось доказать. Совершенно аналогично рассматриваются случаи, когда F имеет вид $G \vee H$ или $G \supset H$. □

Предложение 21. *Пропозициональная формула F выводима в ИИВ тогда и только тогда, когда для канонической оценки f_0 в алгебре Линденбаума L выполняется равенство $f_0(F) = 1_L$.*

Доказательство. Утверждение, что для выводимой формулы F имеет место $f_0(F) = 1_L$, вытекает из того факта, что любая выводимая формула истинна в любой псевдобулевой алгебре. Докажем обратное утверждение. Из предложения 20 вытекает $f_0(F) = [F]$, поэтому, если $f_0(F) = 1_L$, то $[F] = 1_L$, т. е. F принадлежит классу, состоящему из выводимых формул, следовательно, формула F выводима. □

Теорема 39. *Алгебра Линденбаума является точной моделью ИИВ.*

Доказательство. Требуется доказать, что в ИИВ выводимы те и только те формулы, которые истинны в алгебре L. Пусть формула F выводима. Тогда она истинна в любой псевдобулевой алгебре, в частности, в алгебре L. Обратно, пусть формула F истинна в алгебре L. Тогда формула F принимает значение 1_L при любой оценке в алгебре L, в частности, для канонической оценки f_0 имеем $f_0(F) = 1_L$. В силу предложения 21 это означает, что формула F выводима. □

Из теоремы 39 вытекает следующая *теорема о полноте* ИИВ относительно псевдобулевых алгебр.

Теорема 40. *Если пропозициональная формула истинна в любой псевдобулевой алгебре, то эта формула выводима в ИИВ.*

Доказательство. Если пропозициональная формула истинна в любой псевдобулевой алгебре, то эта формула истинна в алгебре Линденбаума и в силу теоремы 39 выводима в ИИВ. □

Теорема 40 и теорема о корректности ИИВ относительно псевдобулевых алгебр (теорема 31) вместе дают следующее утверждение.

Теорема 41. *Пропозициональная формула выводима в ИИВ тогда и только тогда, когда эта формула истинна в любой псевдобулевой алгебре.*

Для алгебры Линденбаума L можно построить алгебру $\Gamma(L)$. При этом, в силу построения алгебры $\Gamma(L)$, ее наибольшим элементом является 1_L. Так как $L \subseteq \Gamma(L)$, то каноническую оценку f_0 в алгебре L можно рассматривать и как оценку в алгебре $\Gamma(L)$.

Предложение 22. *Пропозициональная формула F выводима в ИИВ тогда и только тогда, когда для канонической оценки f_0 в алгебре $\Gamma(L)$ выполняется равенство $f_0(F) = 1_L$.*

Доказательство. Утверждение, что для выводимой формулы F имеет место $f_0(F) = 1_L$, вытекает из того факта, что любая выводимая формула истинна в любой псевдобулевой алгебре. Докажем обратное утверждение. Пусть для канонической оценки f_0 в алгебре $\Gamma(L)$ выполняется равенство $f_0(F) = 1_L$. Допустим, однако, что формула F невыводима. В этом случае, в силу предложения 21, формула F опровергается в алгебре L канонической оценкой f_0. Но тогда, в силу предложения 16, формула F опровергается в алгебре $\Gamma(L)$ той же оценкой f_0, что противоречит условию $f_0(F) = 1_L$. □

§6.6. Свойство дизъюнктивности ИИВ

Свойство дизъюнктивности пропозиционального исчисления означает, что из выводимости в этом исчислении формулы вида $F \vee G$ вытекает выводимость одной из формул F и G. Следующая теорема была впервые без доказательства сформулирована К. Гёделем [18].

Теорема 42. *ИИВ обладает свойством дизъюнктивности.*

Доказательство. Пусть формула $F \vee G$ выводима в ИИВ. Тогда в силу предложения 22 имеет место $f_0(F \vee G) = 1_L$ для канонической оценки f_0 в алгебре $\Gamma(L)$, где L — алгебра Линденбаума.

Так как алгебра $\Gamma(L)$ является гёделевой, то либо $f_0(F) = 1_L$, либо $f_0(G) = 1_L$. В первом случае в силу предложения 22 формула F выводима в ИИВ, во втором — формула G выводима в силу того же предложения.

Приведем другое доказательство свойства дизъюнктивности для ИИВ. Определим понятие «пропозициональная формула A реализуема», обозначаемое $\mathbf{r}\,A$, индукцией по построению формулы A (здесь $\vdash$ означает выводимость в ИИВ):

- никакая переменная не реализуема;
- $\mathbf{r}\,(A \,\&\, B) \rightleftharpoons [\mathbf{r}\,A \,\&\, \mathbf{r}\,B]$;
- $\mathbf{r}\,(A \vee B) \rightleftharpoons [(\mathbf{r}\,A \,\&\, \vdash A) \vee (\mathbf{r}\,B \,\&\, \vdash B)]$;
- $\mathbf{r}\,(A \supset B) \rightleftharpoons [(\mathbf{r}\,A \,\&\, \vdash A) \Rightarrow \mathbf{r}\,B]$;
- $\mathbf{r}\,\neg A \rightleftharpoons$ [неверно, что $(\mathbf{r}\,A \,\&\, \vdash A)$].

Предложение 23. *Если* $\vdash A$, *то* $\mathbf{r}\,A$.

Доказательство. Применяем индукцию по выводу формулы A в ИИВ. Сначала докажем, что все аксиомы реализуемы.

И1. $A \supset (B \supset A)$. Реализуемость этой формулы означает $(\mathbf{r}\,A \,\&\, \vdash A) \Rightarrow [(\mathbf{r}\,B \,\&\, \vdash B) \Rightarrow \mathbf{r}\,A]$. Истинность этого утверждения очевидна. Действительно, если $\mathbf{r}\,A \,\&\, \vdash A$ и $\mathbf{r}\,B \,\&\, \vdash B$, то $\mathbf{r}\,A$.

И2. $(A \supset B) \supset ((A \supset (B \supset C)) \supset (A \supset C))$. Реализуемость этой формулы означает, что если $\mathbf{r}\,(A \supset B) \,\&\, \vdash (A \supset B)$, т. е.

$$[\mathbf{r}\,A \,\&\, \vdash A \Rightarrow \mathbf{r}\,B] \,\&\, \vdash (A \supset B), \tag{6.2}$$

$\mathbf{r}\,(A \supset (B \supset C)) \,\&\, \vdash (A \supset (B \supset C))$, т. е.

$$[\mathbf{r}\,A \,\&\, \vdash A \Rightarrow \mathbf{r}\,(B \supset C)] \,\&\, \vdash (A \supset (B \supset C)), \tag{6.3}$$

и

$$\mathbf{r}\,A \,\&\, \vdash A, \tag{6.4}$$

то $\mathbf{r}\,C$. Из условий (6.2) и (6.4) следует

$$\mathbf{r}\,B \,\&\, \vdash B. \tag{6.5}$$

Из (6.3) и (6.4) следует $\mathbf{r}\,(B \supset C)$, т. е.

$$\mathbf{r}\,B \,\&\, \vdash B \Rightarrow \mathbf{r}\,C. \tag{6.6}$$

Из (6.5) и (6.6) следует $\mathbf{r}\,C$, что и требовалось доказать.

И3. $A \,\&\, B \supset A$. Реализуемость этой формулы означает $[\mathbf{r}\,A \,\&\, \mathbf{r}\,B \,\&\, \vdash (A \,\&\, B)] \Rightarrow \mathbf{r}A$, что очевидно.

И4. $A \,\&\, B \supset B$. Реализуемость этой формулы означает $[\mathbf{r}\,A \,\&\, \mathbf{r}\,B \,\&\, \vdash (A \,\&\, B)] \Rightarrow \mathbf{r}B$, что также очевидно.

И5. $A \supset (B \supset A \,\&\, B)$. Реализуемость этой формулы означает, что если $\mathbf{r}\,A \,\&\, \vdash A$ и $\mathbf{r}\,B \,\&\, \vdash B$, то $\mathbf{r}\,A \,\&\, \mathbf{r}\,B$, что очевидно.

И6. $A \supset A \vee B$. Реализуемость этой формулы означает, что если $\mathbf{r}\,A \,\&\, \vdash A$, то $(\mathbf{r}\,A \,\&\, \vdash A) \vee (\mathbf{r}\,B \,\&\, \vdash B)$, что очевидно.

И7. $B \supset A \vee B$. Реализуемость этой формулы означает, что если $\mathbf{r}\,B \,\&\, \vdash B$, то $(\mathbf{r}\,A \,\&\, \vdash A) \vee (\mathbf{r}\,B \,\&\, \vdash B)$, что также очевидно.

И8. $(A \supset C) \supset ((B \supset C) \supset (A \vee B \supset C))$. Реализуемость этой формулы означает, что если

$$[\mathbf{r}\,A \,\&\, \vdash A \Rightarrow \mathbf{r}\,C] \,\&\, \vdash (A \supset C), \tag{6.7}$$

$$[\mathbf{r}\,B \,\&\, \vdash B \Rightarrow \mathbf{r}\,C] \,\&\, \vdash (B \supset C) \tag{6.8}$$

и

$$[\mathbf{r}\,A \,\&\, \vdash A) \vee (\mathbf{r}\,B \,\&\, \vdash B] \,\&\, \vdash (A \vee B), \tag{6.9}$$

то $\mathbf{r}\,C$. Из (6.9) следует $\mathbf{r}\,A \,\&\, \vdash A$ или $\mathbf{r}\,B \,\&\, \vdash B$. В первом случае с помощью (6.7), а во втором — с помощью (6.8) получаем $\mathbf{r}\,C$, что и требовалось доказать.

И9. $(A \supset B) \supset ((A \supset \neg B) \supset \neg A)$. Реализуемость этой формулы означает, что если

$$[\mathbf{r}\,A \,\&\, \vdash A \Rightarrow \mathbf{r}\,B] \,\&\, \vdash (A \supset B) \tag{6.10}$$

и

$$[\mathbf{r}\,A \,\&\, \vdash A \Rightarrow \mathbf{r}\,\neg B] \,\&\, \vdash (A \supset \neg B), \tag{6.11}$$

то неверно, что $\mathbf{r}\,A \,\&\, \vdash A$. Из (6.10) имеем $\vdash (A \supset B)$, а из (6.11) имеем $\vdash (A \supset \neg B)$, так что очевидно, что формула A невыводима и условие $\mathbf{r}\,A \,\&\, \vdash A$ действительно не выполнено.

И10. $A \supset (\neg A \supset B)$. Реализуемость этой формулы означает, что если

$$\mathbf{r}\,A \,\&\, \vdash A \tag{6.12}$$

и

$$\mathbf{r}\,\neg A \,\&\, \vdash \neg A, \tag{6.13}$$

то $\mathbf{r}\,B$, что очевидно выполнено, ибо условия (6.12) и (6.13) несовместны.

Таким образом, мы доказали, что все аксиомы ИИВ реализуемы. Докажем теперь корректность правила MP: если выводимые формулы A и $A \supset B$ обе реализуемы, то формула B реализуема. Реализуемость и выводимость формулы A означает, что имеет место $\mathbf{r}\,A \,\&\, \vdash A$. Реализуемость формулы $A \supset B$ означает $\mathbf{r}\,A \,\&\, \vdash A \Rightarrow \mathbf{r}\,B$, так что очевидно $\mathbf{r}\,B$, что и требовалось доказать. $\square$

Теперь дизъюнктивность ИИВ доказывается следующим образом. Пусть формула $A \vee B$ выводима в ИИВ. В силу предложения 23 эта формула реализуема, т. е. имеет место $\mathbf{r}\,A \,\&\, \vdash A$ или $\mathbf{r}\,B \,\&\, \vdash B$. В первом случае получаем выводимость формулы A, во втором — выводимость формулы B. $\square$

Упражнения

1. Пусть логическая матрица $\mathbf{M}$ — модель ИИВ. Определим на ней бинарное отношение $\leq$, положив
$$x \leq y \rightleftharpoons x \to y = 1.$$
Доказать, что в этом случае выполняется аксиома A10 псевдобулевой алгебры.

2. Доказать, что алгебра Яськовского J_0 является точной моделью классического исчисления высказываний.

3. Завершить доказательство теоремы Гливенко.

4. Пусть $\bot$ обозначает формулу $\neg(P \supset P)$, а $\top$ — формулу $P \supset P$. Доказать, что в ИИВ выводимы следующие формулы: $\neg\bot \equiv \top$; $\neg\top \equiv \bot$; $\bot \,\&\, \bot \equiv \bot$; $\bot \,\&\, \top \equiv \bot$; $\bot \,\&\, P \equiv \bot$; $\top \,\&\, \bot \equiv \bot$; $\top \,\&\, \top \equiv \top$; $\top \,\&\, P \equiv P$; $P \,\&\, \bot \equiv \bot$; $P \,\&\, \top \equiv P$; $P \,\&\, P \equiv P$; $\bot \vee \bot \equiv \bot$; $\bot \vee \top \equiv \top$; $\bot \vee P \equiv P$; $\top \vee \bot \equiv \top$; $\top \vee \top \equiv \top$; $\top \vee P \equiv \top$; $P \vee \bot \equiv P$; $P \vee \top \equiv \top$; $P \vee P \equiv P$; $\bot \supset \bot \equiv \top$; $\bot \supset \top \equiv \top$; $\bot \supset P \equiv \top$; $\top \supset \bot \equiv \neg\bot$; $\top \supset \top \equiv \top$; $\top \supset P \equiv P$; $P \supset \top \equiv \top$; $P \supset P \equiv \top$.

Глава 7

Модели Крипке для логики высказываний

§7.1. Алгебра открытых множеств

Топологическим пространством называется непустое множество M, рассматриваемое вместе с некоторой системой $\mathcal{T}$ его подмножеств, удовлетворяющей условиям

1) $M \in \mathcal{T}$, $\emptyset \in \mathcal{T}$;

2) объединение всякого множества элементов $\mathcal{T}$ является элементом $\mathcal{T}$;

3) пересечение любых двух элементов $\mathcal{T}$ является элементом $\mathcal{T}$.

Подмножества M, входящие в $\mathcal{T}$, называются *открытыми множествами.* Если $X \subseteq M$, то объединение всех открытых подмножеств X открыто. Это множество называется *внутренностью* множества X и обозначается $Int(X)$. Очевидно, что $Int(X)$ является наибольшим по включению открытым множеством, содержащимся в X.

Теорема 43. *Пусть M — топологическое пространство с системой открытых множеств $\mathcal{T}$. На множестве $\mathcal{T}$ определим отношение $\leq$, положив $X \leq Y \rightleftharpoons X \subseteq Y$. Тогда множество $\mathcal{T}$ с отношением $\leq$ является псевдобулевой алгеброй.*

Доказательство. Очевидно, что отношение $\leq$ является частичным порядком на множестве $\mathcal{T}$. Для любых множеств $X, Y \in \mathcal{T}$, очевидно, существуют их точная верхняя грань $X \cup Y$ и точная нижняя грань $X \cap Y$, принадлежащие семейству $\mathcal{T}$. Псевдодополнением открытого множества X относительно открытого множества Y, по определению, является наибольшее по включению открытое множество Z такое, что $X \cap Z \subseteq Y$. Покажем, что такое множество существует для любых X, Y: это множество $Int(\bar{X} \cup Y)$, где $\bar{X} = M \setminus X$— дополнение множества X. Во-первых, требуется доказать, что $Int(\bar{X} \cup Y) \cap X \subseteq Y$.

Пусть $x \in Int(\bar{X} \cup Y) \cap X$. Тогда $x \in Int(\bar{X} \cup Y)$, следовательно, $x \in \bar{X} \cup Y$, ибо любое множество включает свою внутренность. Кроме того, $x \in X$. Отсюда получаем $x \in Y$. Таким образом, любой элемент множества $Int(\bar{X} \cup Y)$ принадлежит множеству Y, и включение $Int(\bar{X} \cup Y) \cap X \subseteq Y$ доказано.

Докажем теперь, что $Int(\bar{X} \cup Y)$ есть наибольшее по включению среди таких открытых множеств Z, что $X \cap Z \subseteq Y$. Итак, пусть Z — открытое множество и $X \cap Z \subseteq Y$. Так как множество Z открыто, то, в силу определения внутренности, достаточно доказать, что $Z \subseteq \bar{X} \cup Y$. Пусть $z \in Z$. Если $z \in X$, то $z \in X \cap Z \subseteq Y$, следовательно, $z \in Y \subseteq \bar{X} \cup Y$, т. е. $z \in \bar{X} \cup Y$. Если же $z \notin X$, то снова $z \in \bar{X} \cup Y$. Таким образом, любой элемент множества Z принадлежит множеству $\bar{X} \cup Y$, и включение $Z \subseteq \bar{X} \cup Y$ доказано, а значит, доказано и включение $Z \subseteq Int(\bar{X} \cup Y)$. Наименьшим элементом в семействе $\mathcal{T}$ является, очевидно, пустое множество, а псевдодополнением открытого множества X является $Int(\bar{X})$.

Таким образом, семейство $\mathcal{T}$ всех открытых множеств топологического пространства M, рассматриваемое как частично упорядоченное множество с отношением $\subseteq$, является псевдобулевой алгеброй, причем операции определены так:

$$X + Y = X \cup Y,\ X \cdot Y = X \cap Y,$$

$$X \to Y = Int(\bar{X} \cup Y),\ \sim X = Int(\bar{X}),\ 0 = \emptyset.$$

$\square$

Рассмотрим пример топологического пространства. Пусть M — частично упорядоченное множество с отношением порядка $\leq$. Подмножество X множества M назовем открытым, если $(\forall x, y \in M)\,[x \in X \,\&\, x \leq y \Rightarrow y \in X]$. Очевидно, что пустое множество и множество M являются открытыми подмножествами. Объединение любого семейства открытых подмножеств также является открытым подмножеством. Наконец, пересечение любых двух открытых подмножеств открыто. Таким образом, частично упорядоченное множество M, рассматриваемое вместе с семейством $\mathcal{T}$ всех его открытых подмножеств, является топологическим пространством, а семейство $\mathcal{T}$ является псевдобулевой алгеброй с указанными выше операциями.

