МИНИСТЕРСТВО ВЫСШЕГО И СРЕДНЕГО
СПЕЦИАЛЬНОГО ОБРАЗОВАНИЯ РСФСР
АЛТАЙСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

МЕТОДИЧЕСКАЯ РАЗРАБОТКА ПО МАТЕМАТИЧЕСКОЙ ЛОГИКЕ

Барнаул — 1978

МИНИСТЕРСТВО ВЫСШЕГО И СРЕДНЕГО СПЕЦИАЛЬНОГО ОБРАЗОВАНИЯ РСФСР
АЛТАЙСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

МЕТОДИЧЕСКАЯ РАЗРАБОТКА
ПО МАТЕМАТИЧЕСКОЙ ЛОГИКЕ

Барнаул-1978

Настоящая методическая разработка содержит материал, излагающийся во II семестре в курсе "Математическая логика" для студентов-математиков.

Рекомендовано к изданию кафедрой алгебры и математической логики. Составитель - и.о.доцента кафедры алгебры и математической логики, кандидат физико-математических наук В.А.Ганов.

ВВЕДЕНИЕ

Предметом изучения математической логики являются математические рассуждения и основания математики. В специальных разделах математической логики изучаются такие понятия, как "математическое доказательство", "логический вывод", "интерпретация", "модель", "истинность"; вводятся строгие определения понятий "числа", "отношения", "функция"; анализируются понятия "вычислимости" и "алгоритма".

Естественно, что когда мы решаем математическую задачу, доказываем теорему или производим вычисления, то не задумываемся над тем, что такое "решение", "доказательство", "вычисление" или "число". Но если какая-нибудь задача упорно не поддается нашим усилиям, или некоторое утверждение не удается ни доказать, ни опровергнуть, то возникает вопрос, имеет ли данная задача решение, можно ли вообще доказать или опровергнуть это утверждение. Чтобы ответить на подобные вопросы приходиться уточнять, что такое "решение", "доказательство", "вычисление" и т.д.

Впервые подобные проблемы встали перед древнегреческими математиками в связи с открытием несоизмеримых отрезков (Пифагор, У1 в. до н.э.). Пифагорейцы могли бы ввести иррациональные числа и тем самым, расширили бы понятие действительного числа. Однако они не смогли построить арифметическую теорию действительного числа и пытались построить всю математику на геометрической основе. Но и на этом пути непреодолимым препятствием для математиков стала древняя задача о квадратуре круга:

" Построить квадрат, по площади равный данному кругу".

Единственными орудиями геометрических построений в древней

Греции признавались только циркуль и линейка. Оказалось, что с их помощью можно охарактеризовать только некоторые алгебраические числа, являющиеся корнями алгебраических уравнений. Для решения же задачи о квадратуре круга пришлось вновь уточнять понятие действительного числа и вводить трансцендентные числа. В 1882 году было доказано, что число   является трансцендентным и поэтому задача о квадратуре круга не разрешима циркулем и линейкой.

Следующие трудности в обосновании математики греческих ученых были связаны с понятием "бесконечности". Б е с к о н е ч н о е определялось как то, что не может быть достигнуто. Такой взгляд на бесконечность приводил к так называемым " парадоксам Зенона "(У в. до н.э.). Вот один из них.

АХИЛЛЕС И ЧЕРЕПАХА. Быстрый Ахиллес никогда не догонит черепаху. Действительно, Ахиллес должен сначала достичь точки , из которой начала движение черепаха, а за это время черепаха уползет на некоторое расстояние вперед. Ахиллес должен вновь преследовать черепаху. Это будет продолжаться бесконечное число раз,и тем самым Ахиллес никогда не догонит черепаху.

Стремясь преодолеть возникавшие трудности , греческие математики сделали замечательное открытие - "аксиоматический метод" (Евклид, Ш в. до н.э.). Согласно этому методу основные интуитивные понятия геометрии ("точка", "прямая", "плоскость") стали характеризоваться определенными недоказуемыми утверждениями ("постулатами","аксиомами"). Все дальнейшие свойства геометрических объектов выводились из аксиом с помощью специальных логических правил. Эти правила представляли собой общие схемы правильных рассуждений и составляли предмет философской логики. Впервые они систематически были изложены греческим философом Аристотелем (1У в. до н.э.). Затем почти две тысячи лет "логика Аристотеля" считалась завершенной и не нуждающейся в дополнении.

На самом же деле для анализа математических доказательств философская логика была недостаточной. И начиная с середины XIX века, предпринимаются попытки создания специальной математической логики, позволяющей анализировать любые математические рассуждения и понятия. Ее основы были заложены в трудах Джорджа Буля и Августа де Моргана.

В это же время в математике начинает широко распространяться понятие м н о ж е с т в а . Действительные числа определяются дедекиндовыми сечениями в множестве рациональных чисел, действительные функции и отношения представляются в виде специальных множеств действительных чисел. Этим самым трудности , связанные с обоснованием математики, переместились в область теории множеств. Возникла необходимость в уточнении понятия бесконечного множества. В 1879-84 годах немецкий математик Георг Кантор создал общую теорию бесконечных множеств, которая оказала огромное влияние на развитие математики. Однако трудности , связанные с понятием бесконечности, проявились и в теории множеств. В конце XIX века в ней были обнаружены парадоксы. Наибольшую известность приобрел парадокс Рассела:

ПАРАДОКС РАССЕЛА. Совокупность всех множеств распадается на два непустых класса A и B : A - класс всех множеств, которые не содержат себя в качестве элемента, B - класс всех остальных множеств, т.е. тех множеств, которые содержат себя в качестве элемента. Согласно интуитивному понятию "множества" класс A является множеством и потому обязан входить в A или в B . Но если A входит в A , то A должен входить в B , и наоборот, если A входит в B , то A должен входить A . А так как A и B не могут иметь общих элементов, то возникает парадокс.

Часто парадокс Рассела излагается в следующей популярной форме. "Парикмахер некоторой деревни берет на себя обязательство брить всех тех и только тех жителей деревни, которые себя не бреют. Возникает вопрос: "Бреет ли себя парикмахер?" Если он себя бреет, то он не должен себя брить согласно обязательству. Если же он не бреет себя, то должен себя брить согласно тому же обязательству. В обоих случаях мы получили противоречие".

Аналогичные парадоксы были обнаружены в анализе рассуждений, например, рассмотрим ПАРАДОКС ЛЖЕЦА: Некто за всю свою жизнь произнес только одну фразу: "Я лгу." Спрашивается, прав ли он?

Возникшие трудности математической логики благоприятно сказались на ее развитии. В начале ХХ века Рассел, Цермело, Гильберт разрабатывают различные методы устранения обнаруженных парадоксов. В 30-ые годы Черч, Клини, Пост, Тьюринг создают теорию алгоритмов. С ее созданием методы математической логики впервые находят непосредственное практическое применение в моделировании мышления и в создании электронно-вычислительных машин.

Впоследние годы на стыке основных разделов математической логики, алгебры, топологии, теории вероятностей и других наук возникли и интенсивно развивается такие новые направления , как конструктивная математика, теоретическая кибернетика, теория абстрактных автоматов, модальная логика, интуиционизм, теория моделей, математическая лингвистика, теория нумераций и другие.

В данном пособии мы подробно рассматриваем традиционные логические направления и связанные с ними понятия теории моделей и теории алгоритмов. В первом разделе рассматривается содержательный подход к изучению высказываний. Используя интуитивное понятие истинности, мы вводим основные логические операции над высказываниями и исследуем их свойства. В дальнейшем к изучению высказывания применяется аксиоматический метод. Мы строим специальную формальную систему, которая называется исчислением высказывания, и продолжаем изучение свойств логических операций с помощью доказуемых формул. Кроме того, мы обращаем особое внимание на сравнение содержательного и формального подходов к изучению высказываний. Доказывается равносильность этих подходов.