§7.2. Пропозициональные модели Крипке

Модель Крипке — это набор $\mathcal{K} = (K, \preceq, \Vdash)$, где $(K, \preceq)$ — частично упорядоченное множество, называемое *шкалой Крипке*, а $\Vdash$ — соответствие между K и множеством всех переменных такое, что если $\alpha \Vdash P$ и $\alpha \preceq \beta$, то $\beta \Vdash P$. Соответствие $\Vdash$ называется *оценкой*. Интуитивный смысл моделей Крипке соответствует интуиционистским представлениям о становящемся характере истинности высказывания. А именно, элементы множества K можно трактовать как «моменты времени», причем $\alpha \preceq \beta$ означает, что момент α предшествует моменту β. При этом моменты времени следует понимать не в «физическом», а, так сказать, в «логическом» смысле: каждый момент времени характеризуется состоянием знаний в этот момент. Поэтому шкала Крипке («временна́я шкала»), вообще говоря, не является линейно упорядоченным множеством, ибо в будущем развитие знаний может пойти разными путями. Выражение $\alpha \Vdash P$ читается «α вынуждает P» или «P истинно в момент α». Интуитивно $\alpha \Vdash P$ означает, что в момент α утверждение P является доказанным, а условие, что если $\alpha \Vdash P$ и $\alpha \preceq \beta$, то $\beta \Vdash P$, выражает *принцип сохранения истинности.*

На основе соответствия $\Vdash$ определяется соответствие между множеством K и множеством всех формул, также обозначаемое $\Vdash$. Соответствие $\alpha \Vdash A$ задается индукцией по построению формулы A. Для переменной A оно уже определено. Далее полагаем:

$$\alpha \Vdash (A \,\&\, B) \rightleftharpoons [\alpha \Vdash A \,\&\, \alpha \Vdash B]; \; \alpha \Vdash (A \vee B) \rightleftharpoons [\alpha \Vdash A \vee \alpha \Vdash B];$$

$$\alpha \Vdash (A \supset B) \rightleftharpoons \forall\beta\, [\alpha \preceq \beta \Rightarrow (\beta \nVdash A \vee \beta \Vdash B];$$

$$\alpha \Vdash \neg A \rightleftharpoons \forall\beta\, [\alpha \preceq \beta \Rightarrow \beta \nVdash A].$$

Определение $\alpha \Vdash A$ для & и $\vee$ вполне отвечает интуиционистскому пониманию этих операций. Определение этого соответствия для $\supset$ и $\neg$, если и не совсем адекватно интуиционистскому пониманию этих операций, все же согласовано с ним: если в момент α дано обоснование для $A \supset B$, то в любой момент, когда будет получено обоснование для A, мы можем получить обоснование для B. Аналогично, если в момент α дано обоснование для $\neg A$, то никогда в будущем не будет получено обоснование для A.

Через $f(A)$ обозначим множество $\{\alpha \in K \mid \alpha \Vdash A\}$. Говорят, что формула A истинна в модели $\mathcal{K}$, если $f(A) = K$. Если формула A истинна в модели Крипке $\mathcal{K}$, последняя называется моделью для A; в противном случае $\mathcal{K}$ называется контрмоделью для A.

Предложение 24. *Какова бы ни была фомула A, множество $f(A)$ является открытым подмножеством частично упорядоченного множества K.*

Доказательство. Требуется доказать, что если $\alpha \Vdash A$ и $\alpha \preceq \beta$, то $\beta \Vdash A$. Индукция по построению A. Если A — переменная, то утверждение имеет место по определению оценки. Пусть A имеет вид $B \,\&\, C$, причем $f(B)$ и $f(C)$ — открытые множества. Очевидно, что $f(A) = f(B) \cap f(C)$, и $f(A)$ открыто как пересечение двух открытых множеств. Пусть A имеет вид $B \vee C$, причем $f(B)$ и $f(C)$ — открытые множества. Очевидно, что $f(A) = f(B) \cup f(C)$, и $f(A)$ открыто как объединение открытых множеств. Пусть A имеет вид $B \supset C$, причем $f(B)$ и $f(C)$ — открытые множества. Пусть $\alpha \Vdash A$, т. е.

$$\forall\gamma\, [\alpha \preceq \gamma \Rightarrow \gamma \nVdash B \text{ или } \gamma \Vdash C], \tag{7.1}$$

и $\alpha \preceq \beta$. Требуется доказать, что $\forall\gamma\, [\beta \preceq \gamma \Rightarrow (\gamma \nVdash B \vee \gamma \Vdash C]$. Пусть $\beta \preceq \gamma$. Тогда $\alpha \preceq \gamma$, и в силу (7.1) $\gamma \nVdash B$ или $\gamma \Vdash C$, что и требовалось доказать. Пусть, наконец, формула A имеет вид $\neg B$. Пусть $\alpha \Vdash A$, т. е.

$$\forall\gamma\, [\alpha \preceq \gamma \Rightarrow \gamma \nVdash B], \tag{7.2}$$

и $\alpha \preceq \beta$. Требуется доказать, что $\beta \Vdash A$, т. е. $\forall\gamma\, [\beta \preceq \gamma \Rightarrow \gamma \nVdash B]$. Итак, пусть $\beta \preceq \gamma$. Тогда $\alpha \preceq \gamma$, и в силу (7.2) выполняется $\gamma \nVdash B$, что и требовалось доказать. $\square$

Таким образом, для любой формулы A множество $f(A)$ открыто, т. е. является элементом псевдобулевой алгебры открытых подмножеств множества K.

Теорема 44. *Для любых пропозициональных формул A, B выполняются условия:*

$$f(A \vee B) = f(A) + f(B),\ f(A \,\&\, B) = f(A) \cdot f(B),$$

$$f(A \supset B) = f(A) \to f(B),\ f(\neg A) = \sim f(A),$$

где $+, \cdot, \to, \sim$ *— операции в псевдобулевой алгебре открытых подмножеств множества* K.

Доказательство. Очевидно, что

$$f(A \vee B) = f(A) \cup f(B) = f(A) + f(B);$$

$$f(A \,\&\, B) = f(A) \cap f(B) = f(A) \cdot f(B).$$

Докажем, что $f(A \supset B) = f(A) \to f(B) = Int(\overline{f(A)} \cup f(B))$. Сначала докажем включение $f(A \supset B) \subseteq Int(\overline{f(A)} \cup f(B))$. По теореме 24, множество $f(A \supset B)$ открыто, поэтому достаточно доказать, что $f(A \supset B) \subseteq \overline{f(A)} \cup f(B)$. Пусть $\alpha \in f(A \supset B)$, т. е. $\alpha \Vdash A \supset B$. Это означает, что

$$\forall \gamma\, [\alpha \preceq \gamma \Rightarrow (\gamma \nVdash A \vee \gamma \Vdash B].$$

Так как отношение $\preceq$ рефлексивно, то отсюда следует, что либо $\alpha \nVdash A$, и тогда $\alpha \in \overline{f(A)} \subseteq \overline{f(A)} \cup f(B)$, либо $\alpha \Vdash B$, и тогда $\alpha \in f(B) \subseteq \overline{f(A)} \cup f(B)$. Значит, если $\alpha \in f(A \supset B)$, то $\alpha \in \overline{f(A)} \cup f(B)$, и включение $f(A \supset B) \subseteq \overline{f(A)} \cup f(B)$ доказано, а значит, доказано и включение $f(A \supset B) \subseteq Int(\overline{f(A)} \cup f(B))$. Докажем обратное включение $Int(\overline{f(A)} \cup f(B)) \subseteq f(A \supset B)$. Пусть $\alpha \in Int(\overline{f(A)} \cup f(B))$. Докажем, что $\alpha \in f(A \supset B)$, т. е. $\alpha \Vdash A \supset B$. Это означает, что для любого $\beta \in K$ такого, что $\alpha \preceq \beta$, выполняется условие $\beta \nVdash A$, т. е. $\beta \in \overline{f(A)}$, или $\beta \Vdash B$, т. е. $\beta \in f(B)$. Итак, пусть $\alpha \preceq \beta$. Так как множество $Int(\overline{f(A)} \cup f(B))$ открыто, то $\beta \in Int(\overline{f(A)} \cup f(B)) \subseteq \overline{f(A)} \cup f(B)$, т. е. действительно $\beta \in \overline{f(A)}$ или $\beta \in f(B)$, что и требовалось доказать.

Докажем теперь, что $f(\neg A) = \sim f(A) = Int(\overline{f(A)})$. Сначала докажем включение $f(\neg A) \subseteq Int(\overline{f(A)})$. Согласно теореме 24, множество $f(\neg A)$ открыто, поэтому достаточно доказать, что $f(\neg A) \subseteq \overline{f(A)}$. Пусть $\alpha \in f(\neg A)$, т. е. $\alpha \Vdash \neg A$. Это означает, что $\forall \gamma\, [\alpha \preceq \gamma \Rightarrow \gamma \nVdash A]$. Так как отношение $\preceq$ рефлексивно, то отсюда в частности следует, что $\alpha \nVdash A$ и $\alpha \in \overline{f(A)}$. Значит, если $\alpha \in f(\neg A)$, то $\alpha \in \overline{f(A)}$, и включение $f(\neg A) \subseteq \overline{f(A)}$ доказано, а значит, доказано и включение $f(\neg A) \subseteq Int(\overline{f(A)})$. Докажем обратное включение $Int(\overline{f(A)}) \subseteq f(\neg A)$. Пусть $\alpha \in Int(\overline{f(A)})$. Докажем, что $\alpha \in f(\neg A)$, т. е. $\alpha \Vdash \neg A$. Это означает, что для любого $\beta \in K$ такого, что $\alpha \preceq \beta$, выполняется условие $\beta \not\Vdash A$, т. е. $\beta \in \overline{f(A)}$. Итак, пусть $\alpha \preceq \beta$. Так как множество $Int(\overline{f(A)})$ открыто, то $\beta \in Int(\overline{f(A)}) \subseteq \overline{f(A)}$, т. е. действительно $\beta \in \overline{f(A)}$, что и требовалось доказать. □

Таким образом, если дана модель $\mathcal{K} = (K, \preceq, \Vdash)$, то с ней естественным образом связаны псевдобулева алгебра открытых подмножеств частично упорядоченного множества K и естественная оценка f в этой алгебре. При этом, как видно из теоремы 44, значение произвольной формулы A при этой оценке есть в точности множество $f(A)$, состоящее из всех тех элементов $\alpha \in K$, для которых выполняется условие $\alpha \Vdash A$. Отсюда, в частности, вытекает следующая теорема.

Теорема 45. *Формула истинна в модели $\mathcal{K} = (K, \preceq, \Vdash)$ тогда и только тогда, когда она принимает значение 1 в псевдобулевой алгебре открытых подмножеств множества K при естественной оценке.*

Мы видим, что семантика Крипке является в некотором смысле частным случаем алгебраической семантики, основанной на псевдобулевых алгебрах. Установленная связь между моделями Крипке и псевдобулевыми алгебрами позволяет получить некоторые важные теоремы, касающиеся семантики Крипке, используя аналогичные результаты о псевдобулевых алгебрах. Докажем *теорему о корректности* ИИВ относительно моделей Крипке.

Теорема 46. *Если пропозициональная формула A выводима в ИИВ, то A истинна в любой модели Крипке.*

Доказательство. Пусть формула A выводима в ИИВ, и пусть дана модель $\mathcal{K} = (K, \preceq, \Vdash)$. В силу теоремы о корректности ИИВ относительно псевдобулевых алгебр (теорема 31), формула A истинна в любой псевдобулевой алгебре при любой оценке, в частности, формула A принимает значение 1 в псевдобулевой алгебре открытых подмножеств множества K при оценке f. В силу теоремы 45 в этом случае формула A истинна в модели $\mathcal{K}$, что и требовалось доказать. □

§7.3. Операции над шкалами Крипке

Рассмотрим две операции над шкалами Крипке. *Суммой* K_1+K_2 двух непересекающихся частично упорядоченных множеств K_1 и K_2 с отношениями порядка $\leq_1$ и $\leq_2$ назовем их объединение $K = K_1 \cup K_2$, упорядоченное следующим отношением: $x \leq y \Leftrightarrow (\exists i \in \{1, 2\})\, [x, y \in K_i \,\&\, x \leq_i y]$. Очевидно, что такое отношение $\leq$ является частичным порядком на K.

Теорема 47. *Псевдобулева алгебра открытых подмножеств суммы частично упорядоченных множеств K_1 и K_2 изоморфна прямому произведению алгебр открытых подмножеств множеств K_1 и K_2.*

Доказательство. Пусть K — сумма частично упорядоченных множеств K_1 и K_2. Алгебру открытых подмножеств множества K_1 обозначим через A_1, а алгебру открытых подмножеств множества K_2 — через A_2. Если X — открытое подмножество множества K, то очевидно, что $X_1 = X \cap K_1$ есть открытое подмножество множества K_1, а $X_2 = X \cap K_2$ — открытое подмножество множества K_2. Положим $\varphi(X) = \langle X_1, X_2\rangle$. Убедимся, что φ — изоморфизм семейства открытых подмножеств множества K и частично упорядоченного множества $A_1 \times A_2$. Очевидно, что φ — взаимно однозначное соответствие между указанными множествами. Проверим, что отображение φ сохраняет порядок. Пусть X, Y — открытые подмножества множества K, тогда

$$X \leq Y \Leftrightarrow X \subseteq Y \Leftrightarrow [X \cap K_1 \subseteq Y \cap K_1,\ X \cap K_2 \subseteq Y \cap K_2] \Leftrightarrow$$

$$\Leftrightarrow [X_1 \leq Y_1,\ X_2 \leq Y_2] \Leftrightarrow \langle X_1, X_2\rangle \leq \langle Y_1, Y_2\rangle \Leftrightarrow \varphi(X) \leq \varphi(Y),$$

что и требовалось доказать. □

По аналогии с суммой двух непересекающихся частично упорядоченных множеств определяется сумма $K_1 + \ldots + K_n$ попарно непересекающихся частично упорядоченных множеств $K_1, \ldots, K_n$. Псевдобулева алгебра открытых подмножеств суммы частично упорядоченных множеств $K_1, \ldots, K_n$ изоморфна прямому произведению $A_1 \times \ldots \times A_n$, где A_i — алгебра открытых подмножеств множества K_i $(i = 1, \ldots, n)$.

Если K — частично упорядоченное множество, то через K' обозначим множество $K \cup \{\alpha_0\}$, где $\alpha_0 \notin K$, упорядоченное следующим образом: для элементов из K сохраняется тот же порядок, что и в упорядоченном множестве K, и считается, что $\alpha_0 \leq x$ для любого $x \in K'$. Очевидно, что K' также является частично упорядоченным множеством.

Теорема 48. *Пусть A — алгебра открытых подмножеств частично упорядоченного множества K. Тогда алгебра открытых подмножеств множества K' изоморфна алгебре $\Gamma(A)$.*

Доказательство. Очевидно, что открытыми подмножествами множества K' являются все открытые подмножества множества K, а также само множество K', которое является наибольшим элементом в алгебре A' открытых подмножеств множества K'. При этом множество K оказывается гёделевым элементом этой алгебры. Пусть ω — гёделев элемент алгебры A. Рассмотрим отображение $\varphi : A' \to \Gamma(A)$, определяемое следующим образом:

$$\varphi(X) = \begin{cases} X, & \text{если } X \subset K, \\ \omega, & \text{если } X = K, \\ K, & \text{если } X = K'. \end{cases}$$

Очевидно, что φ является изоморфизмом алгебр A' и $\Gamma(A)$. $\square$

Рассмотрим следующую последовательность шкал Крипке K_n $(n = 0, 1, 2, \dots)$. Пусть K_0 — одноэлементное частично-упорядоченное множество. Если K_{n-1} уже определено, рассмотрим n попарно непересекающихся частично упорядоченных множеств $K_{n-1}^1, \dots, K_{n-1}^n$, изоморфных множеству K_{n-1}, и положим $K_n = (K_{n-1}^1 + \dots + K_{n-1}^n)'$.

Теорема 49. *Каково бы ни было натуральное число n, алгебра открытых подмножеств частично упорядоченного множества K_n изоморфна алгебре Яськовского J_n.*

Доказательство. Индукция по n. Пусть $n = 0$. Алгебра открытых подмножеств одноэлементного множества K состоит из элементов $0 = \emptyset$ и $1 = K$, причем $0 \leq 1$. Очевидно, что эта алгебра изоморфна двухэлементной алгебре Яськовского J_0. Предположим, что алгебра открытых подмножеств частично упорядоченного множества K_{n-1} изоморфна алгебре Яськовского

J_{n-1}, и докажем, что алгебра открытых подмножеств частично упорядоченного множества K_n изоморфна алгебре Яськовского J_n. В силу теоремы 47 алгебра открытых подмножеств частично упорядоченного множества $K^1_{n-1}+\ldots+K^n_{n-1}$ изоморфна алгебре J^n_{n-1}, а тогда по теореме 48 алгебра открытых подмножеств частично упорядоченного множества $K_n = (K^1_{n-1}+\ldots+K^n_{n-1})'$ изоморфна алгебре $\Gamma(J^n_{n-1})$, т. е. алгебре J_n, что и требовалось доказать. □

§7.4. Полнота ИИВ относительно моделей Крипке

Пусть F — простая импликация $K \supset Z$, где Z — переменная, K — простая конъюнкция, т. е. конъюнкция формул вида i) P; ii) $\neg P$; iii) $P \supset Q$; iv) $P \supset Q \vee R$; v) $P \,\&\, Q \supset R$; vi) $(P \supset Q) \supset R$, где P, Q, R — переменные. *Рангом* простой импликации F назовем количество конъюнктивных членов вида vi) в простой конъюнкции K. Модель Крипке $\mathcal{K}$ будем называть *строгой контрмоделью* для простой импликации F, если $\mathcal{K} \models K$, $\mathcal{K} \not\models Z$.

Напомним, что последовательность шкал Крипке K_n определяется следующим образом: K_0 — одноэлементное частично упорядоченное множество; $K_{n+1} = (\underbrace{K_n + \ldots + K_n}_{n+1})'$.

Теорема 50. *Пусть F — простая импликация, d — ее ранг. Тогда либо формула F выводима в ИИВ, либо существует строгая контрмодель для F на шкале Крипке K_d.*

Доказательство. Пусть s — количество переменных в простой импликации F. Будем доказывать утверждение индукцией по числу $m = d + s$.

Пусть $m = 1$. Это означает, что $d = 0$, т. е. в K нет конъюнктивных членов вида vi), и $s = 1$, т. е. в F используется только одна переменная Z. Возможны два случая: 1) в K есть конъюнктивный член вида i), т. е. Z; 2) в K нет конъюнктивных членов вида i). В первом случае F выводима в ИИВ. Во втором случае модель Крипке на шкале $K_0 = \{\alpha_0\}$, где $\alpha_0 \not\Vdash Z$, является строгой контрмоделью для F.

Допустим, что утверждение верно для $m \leq k$, и докажем его для $m = k+1$. Пусть F — простая импликация ранга d, и она содержит s переменных, так что $d + s = k + 1$. Рассмотрим случай, когда в K нет конъюнктивных членов вида i). Пусть

$$(P_1 \supset Q_1) \supset R_1, \ldots, (P_d \supset Q_d) \supset R_d$$

суть все конъюнктивные члены вида vi) в K. Если $1 \leq j \leq d$, то через K^j обозначим простую конъюнкцию, полученную вычеркиванием из K конъюнктивного члена $(P_j \supset Q_j) \supset R_j$. Через F^j обозначим простую импликацию $P_j \,\&\, (Q_j \supset R_j) \,\&\, K^j \supset Q_j$. Очевидно, что для каждого $j = 1, \ldots, d$ ранг F^j равен $d - 1$, а количество переменных равно s, так что для этой формулы параметр m равен k, и можно воспользоваться индуктивным предположением: либо F^j выводима в ИИВ, либо существует строгая контрмодель для F^j на шкале K_{d-1}.

Рассмотрим случай, когда для некоторого $j = 1, \ldots, d$ формула F^j выводима в ИИВ.

Лемма 5. *Каково бы ни было $j = 1, \ldots, d$, если F^j выводима в ИИВ, то $F \sim R_j \,\&\, K^j \supset Z$.*

Доказательство. Докажем, что в интуиционистском исчислении высказываний выводима импликация $F \supset (R_j \,\&\, K^j \supset Z)$. Учитывая строение формулы F и теорему о дедукции, достаточно доказать, что

$$((P_j \supset Q_j) \supset R_j) \,\&\, K^j \supset Z,\ R_j \,\&\, K^j \vdash Z.$$

Но это очевидно, так как $R_j \vdash (P_j \supset Q_j) \supset R_j$.

Докажем, что в интуиционистском исчислении высказываний выводима импликация $(R_j \,\&\, K^j \supset Z) \supset F$. Учитывая строение формулы F и теорему о дедукции, достаточно доказать, что

$$R_j \,\&\, K^j \supset Z,\ ((P_j \supset Q_j) \supset R_j) \,\&\, K^j \vdash Z. \tag{7.3}$$

Заметим, что формула $P_j \,\&\, (Q_j \supset R_j)$ эквивалентна в ИИВ формуле $P_j \,\&\, ((P_j \supset Q_j) \supset R_j)$, так что из выводимости формулы F^j вытекает $P_j \,\&\, ((P_j \supset Q_j) \supset R_j) \,\&\, K^j \vdash Q_j$. Отсюда и из теоремы о дедукции вытекает $((P_j \supset Q_j) \supset R_j) \,\&\, K^j \vdash P_j \supset Q_j$. Значит, $((P_j \supset Q_j) \supset R_j) \,\&\, K^j \vdash R_j$. Отсюда немедленно следует (7.3). □

Итак, формула F эквивалентна простой импликации $R_j \mathbin{\&} K^j \supset Z$. Очевидно, что ранг формулы $R_j \mathbin{\&} K^j \supset Z$ равен $d-1$, а количество переменных в ней не превосходит s, так что показатель m для этой формулы не превосходит k, и для нее верно доказываемое утверждение: либо она выводима в интуиционистском исчислении высказываний, либо существует строгая контрмодель для F на шкале Крипке K_{d-1}. В первом случае в силу леммы 5 формула F также выводима в интуиционистском исчислении высказываний, и доказываемое утверждение для нее верно. Если же для формулы $R_j \mathbin{\&} K^j \supset Z$ имеется строгая контрмодель $\mathcal{K}$ на шкале Крипке K_{d-1}, то $\mathcal{K}$ является также строгой контрмоделью для формулы F. Действительно, так как $R_j \vdash (P_j \supset Q_j) \supset R_j$ и $\mathcal{K} \models (R_j \mathbin{\&} K^j)$, то

$$\mathcal{K} \models K,\ \mathcal{K} \not\models Z. \tag{7.4}$$

Определим модель Крипке $\mathcal{K}'$ на шкале

$$K_d = (\underbrace{K_{d-1} + \ldots + K_{d-1}}_{d})'$$

с наименьшим элементом α_0 следующим образом. Если α — элемент шкалы K_d, отличный от α_0, то он принадлежит одному из слагаемых K_{d-1}. Полагаем $\alpha \Vdash P$ в модели $\mathcal{K}'$, если и только это условие выполняется в модели $\mathcal{K}$. Положим $\alpha_0 \Vdash P \Leftrightarrow \mathcal{K} \models P$ для каждой переменной P. Докажем, что для любой пропозициональной формулы A выполняется условие: $\mathcal{K}' \models A \Leftrightarrow \mathcal{K} \models A$. Заметим, что $\mathcal{K}' \models A$ означает $\alpha_0 \Vdash A$, так что из $\mathcal{K}' \models A$ следует $\mathcal{K} \models A$. Поэтому достаточно доказать, что $\mathcal{K} \models A \Rightarrow \alpha_0 \Vdash A$. Если A — пропозициональная переменная, то это утверждение вытекает из определения модели $\mathcal{K}'$. Рассмотрим случай, когда формула A имеет вид $B \mathbin{\&} C$, причем для формул B и C выполняются условия

$$\mathcal{K} \models B \Rightarrow \alpha_0 \Vdash B;\ \mathcal{K} \models C \Rightarrow \alpha_0 \Vdash C. \tag{7.5}$$

Пусть $\mathcal{K} \models (B \mathbin{\&} C)$. Тогда $\mathcal{K} \models B$ и $\mathcal{K} \models C$, следовательно, $\alpha_0 \Vdash B$ и $\alpha_0 \Vdash C$, т. е. $\alpha_0 \Vdash (B \mathbin{\&} C)$, что и требовалось доказать. Аналогично рассматривается случай, когда A имеет вид $B \vee C$ для некоторых формул B и C. Рассмотрим случай, когда A имеет вид $B \supset C$, причем выполняются условия (7.5). Пусть

$$\mathcal{K} \models (B \supset C). \tag{7.6}$$

Докажем, что $\alpha_0 \Vdash (B \supset C)$, т. е. $\beta \Vdash B \Rightarrow \beta \Vdash C$ для любого элемента β шкалы K_d. Это утверждение очевидно, если $\beta \neq \alpha_0$. Пусть $\alpha_0 \Vdash B$. Тогда $\mathcal{K} \models B$ и в силу (7.6) $\mathcal{K} \models C$, а тогда в силу (7.5) $\alpha_0 \Vdash C$, что и требовалось доказать. Случай, когда A имеет вид $\neg B$, рассматривается аналогично.

В силу только что доказанного из (7.4) следует $\mathcal{K}' \models K$ и $\mathcal{K}' \not\models Z$, т. е. $\mathcal{K}'$ является строгой контрмоделью для F.

Рассмотрим случай, когда не существует такого $j = 1, \ldots, d$, что формула F^j выводима в интуиционистском исчислении высказываний. Тогда для каждой из формул F^j существует строгая контрмодель $\mathcal{K}_j$ на шкале Крипке K_{d-1}. Заметим, что шкала каждой модели $\mathcal{K}_j$ имеет наименьший элемент α_j, причем

$$\alpha_j \Vdash P_j,\ \alpha_j \Vdash (Q_j \supset R_i),\ \alpha_j \Vdash K^j,\ \alpha_j \nVdash Q_j. \tag{7.7}$$

Зададим модель Крипке $\mathcal{K} = (\mathcal{K}_1 + \cdots + \mathcal{K}_d)'$ на шкале Крипке K_d с наименьшим элементом α_0. Если α — элемент шкалы K_d, отличный от α_0, то он принадлежит шкале одного из слагаемых $\mathcal{K}_j$. Полагаем $\alpha \Vdash P$ в модели $\mathcal{K}$, если и только это условие выполняется в модели $\mathcal{K}_j$. Положим $\alpha_0 \nVdash P$ для любой переменной P. Докажем, что $\mathcal{K}$ является строгой контрмоделью для формулы $K \supset Z$, т. е. $\alpha_0 \Vdash K$ и $\alpha_0 \nVdash Z$. Последнее условие очевидно выполнено. Докажем, что $\alpha_0 \Vdash K$. Сначала покажем, что для любого конъюнктивного члена G вида ii)–v) простой конъюнкции K имеет место $\mathcal{K} \models G$. Пусть, например, формула G имеет вид iii). Докажем, что $\alpha_0 \Vdash G$, т. е. $\forall \beta\, [\beta \Vdash P \Rightarrow \beta \Vdash Q]$. Условие $\beta \Vdash P \Rightarrow \beta \Vdash Q$ очевидно выполнено, если $\beta = \alpha_0$. Если же β не совпадает с α_0 и принадлежит шкале модели $\mathcal{K}_j$, то это условие выполнено в силу (7.7) и того факта, что $\alpha_j \preceq \beta$ и G является конъюнктивным членом формулы K^j. Аналогично рассматриваются другие случаи. Докажем теперь, что $\alpha_0 \Vdash ((P_k \supset Q_k) \supset R_k)$ для любого $k = 1, \ldots, d$. Пусть число k фиксировано. Требуется доказать, что для любого β выполнено условие: если $\beta \Vdash (P_k \supset Q_k)$, то $\beta \Vdash R_k$. Это условие выполнено, если $\beta = \alpha_0$. Действительно, как следует из (7.7), $\alpha_k \nVdash (P_k \supset Q_k)$, следовательно, $\alpha_0 \nVdash (P_k \supset Q_k)$. Если же β не совпадает с α_0 и принадлежит шкале модели $\mathcal{K}_j$ для $j \neq k$, то это условие выполнено в силу (7.7) и того факта, что $\alpha_j \preceq \beta$ и $(P_k \supset Q_k) \supset R_k$ является конъюнктивным членом формулы K^j. Пусть β принадлежит шкале модели $\mathcal{K}_k$, так что $\alpha_k \preceq \beta$. Отсюда следует, что $\beta \Vdash P_k$ и $\beta \Vdash (Q_k \supset R_k)$. Пусть $\beta \Vdash (P_k \supset Q_k)$. Тогда очевидно $\beta \Vdash Q_k$ и далее $\beta \Vdash R_k$, что и требовалось доказать. Таким образом, случай, когда в K нет конъюнктивных членов вида i), полностью рассмотрен.

Теперь рассмотрим случай, когда в K есть конъюнктивный член вида i). Пусть это переменная P. Если переменная P совпадает с переменной Z, то простая импликация F выводима, и утверждение доказано. Если переменная P отлична от Z и не входит в другие конъюктивные члены из K, то формула F дедуктивно эквивалентна простой импликации $K' \supset Z$, где K' — простая конъюнкция, полученная вычеркиванием из K конъюнктивного члена P. Заметим, что $d(F') = d(F)$, $s(F') = s(F) - 1$, так что для формулы F' значение параметра m равно k, и можно применить индуктивное предположение: либо формула F' выводима, либо для нее существует строгая контрмодель $\mathcal{K}$ на шкале Крипке K_d с наименьшим элементом α_0. В первом случае формула F также выводима, а во втором в модели $\mathcal{K}$ можно положить $\alpha_0 \Vdash P$ и получить строгую контрмодель для простой импликации F.

Рассмотрим случай, когда P входит и в другие конъюнктивные члены из K. Если она входит в конъюнктивный член вида ii), то в K есть конъюнктивные члены P и $\neg P$, а тогда формула F выводима. Пусть P входит в конъюнктивный член вида iii). Тогда с точностью до порядка конъюнктивных членов в K есть подформула $P \,\&\, (P \supset Q)$ или $P \,\&\, (Q \supset P)$. Первая эквивалентна формуле $P \,\&\, Q$, вторая — формуле P. Сделав эквивалентную замену, мы получим простую конъюнкцию K', в которой количество конъюнктивных членов, содержащих переменную P, на единицу меньше, чем в K.

Если P входит в конъюнктивный член вида v), то с точностью до порядка конъюнктивных членов в K есть подформула $P \,\&\, (P \,\&\, Q \supset R)$, или $P \,\&\, (Q \,\&\, P \supset R)$, или $P \,\&\, (Q \,\&\, R \supset P)$. Первые две из них эквивалентны формуле $P \,\&\, (Q \supset R)$, а третья — формуле P. Сделав эквивалентную замену, мы и в этом случае получим простую конъюнкцию K', в которой количество конъюнктивных членов, содержащих переменную P, на единицу меньше, чем в K.

Если P входит в конъюнктивный член вида vi), то с точностью до порядка конъюнктивных членов в K есть подформула $P \mathbin{\&} ((P \supset Q) \supset R)$, $P \mathbin{\&} ((Q \supset P) \supset R)$ или $P \mathbin{\&} ((Q \supset R) \supset P)$. Первая эквивалентна формуле $P \mathbin{\&} (Q \supset R)$, вторая эквивалентна формуле $P \mathbin{\&} R$, а третья — формуле P. Сделав эквивалентную замену, мы снова получим простую конъюнкцию K', в которой количество конъюнктивных членов, содержащих переменную P, на единицу меньше, чем в K.

Наконец, рассмотрим случай, когда P входит в конъюнктивный член вида iv). Тогда с точностью до порядка конъюнктивных членов в K есть подформула $P \mathbin{\&} (P \supset Q \vee R)$, или $P \mathbin{\&} (Q \supset P \vee R)$, или $P \mathbin{\&} (Q \supset R \vee P)$. Вторая и третья формулы эквивалентны формуле P. Сделав эквивалентную замену, мы получим простую конъюнкцию K', в которой количество конъюнктивных членов, содержащих переменную P, на единицу меньше, чем в K. Первая формула эквивалентна формуле $P \mathbin{\&} (Q \vee R)$. Сделав в F эквивалентную замену, мы получим формулу вида $P \mathbin{\&} (Q \vee R) \mathbin{\&} K' \supset Z$, где K' — простая конъюнкция. Проделав эту процедуру со всеми конъюнктивными членами из K вида $P \mathbin{\&} (P \supset Q \vee R)$, мы получим формулу вида

$$P \mathbin{\&} (P_{i_1} \vee P_{j_1}) \mathbin{\&} \ldots \mathbin{\&} (P_{i_m} \vee P_{j_m}) \mathbin{\&} K' \supset Z, \tag{7.8}$$

где K' — простая конъюнкция. Эта формула эквивалентна в интуиционистском исчислении высказываний конъюнкции простых импликаций

$$P \mathbin{\&} P_{k_1} \mathbin{\&} \ldots \mathbin{\&} P_{k_m} \mathbin{\&} K' \supset Z, \tag{7.9}$$

где $k_p \in \{i_p, j_p\}$ $(p = 1, \ldots, m)$, причем переменная P имеет единственное вхождение в эту формулу. Каждая формула (7.9) дедуктивно эквивалентна формуле

$$P_{k_1} \mathbin{\&} \ldots \mathbin{\&} P_{k_m} \mathbin{\&} K' \supset Z, \tag{7.10}$$

в которой переменных на одну меньше, чем в простой импликации F, а ранг тот же, поэтому можно применить индуктивное предположение: каждая из формул (7.10) либо выводима в интуиционистском исчислении высказываний, либо для нее существует строгая контрмодель на шкале Крипке K_d с наименьшим элементом α_0. Если все формулы (7.10) выводимы, то очевидно выводима и формула F. Допустим, что какая-то из формул (7.10) невыводима. Тогда для этой формулы существует строгая контрмодель $\mathcal{K}$ на шкале K_d. Для этой модели выполняются условия $\alpha_0 \Vdash P_{k_p}$ $(p = 1, \ldots, m)$, $\alpha_0 \Vdash K'$, $\alpha_0 \nVdash Z$. Положим $\alpha_0 \Vdash P$. Очевидно, что в полученной модели посылка формулы (7.8) истинна в момент α_0, а заключение не истинно. Но поскольку посылка формулы (7.8) эквивалентна простой конъюнкции K, то $\alpha_0 \Vdash K$, а так как $\alpha_0 \nVdash Z$, то $\mathcal{K}$ — строгая контрмодель для простой импликации F. $\square$

Пропозициональное исчисление называется *разрешимым*, если существует алгоритм, который по любой пропозициональной формуле позволяет установить, выводима ли эта формула в данном исчислении.