в разделе Логика предикатов мы расширяем наше исследование, вводя новые объекты (константы, переменные, предикаты и кванторы), которые позволяют анализировать структуру более широкого класса суждений по сравнению с алгеброй высказываний. В разделе Исчисление предикатов эти исследования продолжаются с помощью аксиоматического метода. В конце раздела приводятся основные утверждения теории моделей. В заключительном разделе дается определение алгоритма в терминах "машин Тьюринга" и изучаются простейшие свойства этого понятия.

Раздел 1. Алгебра высказываний.

1. Формальный язык.

Основным средством передачи тех или иных рассуждений в математике является язык формул. Специальные символы и буквы обозначают различные математические объекты и действия над ними, составленные из них формулы выражают некоторые математические утверждения или описывают математические процессы. И до сих пор формулы рассматривались нами как вспомогательное средство. В математической логике формулы сами становятся объектом изучения. Мы рассматриваем строение формул, способы придания им определенного содержания и основные методы изложения формальных теорий.

Язык формул, в котором описываются утверждения некоторой теории называется формальным языком данной теории. Он состоит из алфавита - множества исходных символов и из словаря - множества правильно образованных формул. Любая конечная последовательность символов алфавита называется словом. Число символов, входящих в слово, называется его длиной.

Пример 1. Пусть алфавит состоит из символов: $0, 1, +, \cdot, =, a, в, (,)$. Тогда последовательности этих символов: aa, $aвaв$, $(0+1)\cdot 1$, $(a+в+a)$, $0+1=+=$ являются словами в данном алфавите и имеют длины 2, 4, 7, 7, 6, соответственно.

Два слова называются графически равными, если они имеют одинаковые длины и их соответствующие символы одинаковы. Например, слова $a+в$ и $в+a$ различны, так как различны их символы, стоящие на первом и третьем местах. Для обозначения произвольных слов данного формального языка мы будем использовать большие латинские буквы, не входящие в алфавит: A, B, C, X, Y.

Пусть A, B - слова какого-нибудь формального языка. Композицией или произведением слов A, B называется слово $A \cdot B$, получаемое приписыванием слова B к слову A справа. Композиция зависит от порядка слов-сомножителей. Например, композиция слов aba, bab есть слово $ababab$, и композиция слов bab, aba есть $bababa$.

Допускается рассмотрение пустого слова, не содержащего символов. Оно обозначается специальным символом Λ, его длина равна нулю. Очевидно, что $\Lambda \cdot A = A \cdot \Lambda = A$.

Отрезки слова A называются его подсловами. Если A_1 подслово A, то существуют слова X, Y (возможно пустые), удовлетворяющие равенству: $A = X \cdot A_1 \cdot Y$. В таких случаях говорят, что A_1 имеет вхождение в A. Подслово A_1 может иметь несколько вхождении в A. Например, $A_1 = aba$ имеет два вхождения в $A = ababab = \Lambda \cdot aba \cdot bab = ab \cdot aba \cdot b$.

Пусть в слове A некоторое вхождение подслова A_1 определяется равенством $A = X \cdot A_1 \cdot Y$, и B - какое-нибудь слово. Слово $X \cdot B \cdot Y$ называется результатом подстановки слова B в слово A вместо выделенного вхождения подслова A_1. Так, подставляя в слово $ababab$ вместо второго вхождения aba слово b, получим слово $abbb$.

Важное место в изучении формальных языков занимают определения и доказательства с помощью математической индукции. Приведем несколько примеров.

Пример 2. Операция сложения чисел определяется с помощью математической индукции следующим образом:

1. База индукции: $(m+0) = m$;
2. Индукционное предположение: пусть $(m+n)$ определено.
3. Индукционный шаг: полагаем, что $m+(n+1) = (m+n)+1$.

Пример 3. Рассмотрим формальный язык, алфавит которого содержит: $0, 1$ - символы констант, $a, b, c, \ldots$ — символы переменных, $+, \cdot$ - символы арифметических действий, $($, $)$ левая и правая скобки. Выражения $(a+b)\cdot c$, $(0+1)$, $+(+a)$, $0 \cdot 1 + a$, $+b \cdot aba$ являются словами этого языка. Однако не все из них суть правильные арифметические выражения. Используя математическую индукцию по длине слова, определим арифметические выражения данного языка.

1. Символы констант $0, 1$ и символы числовых переменных $a, b, c,$ являются арифметическими выражениями.

2. Пусть B и C - произвольные слова, являющиеся арифметическими выражениями. Тогда слова $(B+C)$ и $(B \cdot C)$ являются арифметическими выражениями.

3. Арифметическими выражениями называются только те слова, которые являются арифметическими выражениями вследствие пунктов 1,2.

На первый взгляд схема данного определения отличается от стандартной схемы математической индукции. Однако легко увидеть, что пункт 1 есть база индукции, в нем определяется арифметические выражения , имеющие длину один. Затем, если B и C ранее определенные арифметические выражения, то из них образуются новые арифметрические выражения вида . Нетрудно выделить индукционное предположение и индукционный шаг. Пункт 3 необходим, в нем подчеркивается, что арифметические выражения могут быть получены только согласно правилам, указанным в пунктах 1,2.

Используя данное индукционное определение арифметических выражений, мы можем доказывать различные свойства этих выражений. Такой метод доказательства называется индукцией по построению арифметического выражения.

Пример 4. "Каждое арифметическое выражение имеет одинаковое число левых и правых скобок" - докажем это утверждение индукцией по построению арифметического выражения.

1. Если A является символом константы или числовой переменной, то A не содержит скобок и наше утверждение выполняется.

2. Пусть B и C произвольные арифметические выражения и каждое из них содержит одинаковое число левых и правых скобок. Тогда очевидно, что $(B+C)$ и $(B \cdot C)$ тоже содержат по одинаковому числу левых и правых скобок. Утверждение доказано.

Приведенные примеры показывают, что при изложении некоторых теории в формальном языке целесообразно ограничиться рассмотрением только тех слов, которые описывают осмысленные выражения исследуемой теории. Поэтому в каждом формальном языке вводится понятие формулы и изучение теории сводится к анализу формул языка.

Существует два подхода к анализу формул: содержательный и формальный. При содержательном подходе каждой формуле приписывается определенный смысл (содержание). В этом случае формулы будут выражать некоторые утверждения данной теории, и мы можем говорить об их истинности или ложности. Изучение теории сводится к выяснению истинности тех или иных формул данного языка. Содержательное изучение формального языка называется семантикой языка.

При формальном подходе используется аксиоматический метод. Согласно этому методу построение изучаемой теории осуществляется с помощью задания определенной "формальной системы". Определение этого важного понятия включает в себя следующие пункты: формальный язык, аксиомы, правила вывода, доказательство. Первый из этих пунктов рассмотрен нами выше.

Аксиомы. Некоторые формулы языка объявляются аксиомами. Выбор аксиом зависит от изучаемой теории. Например, если изучается геометрия, аксиомы соответствуют некоторым свойствам геометрических объектов. Заметим, что совсем не обязательно иметь конечное число аксиом, - важно уметь отличать и выделять аксиомы.

Правила вывода - это правила, позволяющие переходить от одной группы формул к некоторой другой формуле. О последней говорят, что она получена с помощью соответствующего правила вывода из упомянутой группы\формул.

Доказательство - это конечная последовательность формул, каждая из которых либо является аксиомой, либо - результат применения одного из правил вывода к предыдущим формулам этой последовательности. Последняя формула в доказательстве называется доказуемой или теоремой формальной системы.

Совокупность доказуемых формул называется исчислением. Изучение чисто формальной части языка называется синтаксисом языка.