Теорема 51. *Интуиционистское исчисление высказываний разрешимо.*

Доказательство. Пусть дана пропозициональная формула A. В силу теоремы 27 она дедуктивно эквивалентна простой импликации F, которая строится эффективно по формуле A. Пусть d — ранг простой импликации F. Число d можно вычислить, имея формулу F. Если формула F истинна в алгебре Яськовского J_d, то она, а следовательно и формула A, выводима в ИИВ, ибо в противном случае она опровергалась бы в алгебре J_d в силу теоремы 49. Если же формула F опровергается в алгебре J_d, то она невыводима, следовательно, и формула A невыводима в интуиционистском исчислении высказываний. $\square$

Упражнения

1. Построить контрмодели для формул $P \vee \neg P$, $\neg\neg P \supset P$, $\neg P \vee \neg\neg P$, $(P \supset Q) \vee (Q \supset P)$, $((P \supset Q) \supset P) \supset P$, $(P \supset Q) \supset (\neg P \vee Q)$.

2. Применить описанную в этой главе технику для выявления выводимости в ИИВ следующих формул или построения контрмоделей для них: $\neg(P \vee Q) \supset (\neg P \,\&\, \neg Q)$, $\neg(P \,\&\, Q) \supset (P \vee Q)$, $(\neg P \vee Q) \supset (P \supset Q)$.

Глава 8

Интуиционистское исчисление предикатов (ИИП)

§8.1. Интуиционизм и элементарные языки

Прежде чем приступить к разработке интуиционистской логики предикатов, нужно осмыслить, что такое элементарный язык с интуиционистской точки зрения. Нет проблем с рассмотрением какой-нибудь непустой предметной области M как множества, заданного правилом порождения его элементов или свойством, выделяющим его элементы среди элементов другого, ранее заданного множества. Не вызывает трудностей и попытка дать имена некоторым элементам M. А как трактовать понятие предиката, заданного на M? Вспомним определение понятия предиката в классической логике. В § 3.4 мы рассматривали несколько возможных вариантов такого определения. Во-первых, предикат можно трактовать как высказывательную форму $P(x_1, \ldots, x_n)$, и при этом с ним связана функция, сопоставляющая каждому набору $a_1, \ldots, a_n$ значений свободных переменных $x_1, \ldots, x_n$ высказывание $P(a_1, \ldots, a_n)$. Такое понимание предиката вполне приемлемо с точки зрения интуиционизма. Но затем, рассматривая лишь истинностные значения высказываний $P(a_1, \ldots, a_n)$, мы приходили к пониманию предиката как произвольной функции, принимающей значения 1 («истина») и 0 («ложь»). Этот шаг интуиционистски неприемлем уже потому, что истинностное значение не является обязательным атрибутом произвольного высказывания, ведь, как мы знаем, бывают и непроверенные высказывания. При этом мы не можем ввести в рассмотрение непроверенность как третье истинностное значение, ибо это состояние высказывания, вообще говоря, является временным. Итак, мы должны остановиться на трактовке предиката как высказывательной формы, записанной на подходящем языке, понятном с интуиционистской точки зрения.

Больше трудностей возникает при рассмотрении понятия произвольной функции. Мы говорим, что задана n-местная функция f на M, если каждому набору $a_1, \ldots, a_n$ элементов M сопоставлен элемент из M, обозначаемый $f(a_1, \ldots, a_n)$. Интуиционистски это означает, что имеется общее правило, сопоставляющее каждому набору $a_1, \ldots, a_n$ элемент $f(a_1, \ldots, a_n)$. Иными словами, можно рассматривать только функции, для которых имеется правило их вычисления. Однако возможно другое представление о произвольной функции, которого мы будем придерживаться. Вместо n-местной функции f будем рассматривать $(n+1)$-местный предикат $F(x_1, \ldots, x_n, y)$, означающий $f(x_1, \ldots, x_n) = y$. Так понятие функции перестает быть исходным, а сводится к понятию предиката. Поэтому в рамках интуиционистской логики мы будем рассматривать лишь элементарные языки, сигнатура которых не содержит функциональных символов.

Интуиционистская интерпретация элементарного языка Ω состоит в выборе непустой предметной области M и сопоставлении константам из Ω элементов из M, а предикатным символам — высказывательных форм с соответствующим числом параметров, записанных на подходящем понятном языке. Тогда каждая замкнутая формула сигнатуры Ω превращается в высказывание, интуиционистткий смысл которого определяется интуиционистким пониманием логических связок и кванторов.

Приведенное описание интуиционистской семантики элементарных языков ни в коем случае нельзя считать математически строгим. Можно сказать, что у нас есть лишь интуитивное понимание интуиционистской семантики элементарных языков. Тем не менее, таких представлений достаточно, чтобы начать разработку формальных систем интуиционистской логики предикатов.

§8.2. Схемы аксиом и правила вывода ИИП

Пусть фиксирована сигнатура Ω, содержащая лишь константы и предикатные символы. *Интуиционистское исчисле-*

ние предикатов (ИИП) в сигнатуре Ω задается следующими схемами аксиом:

1. $A \supset (B \supset A)$;
2. $(A \supset B) \supset ((A \supset (B \supset C)) \supset (A \supset C))$;
3. $A \,\&\, B \supset A$;
4. $A \,\&\, B \supset B$;
5. $A \supset (B \supset A \,\&\, B)$;
6. $A \supset A \vee B$;
7. $B \supset A \vee B$;
8. $(A \supset C) \supset ((B \supset C) \supset (A \vee B \supset C))$;
9. $(A \supset B) \supset ((A \supset \neg B) \supset \neg A)$;
10. $A \supset (\neg A \supset B)$;
11. $\forall v\, A(v) \supset A(t)$;
12. $A(t) \supset \exists v\, A(v)$.

В схемах 11 и 12 $A(v)$ — формула языка Ω, v — переменная, t — терм, свободный для v в $A(v)$. Правила вывода ИИП:

(I) $\dfrac{A, A \supset B}{B}$ (modus ponens; MP);

(II) $\dfrac{A \supset B}{\exists v\, A \supset B}$ (удаление квантора существования);

(III) $\dfrac{B \supset A}{B \supset \forall v\, A}$ (введение квантора всеобщности).

В правилах (II) и (III) B не содержит свободных вхождений v.

В дальнейшем ИИП в сигнатуре Ω будем обозначать посредством ИИП$_\Omega$, а запись ИИП без указания сигнатуры будем употреблять в том случае, если сигнатура может быть произвольной или определяется из контекста.

Как и для классического исчисления предикатов, определяются понятия квазивывода и вывода из гипотез. Для ИИП имеет место *теорема о дедукции*: каковы бы ни были множество формул Γ и формулы Φ, Ψ, если $\Gamma \cup \{\Phi\} \vdash \Psi$, то $\Gamma \vdash \Phi \supset \Psi$. Эта теорема доказывается дословно так же, как и теорема о дедукции для классического исчисления предикатов (теорема 16).

Пусть фиксирована интерпретация языка Ω. Тогда аксиомы ИИП становятся интуиционистски истинными высказываниями или высказывательными формами, замыкания которых кванторами всеобщности по всем параметрам интуиционистски истинны в этой интерпретации, а правила вывода сохраняют интуиционистскую истинность. Для схем аксиом 1 – 10 этот факт отмечался при рассмотрении ИИВ. Рассмотрим схему 11.

Пусть $A(v)$ содержит свободно лишь v, а t — константа c. В данной интерпретации $A(v)$ задает одноместный предикат $P(v)$, а значением c является элемент $m \in M$. Истинность формулы $\forall v\, A(v) \supset A(t)$ означает существование общего метода, позволяющего любое обоснование для $\forall v\, P(v)$ преобразовать в обоснование для $P(m)$. Пусть дано обоснование для $\forall v\, P(v)$, т. е. общий метод, позволяющий для любого $a \in M$ получить обоснование для $P(a)$. Применим этот метод к m и получим обоснования для $P(m)$, что и требовалось. В общем случае $A(v)$ может содержать свободные переменные, отличные от v, а терм t может быть переменной u. Пусть $w_1, \ldots, w_k$ — все параметры формулы $\forall v\, A(v) \supset A(t)$. Требуется доказать, что формула $\forall w_1 \ldots \forall w_k\, (\forall v\, A(v) \supset A(t))$ истинна в любой интерпретации. Пусть фиксирована интерпретация языка Ω. Придадим переменным $w_1, \ldots, w_k$ значения из предметной области. Тогда $A(v)$ превратится в одноместный предикат $P(v)$, а значением терма t будет элемент m. Выше был описан метод, позволяющий из обоснования для $\forall v\, P(v)$ получить обоснование для $P(m)$. Следовательно, высказывание $\forall w_1 \ldots \forall w_k\, (\forall v\, A(v) \supset A(t))$ интуиционистски истинно.

Нетрудно провести аналогичные рассуждения, показывающие, что схема 12 также является схемой интуиционистски истинных высказываний или тождественно истинных высказывательных форм (см. упражнение 1). Правило MP, очевидно, сохраняет интуиционистсткую истинность. Покажем, что правило (II) сохраняет интуиционистскую истинность. Пусть высказывание $\forall w_1 \ldots \forall w_k\, \forall v\, (A(v) \supset B)$, где $w_1, \ldots, w_k$ — все параметры формулы $A(v) \supset B$, отличные от v, интуиционистски истинно в данной интерпретации. Докажем, что высказывание

$$\forall w_1 \ldots \forall w_k\, (\exists v\, A \supset B) \tag{8.1}$$

также истинно в этой интерпретации. Придадим переменным $w_1, \ldots, w_k$ произвольные значения $m_1, \ldots, m_k$ из предметной области. Тогда формула $A(v)$ превратится в некоторый одноместный предикат $P(v)$, а формула B — в некоторое высказывание Q. Докажем, что истинно высказывание $\exists v\, P(v) \supset Q$. Для этого надо описать общий метод, который позволяет из любого обоснования высказывания $\exists v\, P(v)$ получить обоснование высказывания Q. Итак, пусть дано обоснование высказывания

$\exists v\, P(v)$. Это означает, что дан некоторый элемент m из предметной области и обоснование высказывания $P(m)$. В силу истинности высказывания $\forall w_1 \ldots \forall w_k\, \forall v\, (A(v) \supset B)$, можно найти обоснование высказывания $P(m) \supset Q$. Теперь, имея обоснование высказывания $P(m)$, мы получаем обоснование высказывания Q, что и требовалось. В приведенном рассуждении описанное обоснование высказывания $\exists v\, P(v) \supset Q$ не зависело от элементов $m_1, \ldots, m_k$, так что истинность высказывания (8.1) доказана.

Совершенно аналогично доказывается, что правило (III) сохраняет интуиционистскую истинность (см. упражнение 2).

Рассмотрим одну общую конструкцию. Пусть Ω — сигнатура, содержащая константу c. Через Ω' обозначим сигнатуру, полученную удалением c из Ω.

Предложение 25. *Пусть $\Phi_1, \ldots, \Phi_n, \Phi$ — вывод в ИИП$_\Omega$ формулы Φ из множества Γ, состоящего из высказываний, не содержащих константу c, и пусть w — переменная, не входящая ни в одну из формул этого вывода. В каждой формуле Ψ из этого вывода заменим все вхождения c на w, и полученную формулу обозначим Ψ°. Тогда $\Phi_1^\circ, \ldots, \Phi_n^\circ, \Phi^\circ$ — вывод в ИИП$_{\Omega'}$ формулы Φ° из Γ.*

Доказательство. Очевидно, что если $\Psi \in \Gamma$, то Ψ° совпадает с Ψ. Если Ψ — аксиома ИИП$_\Omega$, входящая в данный вывод, то Ψ° — аксиома ИИП$_{\Omega'}$. Действительно, если аксиома Ψ получена по одной из схем аксиом 1 – 10, то Ψ° является аксиомой, полученной по той же схеме. Например, если Ψ получена по схеме аксиом 1 и имеет вид $A \supset (B \supset A)$, то Ψ° имеет вид $A^\circ \supset (B^\circ \supset A^\circ)$. Если Ψ получена по схеме аксиом 11 и имеет вид $\forall v\, A(v) \supset A(t)$, где t — переменная или константа, отличная от c, то Ψ° имеет вид $\forall v\, A^\circ(v) \supset A^\circ(t)$ и является аксиомой ИИП$_{\Omega'}$. Если Ψ имеет вид $\forall v\, A(v) \supset A(c)$, то Ψ° имеет вид $\forall v\, A^\circ(v) \supset A^\circ(w)$ и также является аксиомой ИИП$_{\Omega'}$, так как в $A^\circ(v)$ нет кванторов по w, и потому w свободна для v в этой формуле. Аналогично доказывается, что если Ψ получена по схеме аксиом 12, то Ψ° получается по той же схеме. Если формула Ψ получена по правилу MP из формул Ψ' и $\Psi' \supset \Psi$, то Ψ° получается по тому же правилу из Ψ'° и формулы $(\Psi' \supset \Psi)^\circ$, имеющей вид $\Psi'^\circ \supset \Psi^\circ$. Если формула Ψ имеет вид $\exists v\, A(v) \supset B$ и получена по правилу удаления квантора существования из формулы Ψ' вида $A(v) \supset B$, то Ψ° имеет вид $A^\circ(v) \supset B^\circ$ и получается по тому же правилу из формулы Ψ'°, имеющей вид $A^\circ(v) \supset B^\circ$. Аналогично доказывается, что если формула Ψ получена по правилу введения квантора всеобщности из формулы Ψ', то Ψ° получается по тому же правилу из формулы Ψ'°. Теперь доказательство предложения завершается несложной индукцией по длине вывода формулы Φ из Γ в ИИП$_\Omega$. $\square$

§8.3. Погружение классического исчисления предикатов в интуиционисткое

Пусть фиксирован элементарный язык сигнатуры Ω. Индукцией по построению для каждой формулы A определим формулу A^*. Если A — атом, то A^* есть $\neg\neg A$. Если A имеет вид $B\lambda C$, где $\lambda \in \{\&, \vee, \supset\}$, то A^* есть $\neg\neg(B^*\lambda C^*)$. Если A имеет вид $\neg B$, то A^* есть $\neg B^*$. Если A имеет вид $\kappa x B$, где $\kappa \in \{\forall, \exists\}$, то A^* есть $\neg\neg\kappa x B^*$.

Теорема 52. *Формула A выводима в классическом исчислении предикатов тогда и только тогда, когда формула A^* выводима в ИИП.*

Доказательство. Если формула A^* выводима в интуиционистском исчислении предикатов, то она выводима в классическом исчислении предикатов. Формулы A и A^* эквивалентны в классическом исчислении предикатов. Следовательно, формула A также выводима в классическом исчислении предикатов. Таким образом, если формула A^* выводима в интуиционистском исчислении предикатов, то формула A выводима в классическом исчислении предикатов.

Докажем, что если формула A выводима в классическом исчислении предикатов, то формула A^* выводима в интуиционистском исчислении предикатов. Пусть $B_1, \ldots, B_n$ — вывод формулы A в классическом исчислении предикатов. Докажем, что для любой формулы B_i формула B_i^* выводима в интуиционистском исчислении предикатов. Для этого достаточно показать, что: 1) для любой аксиомы B классического исчисления предикатов формула B^* выводима в интуиционистском исчислении предикатов; 2) если формула B получена по правилу MP из формул C и D, и формулы C^* и D^* выводимы в интуиционистском исчислении предикатов, то формула B^* выводима в интуиционистском исчислении предикатов; 3) если формула B получена по одному из правил Бернайса из формулы C, и формула C^* выводима в интуиционистском исчислении предикатов, то формула B^* выводима в интуиционистском исчислении предикатов.

Пусть B — аксиома, полученная по какой-нибудь схеме классического исчисления высказываний. Это означает, что B получается подстановкой формул $\Phi, \ldots$ языка Ω в пропозициональную тавтологию $A(P, \ldots)$, и B имеет вид $A(\Phi, \ldots)$. Формула B^* имеет вид $A^*(\Phi^*, \ldots)$, где $A^*(P, \ldots)$ — пропозициональная формула, полученная из формулы A навешиванием двойного отрицания $\neg\neg$ на каждую подформулу формулы A, не начинающуюся с символа $\neg$. Формула A^* имеет вид $\neg\neg C$, где C — тавтология. Так как формула C выводима в классическом исчислении высказываний, то в силу теоремы Гливенко формула $\neg\neg C$, т. е. A^*, выводима в ИИВ. Отсюда следует, что формула $A^*(\Phi^*, \ldots)$, т. е. B^*, выводима в интуиционистском исчислении предикатов.

Пусть B — аксиома вида $\forall v\, A(v) \supset A(t)$, где t — терм, свободный для v в $A(v)$. Тогда B^* есть $\neg\neg(\neg\neg\forall v\, A^*(v) \supset A^*(t))$. Так как в интуиционистском исчислении предикатов выводима любая формула вида $\Phi \supset \neg\neg\Phi$, то достаточно доказать выводимость в интуиционистском исчислении предикатов формулы $\neg\neg\forall v\, A^*(v) \supset A^*(t)$. Для этого в силу допустимости правила силлогизма достаточно доказать выводимость в интуиционистском исчислении предикатов формул

$$\neg\neg\forall v\, A^*(v) \supset \forall v\, A^*(v) \tag{8.2}$$

и

$$\forall v\, A^*(v) \supset A^*(t). \tag{8.3}$$

Формула (8.3) является аксиомой интуиционистского исчисления предикатов. Докажем выводимость формулы (8.2). Для этого в силу теоремы о дедукции достаточно вывести формулу $\forall v\, A^*(v)$ из гипотезы $\neg\neg\forall v\, A^*(v)$, для чего в силу правила

$\forall$-введения достаточно вывести из той же гипотезы формулу $A^*(v)$. Формула $A^*(v)$ имеет вид $\neg C(v)$ для некоторой формулы $C(v)$. Поэтому требуется доказать выводимость формулы $\neg C(v)$ из гипотезы $\neg\neg\forall v\,\neg C(v)$. Для этого в силу правила приведения к абсурду достаточно доказать противоречивость множества $\Gamma = \{\neg\neg\forall v\,\neg C(v),\ C(v)\}$. Для этого в свою очередь достаточно доказать выводимость из Γ формулы $\neg\forall v\,\neg C(v)$, для чего в силу правила приведения к абсурду достаточно доказать противоречивость множества $\Delta = \{\neg\neg\forall v\,\neg C(v),\ C(v),\ \forall v\,\neg C(v)\}$. Но очевидно, что из Δ выводима формула $\neg C(v)$ по правилу $\forall$-удаления, так что множество Δ действительно противоречиво. Таким образом, мы доказали, что формула B^* выводима в интуиционистском исчислении предикатов.

Пусть B есть аксиома вида $A(t) \supset \exists v A(v)$, где t — терм, свободный для переменной v в формуле $A(v)$. Тогда B^* есть формула $\neg\neg(A^*(t) \supset \neg\neg\exists v A^*(v))$. Так как в ИИП выводима любая формула вида $\Phi \supset \neg\neg\Phi$, то достаточно доказать выводимость в интуиционистском исчислении предикатов формулы $A^*(t) \supset \neg\neg\exists v A^*(v)$. По той же причине в силу правила силлогизма для этого досточно доказать выводимость формулы $A^*(t) \supset \exists v A^*(v)$, которая является аксиомой. Таким образом, мы доказали, что если B есть аксиома вида $A(t) \supset \exists v A(v)$, то формула B^* выводима в интуиционистском исчислении предикатов.

Пусть формула B получена по правилу MP из формул C и $C \supset B$, причем формулы C^* и $(C \supset B)^*$ выводимы в интуиционистском исчислении предикатов. Докажем, что формула B^* также выводима в интуиционистском исчислении предикатов. Формула $(C \supset B)^*$ имеет вид $\neg\neg(C^* \supset B^*)$. Если мы докажем выводимость формулы $C^* \supset B^*$ в интуиционистском исчислении предикатов из формулы $\neg\neg(C^* \supset B^*)$, то будет доказана и выводимость формулы B^*. Заметим, что формула B^* имеет вид $\neg D$ для некоторой формулы D. Мы докажем, что из формулы $\neg\neg(C^* \supset B^*)$, т. е. $\neg\neg(C^* \supset \neg D)$, выводима формула $C^* \supset B^*$, т. е. $C^* \supset \neg D$. В силу теоремы о дедукции и принципа приведения к абсурду достаточно доказать, что множество $\Gamma = \{\neg\neg(C^* \supset \neg D),\ C^*,\ D\}$ противоречиво. Для этого, в свою очередь, достаточно доказать, что из множества Γ выводима формула $\neg(C^* \supset \neg D)$, для чего, в силу правила приведения к абсурду, достаточно доказать противоречивость множества $\Delta = \{\neg\neg(C^* \supset \neg D), C^*, D, C^* \supset \neg D\}$. Но очевидно, что из Δ выводимы формулы D и $\neg D$, так что множество Δ действительно противоречиво. Таким образом, мы доказали, что если формула B получена по правилу MP из формул C и $C \supset B$, и при этом формулы C^* и $(C \supset B)^*$ выводимы в интуиционистском исчислении предикатов, то B^* также выводима в интуиционистском исчислении предикатов.

Пусть формула B имеет вид $C \supset \forall v\, A(v)$ и получена по правилу Бернайса из формулы $C \supset A(v)$, так что формула C не содержит свободных вхождений переменной v. Предположим, что формула $(C \supset A(v))^*$ выводима в интуиционистском исчислении предикатов, и докажем, что формула B^* также выводима в ИИП. Формула $(C \supset A(v))^*$ имеет вид $\neg\neg(C^* \supset A^*(v))$. Докажем, что из этой формулы выводима формула $C^* \supset A^*(v)$. Заметим, что формула $A^*(v)$ имеет вид $\neg D(v)$ для некоторой формулы $D(v)$. Таким образом, нам требуется доказать выводимость формулы $C^* \supset \neg D(v)$ из гипотезы $\neg\neg(C^* \supset \neg D(v))$. В силу теоремы о дедукции и правила приведения к абсурду для этого достаточно доказать противоречивость множества $\Gamma = \{\neg\neg(C^* \supset \neg D(v)), C^*, D(v)\}$. Для этого достаточно доказать выводимость из Γ формулы $\neg(C^* \supset \neg D(v))$, для чего в свою очередь достаточно доказать противоречивость множества $\Delta = \{\neg\neg(C^* \supset \neg D(v)), C^*, D(v), C^* \supset \neg D(v)\}$. Но очевидно, что из Δ выводятся формулы $D(v)$ и $\neg D(v)$, так что множество Δ действительно противоречиво. Таким образом, если формула $\neg\neg(C^* \supset A^*(v))$ выводима в интуиционистском исчислении предикатов, то формула $C^* \supset A^*(v)$ также выводима. Применяя к ней то же правило Бернайса, получим формулу $C^* \supset \forall v\, A^*(v)$. Очевидно, что из этой формулы выводима формула $\neg\neg(C^* \supset \neg\neg\forall v\, A^*(v))$, которая и есть формула B^*.

Пусть формула B имеет вид $\exists v\, A(v) \supset C$ и получена по правилу Бернайса из формулы $A(v) \supset C$, так что формула C не содержит свободных вхождений переменной v. Предположим, что формула $(A(v) \supset C)^*$ выводима в интуиционистском исчислении предикатов, и докажем, что формула B^* также выводима в интуиционистском исчислении предикатов. Формула

$(A(v) \supset C)^*$ имеет вид $\neg\neg(A^*(v) \supset C^*)$. Докажем, что из этой формулы выводима формула $A^*(v) \supset C^*$. Заметим, что C имеет вид $\neg D$ для некоторой формулы D, не содержащей свободно переменную v. Таким образом, требуется доказать выводимость $A^*(v) \supset \neg D$ из гипотезы $\neg\neg(A^*(v) \supset \neg D)$. В силу теоремы о дедукции и правила приведения к абсурду достаточно доказать противоречивость множества $\Gamma = \{\neg\neg(A^*(v) \supset \neg D),\ A^*(v),\ D\}$. Для этого достаточно доказать выводимость из Γ формулы $\neg(A^*(v) \supset \neg D)$, для чего в свою очередь достаточно доказать противоречивость множества

$$\Delta = \{\neg\neg(A^*(v) \supset \neg D),\ A^*(v),\ D,\ A^*(v) \supset \neg D\}.$$

Очевидно, что из Δ выводятся формулы D и $\neg D$, так что Δ противоречиво. Таким образом, если формула $\neg\neg(A^*(v) \supset \neg D)$ выводима в ИИП, то формула $A^*(v) \supset \neg D$ также выводима. Применяя к ней то же правило Бернайса, получим формулу $\exists v A^*(v) \supset \neg D$. Дважды применяя закон контрапозиции, получаем выводимость формулы $\neg\neg\exists v A^*(v) \supset \neg\neg\neg D$, из которой очевидно выводима формула $\neg\neg\exists v\, A^*(v) \supset \neg D$, т. е. формула $\neg\neg\exists v\, A^*(v) \supset C^*$, которая и есть B^*. $\square$

Упражнения

1. Доказать, что всякое высказывание вида $A(c) \supset \exists v\, A(v)$, где c — константа, истинно с интуционистской точки зрения.

2. Доказать, что если высказывание $\forall v\, (B \supset A(v))$ истинно с интуционистской точки зрения, то истинно и высказывание $B \supset \forall v\, A(v))$.

3. Доказать, что если в ИИП $\Gamma \cup \{A(v)\} \vdash B$, причем v не входит свободно в B и формулы из Γ, то $\Gamma \cup \{\exists v\, A(v)\} \vdash B$.

4. Доказать, что если в ИИП $\Gamma \vdash A(v)$, причем v не входит свободно в формулы из Γ, то $\Gamma \vdash \forall v\, A(v)$.

5. Доказать, что каковы бы ни были формула A, переменная v и формула B, не содержащая свободных вхождений v, следующие формулы выводимы в ИИП: $\exists v\, \neg A \supset \neg\forall v\, A$; $\neg\exists v\, A \supset \forall v\, \neg A$; $\forall v\, \neg A \supset \neg\exists v\, A$; $\forall v\, (A \supset B) \supset (\exists v\, A \supset B)$; $(\exists v\, A \supset B) \supset \forall v\, (A \supset B)$; $\exists v\, (A \supset B) \supset (\forall v\, A \supset B)$.

Глава 9

Модели Крипке для логики предикатов

§9.1. Интуиционистские модели Крипке для логики предикатов

Пусть Ω — элементарный язык без функциональных символов. Модель Крипке для языка Ω — это набор $\mathcal{K} = (K, \preceq, D, \Vdash)$, где $(K, \preceq)$ — частично упорядоченное множество (*шкала Крипке*), D — функция, каждому $\alpha \in K$ сопоставляющая непустое множество D_α, причем $D_\alpha \subseteq D_\beta$, если $\alpha \preceq \beta$. Если Ω содержит константу c, то ей сопоставляется объект $\bar{c}$, который принадлежит любому множеству D_α для $\alpha \in K$. В дальнейшем c отождествляется с элементом $\bar{c}$. Наконец, $\Vdash$ — некоторое соответствие между множеством K и множеством всех атомов вида $P(a_1, \ldots, a_n)$, где P есть (n-местный) предикатный символ сигнатуры Ω, а $a_1, \ldots, a_n$ — элементы множества $\bigcup\limits_{\alpha \in K} D_\alpha$, обладающее тем свойством, что если $\alpha \in K$, $P(a_1, \ldots, a_n)$ — атом указанного вида, и $\alpha \Vdash P(a_1, \ldots, a_n)$, то $\{a_1, \ldots, a_n\} \subseteq D_\alpha$, и если $\alpha \preceq \beta$, то $\beta \Vdash P(a_1, \ldots, a_n)$. Соответствие $\Vdash$ называется *оценкой* атомов в данной модели Крипке. Как и в случае моделей Крипке для логики высказываний, $\alpha \Vdash P(a_1, \ldots, a_n)$ читается «*α вынуждает* $P(a_1, \ldots, a_n)$» или «$P(a_1, \ldots, a_n)$ *истинно* в момент α».

Интуитивный смысл моделей Крипке для логики предикатов аналогичен смыслу моделей Крипке для логики высказываний. Элементы множества K можно трактовать как моменты времени. Множество D_α можно понимать как множество объектов, построенных к моменту α или доступных для исследования в этот момент. Условие $\alpha \preceq \beta \Rightarrow D_\alpha \subseteq D_\beta$ означает, что имеющиеся в данный момент объекты в будущем не исчезают, а остаются доступными для исследования. Интуитивно $\alpha \Vdash P(a_1, \ldots, a_n)$ означает, что к моменту α доказано утверждение $P(a_1, \ldots, a_n)$, причем доказанные утверждения остаются таковыми и в будущем, так что имеет место принцип сохранения истинности.

Соответствие $\Vdash$ между K и множеством атомов расширяется до соответствия $\Vdash$ между K и множеством высказываний следующим образом. Пусть $\alpha \in K$, а A — высказывание сигнатуры Ω, расширенной за счет констант для обозначения всех элементов D_α. Соответствие $\alpha \Vdash A$ задается индукцией по логической длине A. Для атомов оно уже определено. Далее полагаем:

$\alpha \Vdash (A \,\&\, B) \rightleftharpoons [\alpha \Vdash A$ и $\alpha \Vdash B]$;
$\alpha \Vdash (A \vee B) \rightleftharpoons [\alpha \Vdash A$ или $\alpha \Vdash B]$;
$\alpha \Vdash (A \supset B) \rightleftharpoons (\forall \beta \succeq \alpha)\, [\beta \nVdash A$ или $\beta \Vdash B]$;
$\alpha \Vdash \neg A \rightleftharpoons (\forall \beta \succeq \alpha)\, \beta \nVdash A$;
$\alpha \Vdash \exists v\, A(v) \rightleftharpoons (\exists a \in D_\alpha)\, \alpha \Vdash A(a)$;
$\alpha \Vdash \forall v\, A(v) \rightleftharpoons (\forall \beta \succeq \alpha)\, (\forall a \in D_\beta)\, \beta \Vdash A(a)$.

Здесь $\beta \succeq \alpha$ означает $\alpha \preceq \beta$, а $A(a)$ есть результат подстановки константы a вместо переменной v в формулу $A(v)$.

Определение $\alpha \Vdash A$ для пропозициональных связок не отличается от определения в случае моделей Крипке для логики высказываний. Определение этого соответствия для квантора существования вполне отвечает интуиционистскому его пониманию. Определение для квантора всеобщности также согласовано с ним: если в момент α дано обоснование для $\forall v\, A(v)$, то в любой момент в будущем для любого доступного в тот момент объекта a мы можем получить обоснование для $A(a)$.

Говорят, что формула A *истинна* в модели $\mathcal{K} = (K, \preceq, D, \Vdash)$, и пишут $\mathcal{K} \models A$, если для любого $\alpha \in K$ имеет место $\alpha \Vdash A$. Если формула A не истинна в модели Крипке $\mathcal{K}$, т. е. $\mathcal{K} \not\models A$, то $\mathcal{K}$ называют *контромоделью* для A.

Имеет место следующая *теорема о корректности* ИИП относительно моделей Крипке:

Теорема 53. *Если замкнутая формула языка Ω выводима в ИИП, то она истинна в любой модели Крипке для языка Ω.*

Доказательство. Мы докажем более общее утверждение: если формула выводима в ИИП, то ее универсальное замыкание истинно в любой модели Крипке. Очевидно, что достаточно доказать, что универсальное замыкание любой аксиомы истинно в любой модели Крипке, и проверить, что правила вывода сохраняют это свойство.

Пусть $\Phi(x_1, \ldots, x_n)$ — формула с параметрами $x_1, \ldots, x_n$, полученная по одной из схем аксиом 1 – 10. Требуется доказать, что для любой модели $\mathcal{K} = (K, \preceq, D, \Vdash)$ и любого $\alpha \in K$ имеет место $\alpha \Vdash \forall x_1 \ldots \forall x_n \, \Phi(x_1, \ldots, x_n)$. Для этого достаточно убедиться, что для любого $\alpha \in K$ и любых $a_1, \ldots, a_n \in D_\alpha$ имеет место $\alpha \Vdash \Phi(a_1, \ldots, a_n)$. Но $\Phi(a_1, \ldots, a_n)$ получена по той же схеме аксиом, что и $\Phi(x_1, \ldots, x_n)$, и $\alpha \Vdash \Phi(a_1, \ldots, a_n)$ следует из корректности ИИВ относительно моделей Крипке.

Рассмотрим формулу $\forall v \, \Phi(v, x_1, \ldots, x_n) \supset \Phi(t, x_1, \ldots, x_n)$, полученную по схеме аксиом 11, где $x_1, \ldots, x_n$ — список переменных, включающий все параметры рассматриваемой формулы. Если t — переменная, можно считать, что она входит в этот список. Требуется доказать, что для любых модели $\mathcal{K} = (K, \preceq, D, \Vdash)$ и $\alpha \in K$ имеет место

$$\alpha \Vdash \forall x_1 \ldots \forall x_n \, (\forall v \, \Phi(v, x_1, \ldots, x_n) \supset \Phi(t, x_1, \ldots, x_n)),$$

т. е. что для любого $\alpha \in K$ и любых $a_1, \ldots, a_n \in D_\alpha$ имеет место $\alpha \Vdash (\forall v \, \Phi(v, a_1, \ldots, a_n) \supset \Phi(a, a_1, \ldots, a_n))$, где a — значение терма t. Формулу $\Phi(v, a_1, \ldots, a_n)$ обозначим $A(v)$. Требуется доказать $\alpha \Vdash (\forall v \, A(v) \supset A(a))$, т. е. $(\forall \beta \succeq \alpha) \, [\beta \nVdash \forall v \, A(v) \vee \beta \Vdash A(a)]$. Пусть $\beta \succeq \alpha$ и $\beta \Vdash \forall v \, A(v)$. Последнее означает в частности, что $\beta \Vdash A(a)$, что и требовалось доказать.

Аналогично рассматривается формула

$$\Phi(t, x_1, \ldots, x_n) \supset \exists v \, \Phi(v, x_1, \ldots, x_n),$$

полученная по схеме аксиом 12.

Тот факт, что правило MP сохраняет доказываемое свойство формул, довольно очевиден. Рассмотрим другие правила.

Пусть формула $\exists v \, \Phi(v, x_1, \ldots, x_n) \supset \Psi(x_1, \ldots, x_n)$ получена по правилу (II) из формулы $\Phi(v, x_1, \ldots, x_n) \supset \Psi(x_1, \ldots, x_n)$, где $x_1, \ldots, x_n$ — все параметры рассматриваемых формул, отличные от v, и v не входит свободно в $\Psi(x_1, \ldots, x_n)$. Предположим, что для любой модели Крипке $\mathcal{K} = (K, \preceq, D, \Vdash)$ и любого $\alpha \in K$ имеет место

$$\alpha \Vdash \forall x_1 \ldots \forall x_n \forall v \, (\Phi(v, x_1, \ldots, x_n) \supset \Psi(x_1, \ldots, x_n)). \qquad (9.1)$$

Докажем, что для любого $\alpha \in K$ имеет место

$$\alpha \Vdash \forall x_1 \ldots \forall x_n \, (\exists v \, \Phi(v, x_1, \ldots, x_n) \supset \Psi(x_1, \ldots, x_n)).$$

Это означает, что для любого $\alpha \in K$ и любых $a_1, \ldots, a_n \in D_\alpha$ имеет место

$$\alpha \Vdash \exists v\, \Phi(v, a_1, \ldots, a_n) \supset \Psi(a_1, \ldots, a_n).$$

Пусть $\beta \succeq \alpha$ и $\beta \Vdash \exists v\, \Phi(v, a_1, \ldots, a_n)$, т. е. $\beta \Vdash \Phi(a, a_1, \ldots, a_n)$ для некоторого $a \in D_\beta$. Но из (9.1) следует, что

$$\beta \Vdash (\Phi(a, a_1, \ldots, a_n) \supset \Psi(a_1, \ldots, a_n)),$$

так что $\beta \Vdash \Psi(a_1, \ldots, a_n)$, что и требовалось доказать.

Аналогично рассматривается правило (III).