Удачной иллюстрацией формального подхода является игра в шахматы или решение шахматной задачи. Шахматные символы

Кр, Ф, С, К, Л, П, a, b, ..., h, 1, 2, ..., 8, :, +, ×, 0-0

образуют алфавит, шахматные позиции являются формулами. Исходные позиции или заданные позиции в шахматных задачах суть аксиомы. Правила вывода - это правила передвижения фигур, доказательство - запись шахматной игры. Различные принципы , законы, ловушки шахматной игры образуют синтаксис шахматного языка.

На этом мы пока заканчиваем абстрактное изучение формальных языков. Другие вопросы из этой области будут рассмотрены нами в ходе изложения курса.

2. Высказывания, логические операции.

Анализ рассуждений мы начинаем с изучения высказываний . Раздел , в котором изучаются высказывания , будем называть алгеброй высказываний. Само высказывание мы определяем как любое утверждение, о котором имеет смысл судить истинно оно или ложно. В обычном разговорном языке высказывания выражаются повествовательными предложениями, в отличие от них вопросительные предложения выражают вопросы, повелительные предложения - приказы.

Пример 5. а) " + 7 больше, чем - 7 ", "Луна вращается вокруг Земли" - эти утверждения являются истинными высказываниями;

б) " $2 \cdot 2 = 5$ ", "Марк Твен - автор "Золотого теленка", - эти утверждения являются ложными высказываниями;

в) "Завтра будет солнечная погода", "Сегодня воскресенье" - тоже высказывания, хотя нельзя определенно решить истинны они или ложны;

г) "Что такое высказывание?", "Запишите следующее определение", - вопрос и команда, соответственно.

Истинность или ложность какого-либо высказывания можно определить, только вникнув в его содержание. Однако в данном разделе мы ставим цель изучить основные логические связки, с помощью которых из отдельных высказываний составляются различные математические суждения. И чтобы придать общность нашим исследованиям, мы отвлекаемся от конкретного содержания высказываний. Вместо этого мы предполагаем, что имеется некоторый набор простейших высказываний

$$P_1, P_2, \ldots, P_k, \ldots,$$

каждое из которых является истинным или ложным. Остальные высказывания называются сложными и образуются из простейших с помощью специальных логических операций. Для сравнения рассмотрим несколько сложных высказываний из обычного разговорного языка.

Пример 6. а) "Завтра у меня будет свободное время, и я смогу дочитать эту книгу", б) "Если я дочитаю эту книгу, то завтра у меня будет свободное время", в) "Не верно, что я дочитаю эту книгу", г) " Либо я дочитаю эту книгу, либо завтра у меня не будет свободного времени".

Буквой A обозначим простейшее высказывание "Завтра у меня будет свободное время", и буквой B обозначим "Я дочитаю эту книгу". Тогда сложные высказывания а) – г) можно символически представить в виде: а) " A и B ", б) "Если B , то A ", в) " Не верно, что B ", г) "Либо B , либо не A ". Отсюда видно, что сложные высказывания образуются из простейших с помощью специальных соединительных союзов и оборотов. В алгебре высказываний эту роль выполняют логические операции: конъюнкция, дизъюнкция, отрицание и импликация. Но прежде чем определять эти понятия, опишем формальный язык алгебры высказываний.

Определение 1. 1). Алфавит. Основными символами алгебры высказываний являются:

$P_1, P_2, \ldots, P_k, \ldots$ — символы простейших высказываний,

$A, B, C, A_1, \ldots, A_n$ — высказывательные переменные.

$\bar{\ }$, $\wedge$, $\vee$, $\longrightarrow$ — логические символы,

(,) — правая и левая скобки.

2). Формулы. а) Символы простейших высказываний и высказывательные переменные являются формулами,

б) Если A и B формулы, то $\bar{A}, \bar{B}, (A\wedge B), (A\vee B), (A\longrightarrow B)$ являются формулами,

в) других формул нет.

Пример 7. $A, \bar{B}, \bar{\bar{A}}, (\overline{\bar{A}\wedge B}), (\bar{A}\longrightarrow B), (A\vee(A\wedge B))$ - формулы, $(A\vee B\longrightarrow C), (A\rightarrow B\rightarrow C), (A\rightarrow B)\longrightarrow((A\rightarrow B\rightarrow C)\rightarrow$ не являются формулами, ибо в этих словах не хватает скобок.

Если формула A обозначает истинное высказывание, то будем писать $A = И$, и если A обозначает ложное высказывание, то будем писать $A = Л$. Символы $И$, $Л$ будем называть истинностными значениями формул.

Логические символы $\bar{\ }$, $\wedge$, $\vee$, $\longrightarrow$ обозначают следующие логические операции.

ОПРЕДЕЛЕНИЕ 2. Отрицание - логическая операция, которая каждому высказыванию A сопоставляет высказывание $\bar{A}$, являющееся истинным, если $A = Л$, и ложным, если $A = И$.

Зависимость между истинностными значениями высказываний A и $\bar{A}$ может быть выражена следующей таблицей, которая называется таблицей истинности для отрицания:

A	$\bar{A}$
И	Л
Л	И

В первом столбце выписаны истинностные значения A, а во втором - соответствующие значения высказывания $\bar{A}$.

В разговорном языке высказывание $\bar{A}$ читается "не A", "не верно, что A" или "A не выполняется". Вместо $\bar{A}$ иногда используется обозначение $\neg A$. Заметим, что понятие "слово" определялось нами как линейная последовательность символов алфавита. В этом отношении обозначение $\neg A$ в большей степени соответствует данному определению, чем $\bar{A}$. Но мы будем употреблять традиционное обозначение $\bar{A}$, которое не приводит к каким либо серьезным недоразумениям.

ОПРЕДЕЛЕНИЕ 3. Конъюнкция - логическая операция, которая двум высказываниям A и B сопоставляет высказывание $(A \wedge B)$, являющееся истинным в том и только том случае , когда $A = И$ и $B = И$. Конъюнкции соответствует следующая таблица истинности:

A	B	$(A \wedge B)$
И	И	И
И	Л	Л
Л	И	Л
Л	Л	Л

В разговорном языке конъюнкции $(A \wedge B)$ соответствуют следующие обороты: " A и B ", "не только A , но и B ", " A вместе с B ", " A , хотя и B ", " B , несмотря на A ". Кроме обозначения $(A \wedge B)$ употребляется обозначение $(A \& B)$.

ОПРЕДЕЛЕНИЕ 4. Дизъюнкция - это логическая операция , которая двум высказываниям A и B сопоставляет высказывание $(A \vee B)$, являющееся ложным в том и только том случае, когда $A = Л$ и $B = Л$. Дизъюнкции соответствует следующая таблица истинности:

A	B	$(A \vee B)$
И	И	И
И	Л	И
Л	И	И
Л	Л	Л

В разговорном языке дизъюнкции $(A \vee B)$ соответствуют следующие обороты: " A или B ", " A или B , или оба", "либо A , либо B ."

ОПРЕДЕЛЕНИЕ 5. Импликация - логическая операция, которая двум высказываниям A и B сопоставляет высказывание $A \rightarrow B$, являющееся ложным в том и только том случае, когда $A = И$ и $B = Л$. Импликации соответствует следующая таблица истинности:

A	B	$(A \to B)$
И	И	И
И	Л	Л
Л	И	И
Л	Л	И

В разговорном языке импликации $(A \to B)$ соответствуют обороты: "если A, то B", "коль скоро A, то B", "в случае A имеет место B", "из A следует B", "для B достаточно A", "для A необходимо B". Кроме $(A \to B)$ используются обозначения: $(A \supset B)$ или $(A \Rightarrow B)$. В импликации $(A \to B)$ высказывание A называется посылкой, а высказывание B - заключением. Согласно таблице истинности из истинной посылки A должно следовать истинное заключение B, в противном случае импликация $(A \to B)$ ложна. В случае ложной посылки A заключение B может быть как истинным, так и ложным,- импликация остается истинной. Этот факт часто выражают словами: "Из истины следует истина, а из лжи следует что угодно".