$\square$

Пример. Докажем, что формула $\neg\neg\forall x\, (P(x) \vee \neg P(x))$ не выводится в ИИП, построив контрмодель для этой формулы. Положим $K = \mathbf{N}$, причем $m \preceq n \rightleftharpoons m \leq n$ для любых $m, n \in \mathbf{N}$. Пусть $D_n = \{0, \ldots, n\}$. Положим $m \Vdash P(n) \rightleftharpoons m > n$. Допустим, что

$$0 \Vdash \neg\neg\forall x\, (P(x) \vee \neg P(x)). \tag{9.2}$$

В силу определения отношения $\Vdash$ для отрицания (9.2) означает, что $(\forall m \in \mathbf{N})\, m \nVdash \neg\forall x\, (P(x) \vee \neg P(x))$. В частности,

$$0 \nVdash \neg\forall x\, (P(x) \vee \neg P(x)).$$

Это означает, что $m \Vdash \forall x\, (P(x) \vee \neg P(x))$ для некоторого $m \in \mathbf{N}$. Отсюда и из определения соответствия $\Vdash$ для квантора всеобщности следует $m \Vdash P(m) \vee \neg P(m)$, так как $m \in D_m$. В силу определения отношения $\Vdash$ для дизъюнкции это означает, что либо 1) $m \Vdash P(m)$, либо 2) $m \Vdash \neg P(m)$. Однако ни то, ни другое не имеет места. Действительно, условие 1) не выполняется в силу определения отношения $\Vdash$ для атомов. Докажем, что условие 2) также не выполняется. Допустим противное, т. е. $m \Vdash \neg P(m)$. В силу определения отношения $\Vdash$ для отрицания это означает, что $(\forall n \geq m)\, n \nVdash P(m)$. Но это не так, ибо $m + 1 \Vdash P(m)$. Таким образом, предположение (9.2) приводит к противоречию. Значит,

$$0 \nVdash \neg\neg\forall x\, (P(x) \vee \neg P(x)),$$

и построенная модель Крипке является контрмоделью для рассматриваемой формулы.

§9.2. Полнота ИИП относительно моделей Крипке

Пусть дан элементарный язык L_M, не содержащий функциональных символов и содержащий счетное множество констант M. Множество высказываний Γ языка L_M называется *M-насыщенным*, если

1) Γ непротиворечиво: не существует такой формулы Φ, что $\Gamma \vdash \Phi$ и $\Gamma \vdash \neg\Phi$, где $\vdash$ означает выводимость в ИИП;

2) Γ замкнуто относительно выводимости в ИИП: каково бы ни было высказывание Φ языка L_M, если $\Gamma \vdash \Phi$, то $\Phi \in \Gamma$;

3) Γ обладает *свойством дизъюнктивности*: каковы бы ни были высказывания Φ и Ψ, если $(\Phi \vee \Psi) \in \Gamma$, то $\Phi \in \Gamma$ или $\Psi \in \Gamma$;

4) Γ обладает *свойством экзистенциальности*: каково бы ни было высказывание вида $\exists v \Phi(v)$, если оно принадлежит множеству Γ, то $\Phi(c) \in \Gamma$ для некоторой константы $c \in M$.

Предложение 26. *Пусть M — не более чем счетное множество констант, M' — его расширение за счет добавления счетного множества дополнительных констант $\{c_1, c_2, \ldots\}$. Каковы бы ни были множество высказываний Γ и высказывание Φ языка L_M, если $\Gamma \nvdash \Phi$, то существует M'-насыщенное множество высказываний Γ' языка $L_{M'}$ такое, что $\Gamma \subseteq \Gamma'$ и $\Phi \notin \Gamma'$.*

Доказательство. Так как сигнатура языка $L_{M'}$ счетна, множество всех формул этого языка счетно. Будем считать, что нам даны последовательность всех экзистенциальных высказываний языка $L_{M'}$

$$\exists v_0 \Psi_0(v_0),\ \exists v_1 \Psi_1(v_1),\ \exists v_2 \Psi_2(v_2), \ldots \tag{9.3}$$

и последовательность всех дизъюнктивных высказываний языка $L_{M'}$

$$\Psi_0 \vee \Psi_0',\ \Psi_1 \vee \Psi_1',\ \Psi_2 \vee \Psi_2', \ldots . \tag{9.4}$$

Индукцией по n определим множество высказываний Γ_n. При построении каждого из множеств Γ_n будет рассматриваться одна из формул последовательности (9.3) или последовательности (9.4). Поэтому на каждом шаге будет существовать бесконечно много еще не рассмотренных формул в каждой из этих последовательностей. Кроме того в формулах каждого из множеств Γ_n будет использоваться лишь конечное число дополнительных констант $c_1, c_2, \ldots$.

Положим $\Gamma_0 = \Gamma$. Допустим, что для некоторого n множество Γ_n определено, и определим множество Γ_{n+1}.

Случай 1. n четно. В последовательности (9.3) найдем первое еще не рассмотренное высказывание $\exists v \Psi(v)$ такое, что $\Gamma_n \vdash \exists v \Psi(v)$. Пусть c — первая константа из последовательности $c_1, c_2, \ldots$, которая не встречается в формулах из Γ_n и в рассматриваемой формуле $\exists v \Psi(v)$. Положим $\Gamma_{n+1} = \Gamma_n \cup \{\Psi(c)\}$.

Случай 2. n нечетно. В последовательности (9.4) найдем первое еще не рассмотренное высказывание $\Psi \vee \Psi'$ такое, что $\Gamma_n \vdash \Psi \vee \Psi'$. Если $\Gamma_n \cup \{\Psi\} \nvdash \Phi$, положим $\Gamma_{n+1} = \Gamma_n \cup \{\Psi\}$. В противном случае положим $\Gamma_{n+1} = \Gamma_n \cup \{\Psi'\}$.

Положим $\Gamma' = \bigcup\limits_{n=0}^{\infty} \Gamma_n$ и докажем, что Γ' — искомое множество. Во-первых, докажем, что $\Gamma' \nvdash \Phi$. Заметим, что для этого достаточно убедиться, что $\Gamma_n \nvdash \Phi$ для любого n. Докажем это индукцией по n. При $n = 0$ утверждение следует из определения множества Γ_0 и условия предложения. Допустим, что для некоторого n имеет место $\Gamma_n \nvdash \Phi$, и докажем, что $\Gamma_{n+1} \nvdash \Phi$. Допустим, что $\Gamma_{n+1} \vdash \Phi$, и рассмотрим два случая в зависимости от того, n четно или нечетно. Пусть n четно. Тогда $\Gamma_{n+1} = \Gamma_n \cup \{\Psi(c)\}$, причем $\Gamma_n \vdash \exists v \Psi(v)$, а константа c не встречается в $\Psi(v)$ и формулах из Γ_n. Таким образом, по предположению $\Gamma_n \cup \{\Psi(c)\} \vdash \Phi$. По теореме о дедукции существует вывод из Γ_n формулы $\Psi(c) \supset \Phi$. Заменим всюду в этом выводе каждое вхождение константы c на переменную u, которая не встречается ни в одной из формул этого вывода. В силу предложения 25 мы получим вывод из Γ_n формулы $\Psi(u) \supset \Phi$. Отсюда следует $\Gamma_n \vdash \exists v \Psi(v) \supset \Phi$, а так как $\Gamma_n \vdash \exists v \Psi(v)$, то $\Gamma_n \vdash \Phi$, что противоречит индуктивному предположению. Если n нечетно, и $\Gamma_{n+1} = \Gamma_n \cup \{\Psi\}$, причем $\Gamma_n \cup \{\Psi\} \nvdash \Phi$, то доказываемое утверждение очевидно. Рассмотрим случай, когда $\Gamma_{n+1} = \Gamma_n \cup \{\Psi'\}$, причем $\Gamma_n \vdash \Psi \vee \Psi'$ и

$$\Gamma_n \cup \{\Psi\} \vdash \Phi. \tag{9.5}$$

Предположив, что $\Gamma_n \cup \{\Psi'\} \vdash \Phi$, и учитывая (9.5), по правилу ($\vee \to$) получаем $\Gamma_n \cup \{\Psi \vee \Psi'\} \vdash \Phi$ и далее $\Gamma_n \vdash \Phi$, что противоречит индуктивному предположению.

Из доказанного следует, что множество Γ' непротиворечиво. Таким образом, выполнено условие 1) из определения M-насыщенного множества. Докажем, что выполнено условие 2). Допустим $\Gamma' \vdash \Psi$ и докажем, что $\Psi \in \Gamma'$. Очевидно, что $\Gamma_m \vdash \Psi$ для некоторого m. Тогда $\Gamma_i \vdash \Psi \vee \Psi$ для всех $i \geq m$. Следовательно, на некотором нечетном шаге построения последовательности Γ_n формула Ψ попадет в Γ'. Выполнимость условия 3) очевидна: если $\Psi \vee \Psi' \in \Gamma'$, то $\Gamma' \vdash \Psi \vee \Psi'$, и на некотором нечетном шаге построения последовательности Γ_n одна из формул Ψ и Ψ' попадет в Γ'. Докажем выполнимость условия 4). Пусть формула $\exists v\, \Psi(v)$ принадлежит множеству Γ'. Тогда $\Gamma_m \vdash \exists v\, \Psi(v)$ для некоторого m и $\Gamma_i \vdash \exists v\, \Psi(v)$ для всех $i \geq m$. Следовательно, на некотором четном шаге построения последовательности Γ_n формула $\Psi(c)$ попадет в Γ'. Таким образом, множество Γ' является M-насыщенным, причем $\Phi \notin \Gamma'$. □

Теорема 54. *Если множество высказываний Γ языка L_M является M-насыщенным, то существует модель Крипке $\mathcal{K}$ такая, что для любого высказывания Φ языка L_M выполнено условие $\mathcal{K} \models \Phi \Leftrightarrow \Phi \in \Gamma$.*

Доказательство. Последовательность множеств констант M_n определим индуктивно: $M_0 = M$, а M_{i+1} получается добавлением к M_i счетного множества новых констант. Построим модель Крипке $\mathcal{K}$. Пусть K — семейство всех множеств Δ таких, что

1) Δ состоит из замкнутых формул некоторого языка L_{M_i};
2) Δ является M_i-насыщенным;
3) $\Gamma \subseteq \Delta$.

Для $\Delta, \Delta' \in K$ положим $\Delta \preceq \Delta' \rightleftharpoons \Delta \subseteq \Delta'$. Пусть $\Delta \in K$ является M_i-насыщенным. Тогда полагаем $D_\Delta = M_i$, и если $P(c_1, \ldots, c_n)$ — атомная формула с константами $c_1, \ldots, c_n \in M_i$, положим

$$\Delta \Vdash P(c_1, \ldots, c_n) \rightleftharpoons P(c_1, \ldots, c_n) \in \Delta.$$

Таким образом, построена модель Крипке $\mathcal{K} = (K, \preceq, D, \Vdash)$. Докажем, что для любого $\Delta \in K$ выполнено условие: если Δ является M_i-насыщенным, то для любого высказывания Ψ языка L_{M_i}

$$\Delta \Vdash \Phi \Leftrightarrow \Phi \in \Delta. \tag{9.6}$$

Индукция по логической длине Φ. Для атома Φ (9.6) выполнено по определению $\Vdash$. Пусть (9.6) выполнено, когда Φ есть Ψ или Ψ'. Докажем, что это условие выполнено, когда Φ есть $\Psi \,\&\, \Psi'$. Имеем:

$$\Delta \Vdash \Psi \,\&\, \Psi' \Leftrightarrow [\Delta \Vdash \Psi \text{ и } \Delta \Vdash \Psi'] \Leftrightarrow [\Psi \in \Delta \text{ и } \Psi' \in \Delta] \Leftrightarrow$$

$$\Leftrightarrow [\Delta \vdash \Psi \text{ и } \Delta \vdash \Psi'] \Leftrightarrow [\Delta \vdash \Psi \,\&\, \Psi'] \Leftrightarrow \Psi \,\&\, \Psi' \in \Delta.$$

Докажем, что (9.6) выполнено, когда Φ есть $\Psi \vee \Psi'$:

$$\Delta \Vdash \Psi \vee \Psi' \Leftrightarrow [\Delta \Vdash \Psi \text{ или } \Delta \Vdash \Psi'] \Leftrightarrow$$

$$\Leftrightarrow [\Psi \in \Delta \text{ или } \Psi' \in \Delta] \Leftrightarrow \Psi \vee \Psi' \in \Delta.$$

Последняя равносильность основана на замкнутости Δ относительно выводимости и свойстве дизъюнктивности для Δ.

Докажем, что (9.6) выполнено, когда Φ есть $\Psi \supset \Psi'$:

$$\Delta \Vdash \Psi \supset \Psi' \Leftrightarrow (\forall \Delta' \supseteq \Delta)[\Delta' \Vdash \Psi \Rightarrow \Delta' \Vdash \Psi'] \Leftrightarrow$$

$$\Leftrightarrow (\forall \Delta' \supseteq \Delta)[\Psi \in \Delta' \Rightarrow \Psi' \in \Delta'] \Leftrightarrow \Psi \supset \Psi' \in \Delta.$$

В последней равносильности импликация справа налево основана на замкнутости Δ относительно выводимости. Докажем импликацию слева направо. Пусть

$$(\forall \Delta' \supseteq \Delta)\,]\Psi \in \Delta' \Rightarrow \Psi' \in \Delta'], \tag{9.7}$$

но условие $\Psi \supset \Psi' \in \Delta$ не выполнено. Тогда $\Delta \cup \{\Psi\} \nvdash \Psi'$. В силу предложения 26 существует M_{i+1}-насыщенное множество Δ' такое, что $\Delta \subseteq \Delta'$, $\Psi \in \Delta'$, но $\Psi' \notin \Delta'$. Значит, условие (9.7) также не выполнено.

Случай, когда формула Φ есть $\neg\Psi$ рассматривается аналогично.

Пусть дана формула $\Psi(v)$ с единственной свободной переменной v. Тогда для любой константы c формула $\Psi(c)$ замкнута. Допустим, что (9.6) выполнено, когда Φ есть $\Psi(c)$. Докажем, что это условие выполнено, когда Φ есть $\exists v\, \Psi(v)$:

$$\Delta \Vdash \exists v\, \Psi(v) \Leftrightarrow (\exists c \in D_\Delta)\,[\Delta \Vdash \Psi(c)] \Leftrightarrow$$

$$\Leftrightarrow (\exists c \in D_\Delta)\,[\Psi(c) \in \Delta] \Leftrightarrow \exists v\, \Psi(v) \in \Delta.$$

Последняя равносильность основана на замкнутости Δ относительно выводимости и свойстве экзистенциальности для Δ.

Докажем, что (9.6) выполнено, когда Φ есть $\forall v\, \Psi(v)$:

$$\Delta \Vdash \forall v\, \Psi(v) \Leftrightarrow (\forall \Delta' \supseteq \Delta)\,(\forall c \in D_{\Delta'})\,[\Delta \Vdash \Psi(c)] \Leftrightarrow$$
$$\Leftrightarrow (\forall \Delta' \supseteq \Delta)\,(\forall c \in D_{\Delta'})\,[\Psi(c) \in \Delta] \Leftrightarrow \forall v\, \Psi(v) \in \Delta.$$

В последней равносильности импликация справа налево основана на замкнутости Δ относительно выводимости. Докажем импликацию слева направо. Пусть

$$(\forall \Delta' \supseteq \Delta)\,(\forall c \in D_{\Delta'})\,[\Psi(c) \in \Delta], \tag{9.8}$$

но при этом условие $\forall v\, \Psi(v) \in \Delta$ не выполнено. Тогда

$$\Delta \nvdash \forall v\, \Psi(v). \tag{9.9}$$

В этом случае $\Delta \nvdash \Psi(c)$ для любой константы $c \in M_{i+1} \setminus M_i$. Действительно, если существует вывод $\Psi(c)$ из Δ, то, заменив в нем все вхождения c на переменную u, не встречающуюся в этом выводе, в силу предложения 25 получим вывод из Δ формулы $\Psi(u)$ и затем получим $\Delta \vdash \forall u\, \Psi(u)$, откуда нетрудно получить $\Delta \vdash \forall v\, \Psi(v)$, что противоречит условию (9.9). Таким образом, если $c \in M_{i+1} \setminus M_i$, то $\Delta \nvdash \Psi(c)$. В силу предложения 26 существует M_{i+2}-насыщенное множество Δ' такое, что $\Delta \subseteq \Delta'$ и $\Psi(c) \notin \Delta'$. Значит, условие (9.8) не выполнено вопреки предположению.

Таким образом, (9.6) выполняется для любого M_i-насыщенного множества $\Delta \in K$ и любого высказывания Ψ языка L_{M_i}. В частности, имеем $\Gamma \Vdash \Phi \Leftrightarrow \Phi \in \Gamma$, каково бы ни было высказывание Φ языка L_M. Для завершения доказательства теоремы остается заметить, что Γ — наименьший элемент шкалы модели $\mathcal{K}$, так что $\Gamma \Vdash \Phi \Leftrightarrow \mathcal{K} \models \Phi$. $\square$

Теорема 55. *Для любого непротиворечивого множество высказываний существует модель Крипке.*

Доказательство. Пусть Γ — непротиворечивое множество высказываний сигнатуры Ω. Тогда найдется высказывание Φ, невыводимое из Γ. В силу теоремы 26 существует M-насыщенное множество высказываний Γ' сигнатуры Ω', полученной добавлением к Ω счетного множества дополнительных констант, такое, что $\Gamma \subseteq \Gamma'$. По теореме 54 существует модель Крипке $\mathcal{K}$ для множества Γ'. Так как $\Gamma \subseteq \Gamma'$, то $\mathcal{K}$ — модель Крипке для множества Γ. $\square$

Пусть Γ — некоторое множество высказываний элементарного языка, Φ — некоторое высказывание этого языка. Будем говорить, что Φ *логически следует* из Γ и писать $\Gamma \models \Phi$, если в любой модели Крипке для языка Ω, в которой истинны все высказывания из Γ, высказывание Φ также истинно. Имеет место следующая *обобщенная теорема о корректности* ИИП относительно моделей Крипке.

Теорема 56. *Каковы бы ни были множество высказываний* Γ *и высказывание* Φ *языка* Ω, *если* $\Gamma \vdash \Phi$, *то* $\Gamma \models \Phi$.

Доказательство. Пусть $\Gamma \vdash \Phi$. Тогда существует конечное множество $\Delta = \{\Phi_1, \ldots, \Phi_n\} \subseteq \Gamma$ такое, что $\Delta \vdash \Phi$. Применяя n раз теорему о дедукции, получаем $\vdash \Phi_1 \supset (\ldots \supset (\Phi_n \supset \Phi) \ldots)$. В силу теоремы о корректности ИИП (теорема 53) формула

$$\Phi_1 \supset (\ldots \supset (\Phi_n \supset \Phi) \ldots) \tag{9.10}$$

истинна в любой модели Крипке. Докажем, что $\Gamma \models \Phi$. Пусть $\mathcal{K}$ — модель Крипке для языка Ω, в которой истинны все высказывания из Γ. Тогда все формулы $\Phi_1, \ldots, \Phi_n$ истинны в модели $\mathcal{K}$. Так как кроме того формула (9.10) истинна в модели $\mathcal{K}$, то формула Φ также истинна в модели $\mathcal{K}$. $\square$

Обобщенная теорема о полноте интуиционистского исчисления предикатов относительно моделей Крипке формулируется так:

Теорема 57. *Каковы бы ни были множество высказываний* Γ *и высказывание* Φ *языка* Ω, *если* $\Gamma \models \Phi$, *то* $\Gamma \vdash \Phi$.

Доказательство. Докажем, что если $\Gamma \nvdash \Phi$, то $\Gamma \not\models \Phi$. Последнее означает, что существует такая модель Крипке $\mathcal{K}$ для языка Ω, что $\mathcal{K} \models \Gamma$ (т. е. в $\mathcal{K}$ истинны все высказывания из Γ), но $\mathcal{K} \not\models \Phi$. Итак, пусть $\Gamma \nvdash \Phi$, и пусть M' получено добавлением к множеству констант M языка Ω счетного множества новых констант. В силу предложения 26 существует M'-насыщенное расширение Γ' множества Γ такое, что $\Phi \notin \Gamma'$. По теореме 54 существует модель Крипке $\mathcal{K}$ такая, что $\mathcal{K} \models \Psi \Leftrightarrow \Psi \in \Gamma$, каково бы ни было высказывание Ψ языка $L_{M'}$. Так как $\Gamma \subseteq \Gamma'$, то отсюда следует, что $\mathcal{K} \models \Gamma$, а так как $\Phi \notin \Gamma'$, то $\mathcal{K} \not\models \Phi$. Значит, $\mathcal{K}$ — искомая модель. $\square$

Теоремы 56 и 57 вместе дают следующее утверждение:

Теорема 58. *Каковы бы ни были множество высказываний* Γ *и высказывание* Φ *языка* Ω, *имеет место* $\Gamma \models \Phi$ *тогда и только тогда, когда* $\Gamma \vdash \Phi$.

Если множество высказываний Γ языка Ω пусто, то $\Gamma \models \Phi$ означает, что высказывание Φ истинно в любой модели Крипке для языка Ω, а $\Gamma \vdash \Phi$ означает выводимость высказывания Φ. Если в теореме 58 положить Γ пустым, получается следующая *теорема о полноте* ИИП относительно моделей Крипке:

Теорема 59. *Если высказывание* Φ *языка* Ω *истинно в любой модели Крипке для языка* Ω, *то* Φ *выводимо в ИИП.*

Теорема о полноте ИИП относительно моделей Крипке вместе с теоремой о корректности ИИП относительно моделей Крипке (теорема 53) дают следующее утверждение:

Теорема 60. *Высказывание* Φ *языка* Ω *выводимо в ИИП тогда и только тогда, когда* Φ *истинно в любой модели Крипке для языка* Ω.

§9.3. Интуиционистские теории

В классической математической логике *элементарной теорией* называется произвольное множество T высказываний данного элементарного языка L. Интуитивно T понимается как множество аксиом, а теоремами теории T считаются логические следствия из T. В силу теоремы Гёделя о полноте классического исчисления предикатов (теорема 26) теоремы теории T — это в точности все высказывания, выводимые из T в классическом исчислении предикатов.

Следуя этой идее, мы можем определить интуиционистскую теорию как произвольное множество T высказываний данного интуиционистского элементарного языка, а ее теоремами считать такие высказывания Φ, что имеет место $T \models \Phi$ в смысле логического следования, определяемого через модели Крипке. В силу теоремы 57 теоремами интуиционистской теории T являются в точности все высказыания, выводимые из T в ИИП.

Интуиционистская теория называется *противоречивой*, если существует такое высказывание Φ, что оно и его отрицание

$\neg\Phi$ оба являются теоремами этой теории; в противном случае теория называется *непротиворечивой*. Нетрудно убедиться, что теория противоречива тогда и только тогда, когда всякое высказывание является ее теоремой. Из доказательства теоремы о полноте интуиционистского исчисления предикатов следует, что для всякой непротиворечивой теории T существует модель Крипке $\mathcal{K}$ такая, что $\mathcal{K} \models T$. Такая модель Крипке $\mathcal{K}$ называется моделью теории T.

Говорят, что теория T обладает *свойством дизъюнктивности*, если из того, что высказывание вида $\Phi \vee \Psi$ является теоремой теории T, следует, что хотя бы одно из высказываний Φ и Ψ является теоремой этой теории. Теория T обладает *свойством экзистенциальности*, если из того, что высказывание вида $\exists v\, \Phi(v)$ является теоремой теории T, следует, что существует константа c такая, что высказывание $\Phi(c)$ является теоремой этой теории. Очевидно, что имеет смысл говорить об экзистенциальности теории T только в том случае, когда язык этой теории содержит хотя бы одну константу.

Пусть $\mathcal{K}_1 = (K_1, \preceq_1, D^1, \Vdash_1)$ и $\mathcal{K}_2 = (K_2, \preceq_2, D^2, \Vdash_2)$ — модели Крипке, причем $K_1 \cap K_2 = \emptyset$. Их *суммой* называется модель $\mathcal{K} = (K, \preceq, D, \Vdash)$, где

- $K = K_1 \cup K_2$;
- $\alpha \preceq \beta$ тогда и только тогда, когда для некоторого $i \in \{1, 2\}$ имеет место $\alpha \in K_i$, $\beta \in K_i$, и при этом $\alpha \preceq_i \beta$;
- если $\alpha \in K_i$, где $i \in \{1, 2\}$, то $D_\alpha = D^i_\alpha$;
- если $\alpha \in K_i$, где $i \in \{1, 2\}$, то для произвольного атома A имеет место $\alpha \Vdash A$ тогда и только тогда, когда $\alpha \Vdash_i A$.

Сумма моделей $\mathcal{K}_1$ и $\mathcal{K}_2$ обозначается $\mathcal{K}_1 + \mathcal{K}_2$. Очевидно, что для любого высказывания Φ

$$(\mathcal{K}_1 + \mathcal{K}_2) \models \Phi \Leftrightarrow [\mathcal{K}_1 \models \Phi \text{ и } \mathcal{K}_2 \models \Phi].$$

Отсюда следует, что сумма двух моделей теории T также является моделью этой теории.

Сумма $\sum\limits_{i \in I} \mathcal{K}_i$ любого семейства моделей Крипке $\{\mathcal{K}_i \mid i \in I\}$ определяется аналогично. И в этом случае, если все $\mathcal{K}_i$ $(i \in I)$

являются моделями теории T, то $\sum\limits_{i \in I} \mathcal{K}_i$ также является моделью этой теории.

Для произвольной модели Крипке $\mathcal{K} = (K, \preceq, D, \Vdash)$ для языка L_M, где $M \neq \emptyset$, определяется модель $\mathcal{K}' = (K', \preceq', D', \Vdash')$ следующим образом:

- $K' = K \cup \{\alpha_0\}$, где $\alpha_0 \notin K$;
- $\alpha_0 \preceq' \alpha$ для любого $\alpha \in K'$; если $\alpha, \beta \in K$, то $\alpha \preceq' \beta$ тогда и только тогда, когда $\alpha \preceq \beta$;
- $D'_\alpha = D_\alpha$, если $\alpha \in K$, а D'_{α_0} состоит из значений всех констант в модели $\mathcal{K}$, иными словами, $D'_{\alpha_0} = \{\bar{c} \mid c \in M\}$;
- если $\alpha \in K$, то для произвольного атома A имеет место $\alpha \Vdash' A$ тогда и только тогда, когда $\alpha \Vdash A$; $\alpha_0 \Vdash' A$ тогда и только тогда, когда $\mathcal{K} \models A$.

Теорема 61. *Если класс моделей теории T замкнут относительно операции $'$, то теория T обладает свойствами дизъюнктивности и экзистенциальности.*

Доказательство. Пусть класс моделей теории T замкнут относительно операции $'$. Как отмечалось выше, он замкнут и относительно операции суммирования. Докажем, что теория T обладает свойством дизъюнктивности. Пусть $T \vdash A \vee B$. Докажем, что имеет место $T \vdash A$ или $T \vdash B$. Допустим противное: $T \nvdash A$ и $T \nvdash B$. Как следует из доказательства теоремы о полноте ИИП относительно моделей Крипке (теорема 57), существуют такие модели $\mathcal{K}_1$ и $\mathcal{K}_2$ теории T, что $\mathcal{K}_1 \not\models A$, $\mathcal{K}_2 \not\models B$. Это означает, что в шкалах моделей $\mathcal{K}_1$ и $\mathcal{K}_2$ существуют элементы α_1 и α_2 соответственно такие, что $\alpha_1 \nVdash A$, $\alpha_2 \nVdash B$. Рассмотрим модель Крипке $\mathcal{K} = (\mathcal{K}_1 + \mathcal{K}_2)'$, которая очевидно является моделью теории T. Пусть α_0 — наименьший элемент шкалы модели $\mathcal{K}$. Тогда $\alpha_0 \nVdash A \vee B$, так как $\alpha_0 \nVdash A$, ибо $\alpha_0 \preceq \alpha_1$ и $\alpha_1 \nVdash A$, а также $\alpha_0 \nVdash B$, ибо $\alpha_0 \preceq \alpha_2$ и $\alpha_2 \nVdash B$. Это противоречит тому, что $\mathcal{K}$ — модель, а $A \vee B$ — теорема теории T.

Докажем, что теория T обладает также свойством экзистенциальности. Пусть $T \vdash \exists v\, A(v)$. Докажем, что имеет место $T \vdash A(c)$ для некоторой константы $c \in M$, где M — множество всех констант языка теории T. Допустим противное: $T \nvdash A(c)$ для любой константы $c \in M$. Тогда для любой константы $c \in M$ существует такая модель Крипке $\mathcal{K}_c$ теории T, что $\mathcal{K}_c \not\models A(c)$. Это означает, что в шкале модели $\mathcal{K}_c$ существует элемент α_c такой, что $\alpha_c \nVdash A(c)$. Рассмотрим модель Крипке $\mathcal{K} = (\sum\limits_{c \in M} \mathcal{K}_c)'$, которая очевидно является моделью теории T. Пусть α_0 — наименьший элемент шкалы модели $\mathcal{K}$. Тогда $\alpha_0 \nVdash \exists v\, A(v)$, так как $D_{\alpha_0} = M$, но $\alpha_0 \nVdash A(c)$ для любой константы $c \in M$, ибо $\alpha_0 \preceq \alpha_c$ и $\alpha_c \nVdash A(c)$. Это противоречит тому, что $\mathcal{K}$ — модель, а $\exists v\, A(v)$ — теорема теории T. $\square$

§9.4. Теории и модели с равенством

При формализации математических теорий обычно используется предикат равенства $=$. Однако, если в элементарном языке имеется предикатный символ $=$, то в моделях Крипке мы вовсе не обязаны интерпретировать его именно как равенство. Модель Крипке $\mathcal{K} = (K, \preceq, D, \Vdash)$ для языка сигнатуры $\Omega \cup \{=\}$ будем называть *нормальной*, если для любого $\alpha \in K$ и любых $a, b \in D_\alpha$ имеет место $\alpha \Vdash a = b$ тогда и только тогда, когда действительно $a = b$.

Через $Eq(\Omega)$ обозначим следующее множество высказываний сигнатуры $\Omega \cup \{=\}$:

Eq1. $\forall x\,(x = x)$;

Eq2. $\forall x\,\forall y\,(x = y \supset y = x)$;

Eq3. $\forall x\,\forall y\,\forall z\,(x = y \,\&\, y = z \supset x = z)$;

Eq4. $\forall x\,\forall y\,(x = y \vee \neg x = y)$;

Eq(P). $\forall x_1 \ldots \forall x_n\,\forall y_1 \ldots \forall y_n\,(x_1 = y_1 \,\&\, \ldots \,\&\, x_n = y_n \supset$
$$\supset (P(x_1, \ldots, x_n) \supset P(y_1, \ldots, x_y)))$$

для каждого (n-местного) предикатного символа P сигнатуры Ω.

Теорема 62. *Каково бы ни было множество высказываний* Γ *сигнатуры* $\Omega \cup \{=\}$, *оно имеет нормальную модель Крипке тогда и только тогда, когда существует модель Крипке для множества* $\Gamma \cup Eq(\Omega)$.

Доказательство. Допустим, что множество высказываний Γ в сигнатуре $\Omega \cup \{=\}$ имеет нормальную модель Крипке $\mathcal{K}$. Очевидно, что все высказывания из $Eq(\Omega)$ истинны в любой нормальной модели Крипке, в частности, в модели $\mathcal{K}$. Следовательно, $\mathcal{K}$ является моделью множества $\Gamma \cup Eq(\Omega)$.

Обратно, допустим, что существует модель Крипке для $\Gamma \cup Eq(\Omega)$. Следовательно, множество $\Gamma \cup Eq(\Omega)$ непротиворечиво, и в силу предложения 26 его можно расширить до насыщенного множества высказываний Γ_0 в сигнатуре со счетным множеством констант $M_0 = \{c_0^0, c_1^0, c_2^0, \dots\}$. Применим к Γ_0 конструкцию из доказательства теоремы 54 для построения модели Крипке $\mathcal{K}$, в которой истинны в точности все высказывания из Γ_0. Элементами K являются M_i-насыщенные $(i = 0, 1, 2, \dots)$ множества высказываний, где $M_i = M_{i-1} \cup \{c_0^i, c_1^i, c_2^i, \dots\}$. Если $\Delta \in K$ есть M_i-насыщенное множество, будем говорить, что Δ принадлежит уровню i.

Построим нормальную модель Крипке $\mathcal{K}^{\mathrm{n}}$ для Γ следующим образом. Индукцией по i преобразуем все насыщенные множества i-го уровня, входящие в K. При $i = 0$ единственным таким множеством является Γ_0. Определим на множестве M_0 бинарное отношение $\approx$ так: если $a, b \in M_0$, то $a \approx b$ тогда и только тогда, когда $a = b \in \Gamma_0$. Так как в $\mathcal{K}$ истинны высказывания Eq1 – Eq3, то $\approx$ — отношение эквивалентности на M_0. Более того, так как для каждого предикатного символа P в $\mathcal{K}$ истинно высказывание Eq(P), то из $a_1 \approx b_1, \dots, a_n \approx b_n$ следует, что для любого $\Delta \in K$

$$P(a_1, \dots, a_n) \in \Delta \Leftrightarrow P(b_1, \dots, b_n) \in \Delta.$$

Заметим также, что в силу истинности в $\mathcal{K}$ высказывания Eq4, если $a \not\approx b$, то $\neg\, a = b \in \Delta$, каково бы ни было $\Delta \in K$.

Множество M_0 разбивается на классы эквивалентности по отношению $\approx$. Выберем в каждом из них по одному представителю и заменим во всех формулах, входящих хотя бы в одно из множеств $\Delta \in K$ каждую константу из M_0 на выбранный представитель из того класса, в который эта константа входит, и оставим в каждом из M_i только эти выбранные представители. После такого преобразования окажется, что на нулевом уровне истинны только такие высказывания вида $a = b$, где действительно a и b совпадают. При этом каждое из множеств Δ только уменьшится, но порядок по включению между ними сохранится.

Подробно рассмотрим случай $i = 1$. Зафиксируем какое-нибудь насыщенное множество уровня 1 из K. Обозначим его Γ_1. Определим на уже преобразованном множестве M_1 бинарное отношение $\approx$, положив, что для $a, b \in M_1$ имеет место $a \approx b$ тогда и только тогда, когда $a = b \in \Gamma_1$. Так как в $\mathcal{K}$ истинны высказывания Eq1 – Eq3, то $\approx$ — отношение эквивалентности на M_1. Более того, так как для каждого предикатного символа P в $\mathcal{K}$ истинно высказывание Eq(P), то из $a_1 \approx b_1, \ldots, a_n \approx b_n$ следует, что если $\Gamma_1 \subseteq \Delta$, то

$$P(a_1, \ldots, a_n) \in \Delta \Leftrightarrow P(b_1, \ldots, b_n) \in \Delta.$$

Заметим также, что в силу истинности в $\mathcal{K}$ высказывания Eq4 в этом случае из $a \not\approx b$ следует, что $\neg\, a = b \in \Delta$. Множество M_1 разбивается на классы эквивалентности по отношению $\approx$. Выберем в каждом из них по одному представителю, причем этим представителем пусть будет элемент из M_0, если таковой там есть; в противном случае пусть представителем будет константа c^i_j с наименьшим нижним индексом j. Заменим во всех формулах, входящих хотя бы в одно из множеств $\Delta \supseteq \Gamma_1$ каждую константу из M_1 на выбранный представитель из того класса, в который эта константа входит, и оставим в его предметной области M_i только эти выбранные представители.