Введенных выше логических операций достаточно для выражения всевозможных связей между высказываниями, и мы можем дать строгое определение истинностного значения формулы.

Определение 6. 1). Символы простейших высказываний и высказывательные переменные обозначают некоторые высказывания, которые являются истинными или ложными. Полагаем, что истинностные значения этих символов совпадают с истинностными значениями обозначаемых ими высказываний.

2). Если формулы A, B имеют определенные истинностные значения, то значения формул $\bar{A}$, $\bar{B}$, $(A \wedge B)$, $(A \vee B)$, $(A \to B)$ определяются согласно определениям 2 - 5.

Пример 8. Построим таблицы истинности для формул $(\overline{A \wedge B})$, $((\bar{A} \to B) \to (C \to \bar{A}))$, $((A \vee B) \wedge (A \vee C))$.

A	B	$\overline{(A \wedge \bar{B})}$
И	И	И
И	Л	Л
Л	И	И
Л	Л	И

A	B	C	$((\overline{A \to B}) \to (C \to B))$	$((A \vee B) \wedge (A \vee C))$
И	И	И	И	И
И	И	Л	И	И
И	Л	И	Л	И
И	Л	Л	И	И
Л	И	И	И	И
Л	И	Л	И	Л
Л	Л	И	И	Л
Л	Л	Л	И	Л

В приведенных таблицах истинности слева стоят всевозможные наборы истинностных значений переменных , входящих в рассматриваемые формулы . В общем случае n высказывательных переменных $A_1, \ldots, A_n$ имеют 2^n различных наборов истинностных значений. Доказательство этого факта проводится индукцией по n , и мы предоставляем его читателю в качестве самостоятельного упражнения.

3. Тождественно истинные формулы.

Формулы алгебры высказываний используются нами для описания рассуждений: каждому рассуждению соответствует определенная формула. В свою очередь, при замене букв , входящих в произвольную формулу, конкретными высказываниями мы получаем определенные утверждения. Однако из той же самой формулы при замене переменных другими высказываниями мы будем получать новые рассуждения. Тем самым, формулы алгебры высказываний описывают не сами рассуждения, а их схемы. И первоочередной интерес для нас представляют те формулы, которые описывают схемы правильных рассуждений.

Рассмотрим рассуждение: " 127 - простое число, или 127 не является простым числом". Это утверждение верно независимо от истинности составляющих его простейших высказываний. Схема этого рассуждения описывается формулой $(B \vee \bar{B})$, которая принимает значение "истина" также независимо от истинностных значений буквы B. Если в $(B \vee \bar{B})$ вместо B подставлять другие высказывания, то мы будем получать только истинные утверждения. Подобные формулы выражают схемы правильных рассуждений и описывают их законы.

Определение 7. Формула A алгебры высказываний называется тождественно истинной или тавтологией, если она истинна при любых истинностных значениях входящих в нее букв (обозначение: $\models A$)

Рассмотрим основные тавтологии алгебры высказываний и законы их образования.

ТЕОРЕМА 1. Пусть Q формула алгебры высказываний, в которую входят переменные $A_1, \ldots, A_n$, а Q^* – формула,[*)] получаемая из Q одновременной подстановкой формул $R_1, \ldots, R_n$ вместо переменных $A_1, \ldots, A_n$ соответственно. Тогда если $\models Q$, то $\models Q^*$

Доказательство. Значения формул $R_1, \ldots, R_n$ являются допустимыми значениями переменных $A_1, \ldots, A_n$, а так как формула Q истинна независимо от значения переменных $A_1, \ldots, A_n$, то Q^* будет истинна независимо от значений формул $R_1, \ldots, R_n$, т.е. Q^* тождественно истинна.

Пример 9. Формула $(A \to A)$ тождественно истинна, следовательно, следующие формулы будут тождественно истинными:

$$((B \wedge \bar{C}) \to (B \wedge \bar{C})), \quad ((B \to C) \to (B \to C))$$

Рассмотрим основные свойства логических операций. Обычно свойства математических операций описываются с помощью специальных тождеств или равенств, включающих эти операции. В алгебре высказываний вместо равенства мы используем отношение эквивалентности формул.

ОПРЕДЕЛЕНИЕ 8. Формулы R и Q называются эквивалентными, если значения R и Q совпадают при любых значениях входящих в них переменных. (Обозначение: $R \sim Q$)

Заметим, что формулы R и Q вообще говоря зависят от

---

*) Интуитивно ясно, что Q^* есть формула. Строгое доказательство этого факта производится индукцией по длине формулы Q.

разных переменных: $R = R(A_1, \ldots, A_n)$, $Q = Q(B_1, \ldots, B_m)$.
Однако при сравнении этих формул желательно, чтобы они зависели от одних и тех же букв. С этой целью допускается введение так называемых "фиктивных переменных", т.е. мы считаем, что высказывание $R(A_1, \ldots, A_n)$ зависит не только от $A_1, \ldots, A_n$, но и от $B_1, \ldots, B_m$, хотя последние быть может не входят в формулу $R(A_1, \ldots, A_n)$. Учитывая это замечание, можно считать, что формулы R и Q эквивалентны, если они имеют одинаковые таблицы истинности.

Пример 10. $(A \vee (A \wedge B)) \sim A$

A	B	$(A \vee (A \wedge B))$	A
И	И	И	И
И	Л	И	И
Л	И	Л	Л
Л	Л	Л	Л

Теорема 2. При любом выборе формул A, B, C алгебры высказываний выполняются следующие эквивалентности:

1. $(A \wedge B) \sim (B \wedge A)$ / коммутативность /
   $(A \vee B) \sim (B \vee A)$
2. $(A \wedge (B \wedge C)) \sim ((A \wedge B) \wedge C)$ / ассоциативность /
   $(A \vee (B \vee C)) \sim ((A \vee B) \vee C)$
3. $(A \vee (B \wedge C)) \sim ((A \vee B) \wedge (A \vee C))$ / дистрибутивность /
   $(A \wedge (B \vee C)) \sim ((A \wedge B) \vee (A \wedge C))$
4. $A \wedge A \sim A$ / идемпотентность /
   $A \vee A \sim A$
5. $(A \vee (A \wedge B)) \sim A$ / закон поглощения /
   $(A \wedge (A \vee B)) \sim A$
6. $(A \vee \bar{A}) \wedge B \sim B$
   $(A \wedge \bar{A}) \vee B \sim B$
7. $(\overline{A \vee B}) \sim (\bar{A} \wedge \bar{B})$ / законы де Моргана/
   $(\overline{A \wedge B}) \sim (\bar{A} \vee \bar{B})$

8. $\bar{\bar{A}} \sim A$ / закон двойного отрицания /

9. $(A \vee \bar{A}) \sim И$ / закон исключенного третьего /

$(A \wedge \bar{A}) \sim Л$ / закон противоречия /

10. $\bar{Л} \sim И$, $\bar{И} \sim Л$

11. $A \vee И \sim И$, $A \wedge Л \sim Л$

12. $A \vee Л \sim A$, $A \wedge И \sim A$

13. $(A \longrightarrow B) \sim (\bar{A} \vee B)$

Буквами $И$ и $Л$ здесь обозначены соответственно тождественно истинная и тождественно ложная формулы; справа указаны общепринятые названия свойств, выражаемых данными эквивалентностями. Чтобы доказать эквивалентность формул достаточно вычислить таблицы истинности формул, стоящих по обе стороны от знака $\sim$ и сравнить соответствующие значения этих формул. Доказательство теоремы мы предлагаем читателю в качестве самостоятельного упражнения.