Проделаем эту процедуру со всеми множествами Γ_1 первого уровня. Докажем, что если $\Delta \in K$ является расширением множеств Γ_1 и Γ'_1 первого уровня, то в результате преобразований, связанных с этими множествами, из Δ получается одно и то же множество. Для этого достаточно убедиться, что невозможен случай, когда для некоторых $a, b \in M_1$ имеет место одновременно $a = b \in \Gamma_1$ и $\neg\, a = b \in \Gamma'_1$. Но это действительно так, ибо в противном случае получилось бы, что одновременно $a = b \in \Delta$ и $\neg\, a = b \in \Delta$. Значит, описанное преобразование корректно.

После такого преобразования окажется, что на первом уровне истинны только такие высказывания вида $a = b$, где действительно a и b совпадают. При этом множества высших уровней из K только уменьшатся, но порядок по включению между ними сохранится.

Проделав эту процедуру для всех $i = 0, 1, 2, \dots$, мы получим нормальную модель для $\Gamma \cup Eq(\Omega)$, а следовательно и для Γ, что и требовалось доказать. $\square$

Исчисление, полученное добавлением к ИИП$_\Omega$ множества аксиом $Eq(\Omega)$, называется *ИИП$_\Omega$ с разрешимым равенством.*

Теорема 63. *Если множество замкнутых формул* Γ *сигнатуры* $\Omega \cup \{=\}$ *непротиворечиво в ИИП$_\Omega$ с разрешимым равенством, то* Γ *имеет нормальную модель Крипке.*

Доказательство. Так как в ИИП$_\Omega$ с разрешимым равенством из множества высказываний Γ не выводится противоречие, то множество высказываний $\Gamma \cup Eq(\Omega)$ непротиворечиво в обычном смысле. В силу теоремы 55 для множества $\Gamma \cup Eq(\Omega)$ существует модель Крипке, а тогда по теореме 62 множество Γ имеет нормальную модель. $\square$

§9.5. Свойства дизъюнктивности и экзистенциальности ИИП

Пусть фиксирована сигнатура Ω, содержащая лишь константы и предикатные символы. В силу теоремы о корректности ИИП относительно моделей Крипке (теорема 53) любая модель Крипке является моделью пустой теории T, т. е. теории, не содержащей ни одной аксиомы. Теоремами этой теории являются в точности все высказывания, выводимые в ИИП. Очевидно, что класс моделей теории T замкнут относительно операции $'$. Поэтому из теоремы 61 следует, что ИИП обладает свойством дизъюнктивности: если в этом исчислении выводимо высказывание языка Ω вида $A \vee B$, то выводима хотя одна из формул A и B. Если же язык Ω содержит хотя бы одну константу, то из теоремы 61 следует, что ИИП обладает также и свойством экзистенциальности: если высказывание вида $\exists v\, A(v)$ выводимо в ИИП, то для некоторой константы c высказывание $A(c)$ выводимо в ИИП. Приведем другое доказательство этих свойств для ИИП, использующее понятие реализуемости, которое применялось в § 6.6 при доказательстве свойства дизъюнктивности для ИИВ (теорема 42).

Теорема 64. *Если сигнатура Ω содержит хотя бы одну константу, то ИИП$_\Omega$ обладает свойствами дизъюнктивности и экзистенциальности.*

Доказательство. Определим понятие «высказывание A языка Ω реализуемо», обозначаемое $\mathbf{r}\,A$, индукцией по логической длине A (здесь $\vdash$ означает выводимость в ИИП):

- никакое атомное высказывание не реализуемо;
- $\mathbf{r}\,(A \,\&\, B) \rightleftharpoons [\mathbf{r}\,A \,\&\, \mathbf{r}\,B]$;
- $\mathbf{r}\,(A \vee B) \rightleftharpoons [(\mathbf{r}\,A \,\&\, \vdash A) \vee (\mathbf{r}\,B \,\&\, \vdash B)]$;
- $\mathbf{r}\,(A \supset B) \rightleftharpoons [(\mathbf{r}\,A \,\&\, \vdash A) \Rightarrow \mathbf{r}\,B]$;
- $\mathbf{r}\,\neg A \rightleftharpoons$ [неверно, что $(\mathbf{r}\,A \,\&\, \vdash A)$];
- $\mathbf{r}\,\forall v\, A(v) \rightleftharpoons [\mathbf{r}\,A(c)$ для любой константы c сигнатуры $\Omega]$;
- $\mathbf{r}\,\exists v\, A(v) \rightleftharpoons [(\mathbf{r}\,A(c) \,\&\, \vdash A(c))$ для некоторой константы c сигнатуры $\Omega]$.

Предложение 27. *Каково бы ни было высказывание A языка Ω, если $\vdash A$, то $\mathbf{r}\,A$.*

Доказательство. Поскольку даже в выводе высказывания могут встречаться формулы со свободными переменными, чтобы использовать индукцию по выводу формулы A в ИИП мы будем доказывать более сильное утверждение: если формула $A(v_1, \ldots, v_n)$ с параметрами $v_1, \ldots, v_n$ выводима в ИИП, то реализуемо высказывание $A(c_1, \ldots, c_n)$, каковы бы ни были константы $c_1, \ldots, c_n$ сигнатуры Ω. Сначала докажем, что этим свойством обладают все аксиомы. Будем считать, что подстановка произвольных констант вместо параметров каждой из рассматриваемых аксиом уже произведена. Схемы аксиом 1 – 10 ИИП совпадают со схемами И1 – И10 ИИВ, и доказательство реализуемости замкнутых аксиом, полученных по этим схемам, проводится, как в доказательстве теоремы 42.

Рассмотрим схемы аксиом 11 и 12.

11. $\forall v\, A(v) \supset A(c)$, где c — произвольная константа сигнатуры Ω. Реализуемость этого высказывания означает, что если высказывание $\forall v\, A(v)$ реализуемо и выводимо, то $\mathbf{r}\, A(c)$, но это очевидно, ибо реализуемость $\forall v\, A(v)$ как раз и означает реализуемость $A(c)$ для любой константы c.

12. $A(c) \supset \exists v\, A(v)$, где c — произвольная константа сигнатуры Ω. Реализуемость этого высказывания означает, что если $\mathbf{r}\, A(c)$ и $\vdash A(c)$, то $\mathbf{r}\, A(c') \,\&\, \vdash A(c')$ для некоторой константы c', что очевидно, если в качестве c' взять c.

Корректность правила MP устанавливается так же, как в доказательстве теоремы 42. Докажем корректность правил Бернайса. Рассмотрим правило удаления квантора существования. Пусть это правило применяется к выводимой формуле $A(v) \supset B$, где B — высказывание. Предположим, что для нее верно доказываемое утверждение, которое означает

$$\mathbf{r}\, A(c) \,\&\, \vdash A(c) \Rightarrow \mathbf{r}\, B \tag{9.11}$$

для любой константы c. Требуется доказать реализуемость высказывания $\exists v\, A(v) \supset B$. Она означает, что если $\mathbf{r}\, A(c) \,\&\, \vdash A(c)$ для некоторой константы c, и $\vdash \exists v\, A(v)$, то $\mathbf{r}\, B$, но это очевидно в силу (9.11).

Докажем корректность правила введения квантора всеобщности. Пусть это правило применяется к выводимой формуле $B \supset A(v)$, где B — высказывание. Предположим, что для нее верно доказываемое утверждение, которое означает

$$\mathbf{r}\, B \,\&\, \vdash B \Rightarrow \mathbf{r}\, A(c) \tag{9.12}$$

для любой константы c. Требуется доказать реализуемость высказывания $B \supset \forall v\, A(v)$. Она означает, что если $\mathbf{r}\, B \,\&\, \vdash B$, то $\mathbf{r}\, \forall v\, A(v)$, т. е. $\mathbf{r}\, A(c)$ для любой константы c, но это очевидно в силу (9.12). $\square$

Теперь свойство дизъюнктивности ИИП доказывается следующим образом. Пусть высказывание $A \vee B$ выводимо в ИИП. В силу предложения 27 это высказывание реализуемо, т. е. имеет место $\mathbf{r}\, A \,\&\, \vdash A$ или $\mathbf{r}\, B \,\&\, \vdash B$. В первом случае получаем выводимость высказывания A, во втором — выводимость высказывания B.

Докажем свойство экзистенциальности ИИП. Пусть высказывание $\exists v\, A(v)$ выводимо в ИИП. В силу предложения 27 это высказывание реализуемо, т. е. имеет место $\mathbf{r}\, A(c) \,\&\, \vdash A(c)$ для некоторой константы c, но тогда выводима формула $A(c)$, что и требовалось доказать. $\square$

Мы доказали свойство дизъюнктивности для ИИП$_\Omega$ только в случае, когда сигнатура Ω содержит хотя бы одну константу. Оказывается, это ограничение несущественно.

Теорема 65. *ИИП в любой сигнатуре Ω обладает свойством дизъюнктивности.*

Доказательство. Если сигнатура Ω содержит хотя бы одну константу, доказываемое утверждение следует из теоремы 64. Пусть сигнатура Ω не содержит констант. Добавим к ней константу c и получим сигнатуру Ω'. Допустим, что имеется вывод высказывания $A \vee B$ в ИИП$_\Omega$. Этот вывод является выводом того же высказывания в ИИП$'_\Omega$. Так как по теореме 64 это исчисление обладает свойством дизъюнктивности, то имеется вывод в этом исчислении хотя бы одной из формул A и B. Заменим в формулах из этого вывода все вхождения константы c на переменную w, не входящую ни в одну из этих формул. В силу предложения 25 получится вывод формулы A° или B° в ИИП$_\Omega$. Но A и B — высказывания языка Ω и потому не содержат вхождений константы c, так что A° и B° совпадают с A и B соответственно. Следовательно, одно из высказываний A и B выводимо в ИИП$_\Omega$. $\square$

В заключение установим еще один любопытный факт, касающийся ИИП.

Теорема 66. *Пусть сигнатура Ω не содержит констант. Тогда высказывание вида $\exists v\, A(v)$ выводимо в ИИП$_\Omega$, если и только если в этом исчислении выводимо высказывание $\forall v\, A(v)$.*

Доказательство. Пусть дан вывод $\ldots, \forall v\, A(v)$ высказывания $\forall v\, A(v)$ в ИИП$_\Omega$. Продолжим его следующим образом: $\ldots, \forall v\, A(v), \forall v\, A(v) \supset A(v)$ (аксиома 11), $A(v)$ (по правилу MP),

$A(v) \supset \exists v\, A(v)$ (аксиома 12), $\exists v\, A(v)$ (по правилу МР). Получился вывод формулы $\exists v\, A(v)$. Таким образом, мы доказали, что высказывание $\exists v\, A(v)$ выводимо в ИИП, если выводимо высказывание $\forall v\, A(v)$.

Докажем обратное утверждение. Пусть высказывание $\exists v\, A(v)$ выводимо в ИИП$_\Omega$. Тогда это высказывание выводимо в ИИП$'_\Omega$, полученной добавлением к Ω константы c. В силу теоремы 64 ИИП$'_\Omega$ обладает свойством экзистенциальности, следовательно, высказывание $A(c)$ выводимо в ИИП$'_\Omega$, т. е. существует вывод этого высказывания в ИИП$'_\Omega$. Пусть w — переменная, не входящая ни в одну из формул этого вывода. В каждой формуле из этого вывода заменим все вхождения константы c на w. В силу предложения 25 мы получим вывод $\ldots, A(w)$ формулы $A(w)$ в ИИП$_\Omega$. Зафиксируем некоторую замкнутую аксиому B ИИП$_\Omega$ и продолжим этот вывод следующим образом: $\ldots, A(w)$, $A(w) \supset (B \supset A(w))$ (аксиома 1), $B \supset A(w)$ (по правилу МР), $B \supset \forall w\, A(w)$ (по правилу введения квантора всеобщности), B (аксиома), $\forall w\, A(w)$ (по правилу МР), $\forall w\, A(w) \supset A(v)$ (аксиома 11), $\forall w\, A(w) \supset \forall v\, A(v)$ (по правилу введения квантора всеобщности), $\forall v\, A(v)$ (по правилу МР). Получился вывод формулы $\forall v\, A(v)$, что и требовалось. $\square$

Заметим, что в теореме 66 существенно требование, чтобы сигнатура Ω не содержала констант. Так, если, например, сигнатура Ω содержит константу c и одноместный предикатный символ P, то формула $\exists v\,(P(c) \supset P(v))$ выводима в ИИП$_\Omega$, однако формула $\forall v\,(P(c) \supset P(v))$ невыводима.

Упражнения

1. С помощью подходящих контрмоделей доказать, что следующие формулы невыводимы в ИИП:
$$\neg\forall x\,\neg P(x) \supset \exists x\, P(x);\ (P \supset \exists x\, Q(x)) \supset \exists x\,(P \supset Q(x));$$
$$\neg\forall x\, P(x) \supset \exists x\,\neg P(x);\ \neg\exists x\,\neg P(x) \supset \forall x\, P(x);$$
$$\forall x\,(P(x) \vee \neg P(x))\,\&\,\neg\neg\exists x\, P(x) \supset \exists x\, P(x).$$

2. Доказать, что если существует модель Крипке $\mathcal{K}$ такая, что для любого высказывания Φ из множества высказываний Γ языка L_M выполнено условие $\mathcal{K} \models \Phi \Leftrightarrow \Phi \in \Gamma$, то множество Γ является M-насыщенным.

Литература

[1] А. В. Идельсон и Г. Е. Минц, ред. *Математическая теория логического вывода.* Наука, М., 1967.

[2] Е. Расёва и Р. Сикорский. *Математика метаматематики.* Наука, М., 1972.

[3] А. Френкель и И. Бар-Хиллел. *Основания теории множеств.* Мир, М., 1966.

[4] Д. Гильберт и П. Бернайс. *Основания математики. Логические исчисления и формализация арифметики.* Наука, М., 1979.

[5] А. Н. Колмогоров. О принципе *tertium non datur*. *Математический сборник*, 32:646–667, 1925. См. также [9], с. 45-69.

[6] С. К. Клини. *Введение в метаматематику.* ИЛ, М., 1957.

[7] В. А. Янков. О связи между выводимостью в интуиционистском исчислении высказываний и конечными импликативными структурами. *Доклады Академии наук СССР*, 151:1293–1294, 1963.

[8] А. Г. Драгалин. *Математический интуиционизм. Введение в теорию доказательств.* Наука, М., 1970.

[9] А. Н. Колмогоров. *Избранные труды. Математика и механика.* Наука, М., 1985.

[10] В. Е. Плиско. Исчисление А. Н. Колмогорова как фрагмент минимального исчисления. *Успехи математических наук*, 43:79–91, 1988.

[11] А. Гейтинг. *Обзор исследований по основаниям математики.* ОНТИ, М.; Л., 1936.

[12] А. Гейтинг. *Интуиционизм.* Мир, М., 1965.

[13] L. E. J. Brouwer. Begründung der Mengenlehre unabhängig vom logischen Satz vom ausgeschlossenen Dritten. I und II. *Verhandelingen der Koninklijke Akad. van Wetenschappen te Amsterdam (eerste sectie)*, 12, 1918–1919.

[14] L. E. J. Brouwer. Consciousness, philosophy and mathematics. *Proc. X Internat. Congress Philosophy*, pp. 1235–1249, 1948.

[15] G. Cantor. *Gesammelte Abhandlungen mathematischen und philosophischen Inhalts.* Berlin, 1932.

[16] G. Gentzen. Untersuchungen über das logische Schliessen. I, II. *Mathematische Zeitschrift*, 39:176–210, 405–431, 1934-1935. Русский перевод [1], с. 9-74.

[17] V. I. Glivenko. Sur quelques points de la logique de M. Brouwer. *Bulletin Classe des Sciences Academie Royal Belgique, Série 5*, 15:183–188, 1929.

[18] K. Gödel. Eine Interpretation des intuitionistischen Aussagenkalküls. *Ergebnisse eines mathematischen Kolloquiums*, 4:40, 1933.

[19] K. Gödel. Zur intuitionistischen Aussagenkalkül. *Ergebnisse eines mathematischen Kolloquiums*, 4:39–40, 1933.

[20] A. Heyting. Die formalen Regeln der intuitionistischen Logik. *Sitzungsberichte der Preussischen Akademie der Wissenschaften. Physikalisch-mathematische Klasse*, pp. 42–52, 1930.

[21] D. Hilbert. Die logischen Grundlagen der Mathematik. *Mathematische Annalen*, 88:151–165, 1923.

[22] S. Jaśkowski. Recherches sur le système de ls logique intuitioniste. *Actes du Congrès International de Philosophie Scientifique, VI, Philosophie des mathématique. Actualités scientifique et industrielle*, 393:58–61, 1936.

[23] I. Johansson. Der Minimalkalkül, ein reduzierte intuitionistischer Formalismus. *Compositio Mathematica*, 4:119–136, 1937.

[24] S. C. Kleene. On the interpretation of intuitionistic number theory. *Journal of Symbolic Logic*, 10:109–124, 1945.

[25] A. N. Kolmogorov. Zur Deutung der intuitionistischen Logik. *Mathematische Zeitschrift*, 35:58–65, 1932. Русский перевод [9], с. 142-148.

[26] B. Russell. *The principles of mathematics*. London, 1903.

[27] D. van Dalen. Lectures on intuitionism. *Lect. Notes Math.*, 337:1–94, 1973.

Предметный указатель

Учебное издание

Интуиционистская логика

В. Е. Плиско, В. Х. Хаханян

Оригинал-макет изготовлен издательской группой механико-математического факультета МГУ

Подписано в печать 23.11.2009 г.
Формат 60×90 1/16. Объем 10 п.л.
Заказ 23 Тираж 100 экз.

Отпечатано на типографском оборудовании механико-математического факультета МГУ
119992, г. Москва, Ленинские горы, д. 1.