Когда мы вводили логические операции, то стремились убедить читателя в том, что они выполняют роль связок между высказываниями. Естественно было ожидать, что свойства логических операций ($^{-}$, $\wedge$, $\vee$, $\rightarrow$) будут идентичны свойствам соответствующих им логических связок / не, и, или, если ... то ... /Отчасти так и произошло, например: высказывание « Кассиус Клей выиграет этот бой, или он его проиграет » эквивалентно $И$; а высказывание « не верно, что этим летом я побывал в Москве или посещу Ленинград » эквивалентно высказыванию « этим летом я не побывал в Москве и не посещу Ленинград ». Эквивалентность этих высказываний соответствует законам 6 и 7 теоремы 2.

Однако в обычных рассуждениях приходится иметь дело с конкретным смыслом рассматриваемых высказываний. В таких случаях даже место расположения высказываний может внести дополнительный смысл в рассуждения, и поэтому возможны нарушения указанных свойств. Например, хотя для конъюнкции выполняется закон коммутативности, высказывания: "Джон купил автомобиль и разбился", "Джон разбился и купил автомобиль",-нельзя считать эквивалентными. В этом примере порядок высказываний наводит на мысль о следовании во времени.

В математических рассуждениях, изучение которых составляет основную цель данного курса, каждое высказывание принимает только одно истинностное значение, которое не меняется в ходе всего рассуждения и не зависит от положения этого высказывания в рассуждениях. Поэтому указанные в теореме 2 законы отражают действительные свойства логических связей между математическими высказываниями. Например, при решении числовых неравенств часто мы используем как утверждения вида " $n>2$ и $n>3$ ", так и утверждения вида " $n>3$ и $n>2$ ", считая их эквивалентными.

ТЕОРЕМА 3 (о замене эквивалентных формул). Пусть C_A формула, содержащая некоторую формулу A в качестве составной части,[*] $C_A = X \cdot A \cdot Y$, и C_B - формула, получаемая из C_A подстановкой формулы B вместо выделенного вхождения A: $C_B = X \cdot B \cdot Y$. Тогда если $A \sim B$, то $C_A \sim C_B$.

Доказательство. Пусть $A \sim B$, тогда A и B имеют одинаковые таблицы истинности и следовательно, при вычислении значений формулы C_A мы можем менять значения A на значения формулы B, - результат не изменится, так как эти значения одинаковы. Отсюда следует, что формулы C_A и C_B эквивалентны.

Эта теорема позволяет использовать эквивалентности для преобразования формул.

[*] Смотрите сноску на с. 18.

Пример 11. $(A \to ((B \vee C) \to (C \to \bar{A}))) \overset{(13)}{\sim}$

$$\sim (A \to ((B \vee C) \to (\bar{C} \vee \bar{A}))) \overset{(13)}{\sim}$$

$$\sim (A \to (\overline{(B \vee C)} \vee (\bar{C} \vee \bar{A}))) \overset{(13)}{\sim}$$

$$\sim (\bar{A} \vee (\overline{B \vee C}) \vee \bar{C} \vee \bar{A} \overset{(4)}{\sim} ((\overline{B \vee C}) \vee \bar{C} \vee \bar{A}) \overset{(7)}{\sim}$$

$$\sim ((\bar{B} \wedge \bar{C}) \vee \bar{C}) \vee \bar{A} \overset{(5)}{\sim} (\bar{C} \vee \bar{A}).$$

Эквивалентность 13 теоремы 2 показывает, что вместо высказываний вида $(A \to B)$ можно использовать высказывания вида $(\bar{A} \vee B)$. Но в анализе доказательств и выводов употребление импликации оказывается более удобным, и потому ей отводится важная роль. Обычно каждая теорема формулируется в виде : "если A, то B ", т.е. в виде $(A \to B)$. Многие доказательства осуществляются по следующей схеме: сначала устанавливается истинность высказываний A и $(A \to B)$, а затем делается вывод : B истинно. Такой способ доказательств обосновывается в следующей теореме.

ТЕОРЕМА 4. Если $\vDash A$ и $\vDash (A \to B)$, то $\vDash B$.

Доказательство. Пусть A и $(A \to B)$ тавтология, тогда для любых истинностных значений переменных формулы A, $(A \to B)$ истинны. Так как $A = И$, то импликация $(A \to B)$ равна истине только при $B = И$. Поэтому формула B истинна при любых значениях своих переменных, т.е. $\vDash B$.

В следующем разделе для анализа схем математических доказательств свойства логических операций $(\bar{\ }, \wedge, \vee, \to)$ оказывается более удобным задавать в виде специальных импликаций / аксиом /. В следующей теореме мы приводим эти импликации и утверждаем, что они являются тавтологиями .

ТЕОРЕМА 5. Для любых высказываний A, B, C следующие формулы являются тавтологиями:

I.1. $(A \to (B \to A))$

2. $((A \to B) \to ((A \to (B \to C)) \to (A \to C)))$

II.1. $((A \wedge B) \to A)$

2. $((A \wedge B) \to B)$

3. $(A \to (B \to (A \wedge B)))$

III.1. $(A \to (A \vee B))$

2. $(B \to (A \vee B))$

3. $((A \to C) \to ((B \to C) \to ((A \vee B) \to C)))$

IV.1. $((A \to B) \to ((A \to \bar{B}) \to \bar{A}))$

2. $(\bar{\bar{A}} \to A)$.

Доказательство предоставляется читателю в качестве самостоятельного упражнения.

4. Совершенные нормальные формы.

Пусть дана таблица истинности / сама по себе , как объект /:

A	B	C	$P(A,B,C)$
И	И	И	Л
И	И	Л	Л
И	Л	И	Л
И	Л	Л	И
Л	И	И	Л
Л	И	Л	Л
Л	Л	И	Л
Л	Л	Л	Л

Возникает задача: построить формулу P, имеющую такую же таблицу истинности.

В приведенной таблице искомая формула должна быть истинной только на наборе истинностных значений (И, Л, Л) . На таком же наборе истинна формула $(A \wedge \bar{B} \wedge \bar{C})$, и более того, эта формула в остальных случаях ложна. Поэтому формула $(A \wedge \bar{B} \wedge \bar{C})$ искомая:

$$P \sim (A \wedge \bar{B} \wedge \bar{C}).$$

Чтобы обосновать этот метод построения искомой формулы, введем следующие понятия.

ОПРЕДЕЛЕНИЕ 10. а/. Формула $P(A_1,\dots,A_n)$ называется элементарной конъюнкцией, если $P(A_1,\dots,A_n)$ есть конъюнкция высказывательных букв или их отрицаний.

б/. Формула $P(A_1,\dots,A_n)$ называется элементарной дизъюнкцией, если она есть дизъюнкция высказывательных букв или их отрицаний.

Пример 12. $(A\wedge\bar{B}\wedge\bar{C})$, $(\bar{A}\wedge B\wedge\bar{C})$, $(B\wedge C)$, $\bar{A}$ - элементарные конъюнкции, $(A\vee\bar{B}\vee\bar{C})$, $(A\vee B)$, $(B\vee\bar{A})$, $\bar{A}$, A, $\bar{B}$ элементарные дизъюнкции.

ЛЕММА 1. а/. Каждой элементарной конъюнкции соответствует точно один набор истинностных значений входящих в нее букв, при котором эта конъюнкция истинна.

б/. Каждой элементарной дизъюнкции соответствует точно один набор истинностных значений входящих в нее букв, при котором эта дизъюнкция ложна.

Доказательство. а/. Рассмотрим элементарную конъюнкцию, например: $A\wedge\bar{B}\wedge\bar{C}\wedge D$. Очевидно, что эта конъюнкция истинна в том и только том случае, когда входящие в нее буквы без отрицания имеют значение $И$, а буквы с отрицанием имеют значение $Л$:

$$(A\wedge\bar{B}\wedge\bar{C}\wedge D)=И \longleftrightarrow (A=И,\ B=Л,\ C=Л,\ D=И).$$

б/. Так же легко увидеть, что элементарная дизъюнкция /например, $\bar{A}\vee B\vee\bar{C}\vee D$/ ложна тогда и только тогда, когда входящие в нее буквы без отрицания имеют значение $Л$, а буквы с отрицанием – значение $И$:

$$(\bar{A}\vee B\vee\bar{C}\vee D)=Л \longleftrightarrow (A=И,\ B=Л,\ C=И,\ D=Л).$$

ОПРЕДЕЛЕНИЕ 11. а/. Формула $P(A_1,\dots,A_n)$ называется совершенной дизъюнктивной нормальной формой /сокращенно: СДНФ/, если $P(A_1,\dots,A_n)$ есть дизъюнкция элементарных конъюнкций, в которых каждая буква $A_1,\dots,A_n$ встречается ровно один раз.

б/. Формула $P(A_1,\dots,A_n)$ называется совершенной конъюнктивной нормальной формой /СКНФ/, если $P(A_1,\dots,A_n)$ есть конъюнкция элементарных дизъюнкций, в которых каждая буква $A_1,\dots,A_n$

встречается ровно один раз.

Пример 13. $P(A,B,C)=(A\wedge\bar{B}\wedge\bar{C})\vee(A\wedge B\wedge C)\vee(A\wedge\bar{B}\wedge C)$ – СДНФ,

$P(A,B,C)=(\bar{A}\vee B\vee C)\wedge(A\vee B\vee\bar{C})\wedge(\bar{A}\vee\bar{B}\vee\bar{C})$ – СКНФ,

$P(A,B,C)=(A\vee\bar{B})\wedge(A\vee C)$ не СКНФ, ибо в первой скобке нет C, а во второй нет B, $P(A,B,C)=(A\wedge B)\vee(A\wedge B\wedge C)$ – не СДНФ, ибо в первой скобке нет буквы C.

ТЕОРЕМА 6. а/. Всякая не тождественно ложная формула $P(A_1,\dots,A_n)$ эквивалентна совершенной дизъюнктивной нормальной форме;

б/. Всякая не тождественно истинная формула $P(A_1,\dots,A_n)$ эквивалентна совершенной конъюнктивной нормальной форме.

Доказательство. а/. По данной формуле $P(A_1,\dots,A_n)$ строим ее таблицу истинности, в этой таблице выделяем все наборы истинностных значений, на которых $P(A_1,\dots,A_n)=И$. Берем дизъюнкцию тех элементарных конъюнкций, которые истинны на выделенных наборах,– это искомая СДНФ.

б/. По данной формуле строим таблицу истинности, в этой таблице выделяем все наборы истинностных значений, на которых $P(A_1,\dots,A_n)=Л$. Затем берем конъюнкцию тех элементарных дизъюнкций, которые ложны на выделенных наборах,– это искомая СКНФ.

Доказательство данной теоремы также дает решение задачи, поставленной нами в начале пункта, а именно, по данной таблице истинности мы строим соответствующие СКНФ или СДНФ, которые и будут искомыми формулами.

Пример 14. Построить СДНФ и СКНФ для

$$P=(A\to((B\vee C)\to(C\to\bar{A})))$$

A	B	C	$(A\to((B\vee C)\to(C\to\bar{A})))$
И	И	И	Л
И	И	Л	И
И	Л	И	Л
И	Л	Л	И
Л	И	И	И
Л	И	Л	И
Л	Л	И	И
Л	Л	Л	И

$P \sim (A \wedge B \wedge \bar{C}) \vee (A \wedge \bar{B} \wedge \bar{C}) \vee (\bar{A} \wedge B \wedge C) \vee (\bar{A} \wedge B \wedge \bar{C}) \vee (\bar{A} \wedge \bar{B} \wedge C) \vee (\bar{A} \wedge \bar{B} \wedge \bar{C})$ – СДНФ; $P \sim (\bar{A} \vee \bar{B} \vee \bar{C}) \wedge (\bar{A} \vee B \vee \bar{C})$ – СКНФ.

Таким образом, формулы алгебры высказываний не являющиеся тождественно истинными или тождественно ложными, имеют эквивалентные СДНФ и СКНФ. Поэтому дальнейшее изучение высказываний можно ограничить изучением только СДНФ и СКНФ, которые имеют сравнительно простое строение. И обычно математики, имеющие дело с формулами алгебры высказываний, предпочитают рассматривать лишь СДНФ и СКНФ. Однако в практических задачах, связанных, например, с построением релейно-контактных схем или с конструированием различного рода вычислительных устройств, СДНФ и СКНФ оказываются слишком громоздкими и потому неудобными. В таких задачах всегда встает вопрос о сокращении числа букв и логических знаков, входящих в данную формулу. Подобное сокращение можно осуществить с помощью построения сокращенных таблиц истинности. Рассмотрим этот метод на следующем примере:

Пример 15. Пусть $P = (A \to ((B \vee C) \to (C \to \bar{A})))$, эту формулу можно рассматривать как формулу вида $(A \to Q)$, где $Q = ((B \vee C) \to (C \to \bar{A}))$.
Если $A = Л$, то независимо от значений формулы Q: $P = И$.
Если $A = И$, то значения P зависят от значений Q, причем $P \sim Q$. В свою очередь формула Q при $A = И$ принимает вид $((B \vee C) \to (C \to Л))$. Легко проверить, что скобка $(C \to Л)$ эквивалентна $\bar{C}$. Поэтому $Q \sim ((B \vee C) \to \bar{C})$.

Придавая C значения $И$ и $Л$, получим / независимо от B / соответствующие значения: $Q = Л$, $P = Л$ и $Q = И$, $P = И$. Таким образом, для вычисления всех значений формулы P оказалось достаточно рассмотреть лишь некоторые значения букв A и C. Запишем наши рассуждения в виде следующей сокращенной таблицы истинности:

A	B	C	$(A \to ((B \vee C) \to (C \to \bar{A})))$
Л	–	–	И
И	–	И	Л
И	–	Л	И

В этой таблице только три неполные строки истинностных значений вместо восьми строк, которые должна содержать полная таблица / см. пример 14/. Теперь по сокращенной таблице строим сокращенные конъюнктивную и дизъюнктивную нормальные формы, аналогично тому, как строились СКНФ и СДНФ. Первой и третьей строкам, в которых $P = \text{И}$, сопоставим элементарные конъюнкции $\bar{A}$, $(A \wedge \bar{C})$, тогда $P \sim (\bar{A} \vee (A \wedge \bar{C}))$ - дизъюнктивная нормальная форма. Второй строке, в которой $P = \text{Л}$, сопоставим следующую элементарную дизъюнкцию $(\bar{A} \vee \bar{C})$, тогда $P \sim (\bar{A} \vee \bar{C})$ конъюнктивная нормальная форма. Полученные формулы сравните с примерами 11 и 14.

Таким образом, правило построения сокращенной таблицы истинности заключается в следующем: мы приписываем значения И или Л одной единственной букве, и, исходя из этого, производим простейшие упрощения искомой формулы; затем приписываем значения другой какой-нибудь букве, и так до тех пор, пока не вычислим все значения формулы. Отличие от построения полных таблиц истинности заключается в том, что в данном методе не нужно приписывать значения всем буквам. Отметим, что если букве или формуле приписано некоторое значение / И или Л /, то упрощения формул основываются на следующих эквивалентностях:

$$(\text{И} \wedge A) \sim A, \quad (\text{Л} \wedge A) \sim \text{Л}, \quad (A \wedge \text{И}) \sim A, \quad (A \wedge \text{Л}) \sim \text{Л},$$
$$(\text{И} \vee A) \sim \text{И}, \quad (\text{Л} \vee A) \sim A, \quad (A \vee \text{И}) \sim \text{И}, \quad (A \vee \text{Л}) \sim A,$$
$$(\text{И} \rightarrow A) \sim A, \quad (\text{Л} \rightarrow A) \sim \text{И}, \quad (A \rightarrow \text{И}) \sim \text{И}, \quad (A \rightarrow \text{Л}) \sim \bar{A},$$
$$(\bar{\text{И}}) \sim \text{Л}, \quad \bar{\text{Л}} \sim \text{И}, \quad \bar{\bar{A}} \sim A.$$

Кроме того, рекомендуется выбирать в качестве буквы, которой приписываются значения И или Л, ту букву, которая чаще встречается в рассматриваемой формуле. Например, в качестве упражнения мы предлагаем читателю построить сокращенные таблицы истинности следующих формул:

$$(\bar{A} \vee \overline{(B \rightarrow A)}); \quad (((A \rightarrow B) \wedge C) \rightarrow A);$$
$$(\bar{C} \rightarrow ((C \rightarrow (B \vee \bar{A})) \vee A)).$$

Раздел 2. Исчисление высказываний.

Если некоторое математическое рассуждение описано подходящей формулой алгебры высказываний, то рассматривая таблицу истинности этой формулы, мы можем проверить правильность данного рассуждения. Однако в математике часто рассуждения представляют собой последовательности высказываний, каждое из которых является логическим следствием предыдущих высказываний этой последовательности. Такие рассуждения называются доказательствами или выводами. Для анализа методов построения математических доказательств оказывается более удобным формальный подход, основные положения которого были описаны нами в предыдущем разделе. Поэтому в этом разделе для дальнейшего изучения высказываний мы вводим специальную формальную систему, которая называется исчислением высказываний (сокращенно: ИВ). При этом мы используем формальный язык алгебры высказываний, но отказываемся от рассмотрения истинностных значений формул. Вместо таблиц истинности вводятся аксиомы и правила вывода.

В исчислении высказываний логические символы $\neg, \wedge, \vee, \rightarrow$ мы по-прежнему будем называть отрицанием, конъюнкцией, дизъюнкцией, импликацией, но мы не должны употреблять свойства этих символов, доказанные нами в алгебре высказываний. В ней эти свойства доказывались с помощью истинностных значений, которые не рассматриваются в ИВ. Все свойства этих символов в ИВ доказываются, исходя из аксиом и правил вывода. Некоторые из этих свойств будут вновь передоказаны в ИВ, а также будут рассмотрены некоторые другие свойства.

В заключении мы показываем равносильность содержательного и формального подходов к изучению высказываний, а именно: показываем, что тождественно истинные формулы алгебры высказываний и доказуемые в ИВ формулы суть одни и те же.

1. Аксиомы, правила вывода и.в.

Формальным языком исчисления высказываний является язык алгебры высказываний. При этом простейшие высказывания рассматриваются как обычные высказывательные переменные.

ОПРЕДЕЛЕНИЕ 1. Аксиомами исчисления высказываний являются все формулы, имеющие один из следующих видов:

I. 1. $(A \to (B \to A))$

2. $((A \to B) \to ((A \to (B \to C)) \to (A \to C)))$

II. 1. $((A \wedge B) \to A)$

2. $((A \wedge B) \to B)$

3. $(A \to (B \to (A \wedge B)))$

III. 1. $(A \to (A \vee B))$

2. $(B \to (A \vee B))$

3. $((A \to C) \to ((B \to C) \to ((A \vee B) \to C)))$

IV. 1. $((A \to B) \to ((A \to \bar{B}) \to \bar{A}))$

2. $(\bar{A} \to A)$

Формулы I.1 – IV.2 называются схемами аксиом. Каждая схема аксиом определяет бесконечное число аксиом, а именно: при любом конкретном выборе формул, обозначенных буквами A, B, C получается одна из аксиом.

Пример 1. Пусть A, B, C высказывательные переменные, тогда следующие формулы суть аксиомы, полученные по схеме I.1:

$(A \to (A \to A))$, $(A \to (B \to A))$, $(B \to ((A \vee C) \to B))$,

$(\bar{A} \to ((A \wedge C) \to \bar{A}))$, $((A \to (\bar{C} \to \bar{A})) \to (C \to (A \to (\bar{C} \to \bar{A}))))$.

В дальнейшем для указания схемы, по которой получается рассматриваемая аксиома, мы будем использовать следующие сокращения: СА I.1, СА I.2, СА II.1, СА II.2, ..., СА IV.2.

<u>ОПРЕДЕЛЕНИЕ 2.</u> Исчисление высказываний содержит единственное правило вывода "<u>модус поненс</u>" или "правило отделения".

<u>Модус поненс</u> – это процедура перехода от двух формул вида A и $(A \to B)$ к формуле B.

Символически это правило записывается в виде:

$$\frac{A,\ (A \to B)}{B} \qquad (\text{МП})$$

<u>Пример 2.</u> а) Формула $(B \to A)$ получена с помощью МП из формул $A,\ (A \to (B \to A))$:

$$\frac{A,\ (A \to (B \to A))}{(B \to A)}$$

б) $\bar{A}$ получена по МП из формул $(A \to B),\ ((A \to B) \to \bar{A})$:

$$\frac{(A \to B),\ ((A \to B) \to \bar{A})}{\bar{A}}$$

<u>ОПРЕДЕЛЕНИЕ 3.</u> <u>Доказательством</u> или <u>выводом</u> в ИВ называется конечная последовательность формул $B_1, \ldots, B_k$, каждая из которых есть либо аксиома, либо получается по модус поненс из предыдущих формул этой последовательности. Формула A называется <u>доказуемой</u> в ИВ или <u>выводимой</u>, если существует конечный вывод $B_1, \ldots, B_k$, в котором последняя формула есть A : $B_k = A$.

Обозначение: „$\vdash A$" „A-доказуема в ИВ"

<u>Пример 3.</u> Построим вывод формулы $(A \to A)$, где A - произвольная формула ИВ.

1. $(A \to (A \to A))$ (Сх 1.1)
2. $(A \to (A \to A)) \to [(A \to ((A \to A) \to A)) \to (A \to A)]$ (Сх 1.2)
3. $[(A \to ((A \to A) \to A)) \to (A \to A)]$ (МП к 1,2)
4. $(A \to ((A \to A) \to A))$ (Сх 1.1)
5. $(A \to A)$ (МП к 3,4)

Данное нами определение выводимости полностью соответствует аксиоматическому методу. Однако для точной характеризации математических рассуждений необходимо ввести важное обобщение этого понятия. В математике часто для доказательства теорем [illegible] специальные допущения. Эти допущения фактически функционируют как аксиомы: мы ссылаемся на них, используем и в конечном итоге говорим, что из данных предположений вытекает искомое утверждение. В подобных рассуждениях участвует понятие "выводимости из гипотез".

Определение 4. Дана последовательность формул $A_1, \ldots, A_m$. Будем говорить, что формула A выводима из гипотез $A_1, \ldots, A_m$ в ИВ, если существует конечная последовательность формул $B_1, \ldots, B_k$, каждая из которых есть либо аксиома, либо одна из гипотез $A_1, \ldots, A_m$, либо получается по модус поненс из предыдущих формул этой последовательности, и $B_k = A$ (обозначение : $A_1, \ldots, A_m \vdash A$)

Пример 4. покажем, что $(A \to (B \to C)), \ (A \wedge B) \vdash C$

1.	$(A \wedge B)$	(гипотеза)
2.	$((A \wedge B) \to A)$	(СА П.1)
3.	A	(МП к2,1)
4.	$(A \to (B \to C))$	(гипотеза)
5	$(B \to C)$	(МП к 3,4)
6	$((A \wedge B) \to B)$	(СА П.2)
7.	B	(МП к 1,6)
8	C	(МП к 5,7)

Таким образом , нами дано строгое определение математического доказательства, и дальнейшая цель состоит в изучении различных схем доказательств и доказуемых формул. Для облегчения построения выводов схемы аксиом разбиты на группы, каждая из которых характеризует свойства определенного логического символа. Например, схемы аксиом 1.1,2 характеризуют символ „ $\to$ " и позволяют доказывать формулы, содержащие „ $\to$; аксиомы II.1-3 характеризуют „ $\wedge$ и позволяют выводить формулы, содержащие $\wedge$ и т.д. Более того, практика построения выводов показывает, что во многих случаях если некоторая формула содержит ,например, символ „ $\wedge$ и не содержит „ $\vee$, то для ее вывода аксиомы III.1-3 не нужны. Это обстоятельство проиллюстрировано в примере 5: формула ($A \to A$) содержит только символ „$\rightarrow$", поэтому для ее вывода потребовались лишь схемы 1.1,2 и правило МП. Мы рекомендуем читателю обратить внимание на это обстоятельство – оно поможет нам при построении выводов.

Замечание 1. Символ "$\vdash$" не входит в язык ИВ и используется нами в качестве вспомогательного символа для характеризации интересующих нас понятий. Однако встречается такое изложение курса математической логики, когда знак "$\vdash$" включается в язык исчисления. В подобных случаях вводится специальная система аксиом, включающих символ "$\vdash$"; выражения, содержащие этот символ, называются секвенциями, а само исчисление называют исчислением секвенций. В настоящем курсе подобные рассмотрения отсутствуют.

2. Выводимость из гипотез

В данном пункте рассматриваются основные свойства понятия выводимости. Начнем с простейших из них.

ТЕОРЕМА 1. $A_1, A_2, \dots, A_m \vdash A_i$, где $i = 1, 2, \dots, m$.

Утверждение этой теоремы очевидно, оно выражает естественный факт, что любая гипотеза является выводимой из самой себя.

ТЕОРЕМА 2. Если $A_1, \dots, A_m \vdash B$ и $B \vdash C$, то $A_1, \dots, A_m \vdash C$.

Доказательство: Пусть $A_1, \dots, A_m \vdash B$, $B \vdash C$ и $C_1, \dots, C_k$ вывод C из B. Тогда каждое вхождение B в $C_1, \dots, C_k$ заменим на соответствующий вывод B из $A_1, \dots, A_m$, – получим вывод формулы C из $A_1, \dots, A_m$. Теорема доказана.

Доказанная теорема описывает схему, которая часто встречается в логических рассуждениях. Например, ей соответствует следующее рассуждение: " Если будет хорошая погода, то мы пойдем в лес. Если мы пойдем в лес, то прекрасно проведем время. Следовательно, если будет хорошая погода, то мы прекрасно проведем время".

Данная схема рассуждений называется правилом силлогизма (ПС).

ТЕОРЕМА 3. Если $A_1, \dots, A_{m-1} \vdash (A_m \rightarrow B)$ то $A_1, \dots, A_{m-1}, A_m \vdash B$

Доказательство. Пусть $A_1, \dots, A_{m-1} \vdash (A_m \to B)$ $B_1, \dots, B_k$ – вывод формулы $(A_m \to B)$ из $A_1, \dots, A_{m-1}$. Дополним этот вывод до вывода формулы B из $A_1, \dots, A_{m-1}, A_m$. По определению вывода имеем: $B_k = (A_m \to B)$. Возьмем в качестве формул B_{k+1}, B_{k+2} формулы A_m, B соответственно. Последние являются гипотезой и результатом применения МП к $B_{k+1} = A_m$ и $B_k = (A_m \to B)$. Теорема доказана.

Как было отмечено выше (с.22), почти каждая математическая теорема имеет вид $(A \to B)$. При этом A называется <u>условием</u> теоремы, а B – её <u>заключением</u>. Из теоремы 3 следует, что если некоторая теорема вида $(A \to B)$ доказана, то из условия этой теоремы A всегда выводимо её заключение B. Аналогичное утверждение было рассмотрено нами и в алгебре высказываний (теорема 4, с.22). Однако при доказательстве подобных теорем часто встречается противоположная ситуация. Доказательство теоремы $(A \to B)$ начинается с предположения; "пусть выполняется условие теоремы A", затем следуют рассуждения, в результате которых выводится заключение B. Такое доказательство представимо в виде следующей схемы:

" пусть A, тогда B " или символически: " $A \vdash B$ "

Ясно, что эта схема отличается от вида самой теоремы "$(A \to B)$". Тем не менее, доказательство теоремы на этом заканчивается. Например выше таким образом доказаны теоремы 2 и 3. В подобных случаях неявно используется специальный логический закон, называемый <u>правилом дедукции</u> (ПД). Покажем, что этот закон выполняется в исчислении высказываний.

<u>ТЕОРЕМА</u> 4 (<u>правило дедукции</u>). Если $A_1, \dots, A_{m-1}, A_m \vdash B$, то $A_1, \dots, A_{m-1} \vdash (A_m \to B)$

<u>Доказательство.</u> Пусть $A_1, \dots, A_{m-1}, A_m \vdash B$ и $B_1, \dots, B_k$ вывод формулы B из $A_1, \dots, A_m$. Отметим, что этот вывод может содержать формулу A_m. Для доказательства теоремы требуется построить вывод формулы $(A_m \to B)$, исходя только из гипотез $A_1, \dots, A_{m-1}$.

Рассмотрим последовательность формул

$(A_m \to B_1),\ (A_m \to B_2),\ \ldots,\ (A_m \to B_k)$ (*)

Последняя формула в (*) есть искомая $(A_m \to B)$, однако эта последовательность еще не является выводом. Но мы дополним (*) до искомого вывода. Для этого воспользуемся математической индукцией по номерам формул $B_1, B_2, \ldots, B_k$.

1). В формуле $(A_m \to B_1)$ формула B_1 является либо аксиомой, либо одной из гипотез $A_1, \ldots, A_{m-1}, A_m$. Рассмотрим эти случаи.

а). B_1 - аксиома. Тогда следующая последовательность формул образует доказательство формулы $(A_m \to B_1)$:

1. B_1 (аксиома)
2. $(B_1 \to (A_m \to B_1))$ (СА 1.1)
3. $(A_m \to B_1)$ (МП к 1,2)

б). B_1 - одна из гипотез $A_1, \ldots, A_{m-1}$. Тогда вывод $(A_m \to B_1)$ следующий:

1. B_1 (гипотеза)
2. $(B_1 \to (A_m \to B_1))$ (СА 1,1)
3. $(A_m \to B_1)$ (МП к 1,2)

в). $B_1 = A_m$. Тогда $(A_m \to B_1)$ имеет вид $(A_m \to A_m)$, доказательство последней формулы было рассмотрено в примере 5.

2). Предположим, что для всех $i < l$ формулы $(A_m \to B_i)$ выводимы из $A_1, \ldots, A_{m-1}$. Рассмотрим $(A_m \to B_l)$. В этой формуле B_l является либо аксиомой, либо одной из гипотез, либо получается по МП из некоторых предыдущих формул B_i, B_j $(i, j < l)$. Первые из этих случаев рассматриваются так же, как в пункте 1). Рассмотрим последний случай: пусть B_l получается по МП из B_i, B_j $(i, j < l)$. Тогда по определению МП имеем: $B_i = (B_j \to B_l)$.

Согласно предположению формулы $(A_m \to B_i)$ и $(A_m \to B_j)$ выводимы из $A_1, \ldots, A_{m-1}$. Тогда выводы этих формул мы дополним до вывода формулы $(A_m \to B_l)$ следующим образом:

1. $(A_m \to B_j)$ (выводима из $A_1, \ldots, A_{m-1}$)
2. $(A_m \to (B_j \to B_l))$ (выводима из $A_1, \ldots, A_{m-1}$)

3. $((A_m \to B_j) \to ((A_m \to (B_j \to B_\ell)) \to (A_m \to B_\ell)))$ / СА 1.2 /

4. $((A_m \to (B_j \to B_\ell)) \to (A_m \to B_\ell))$ / МП к 1,3 /

5. $(A_m \to B_\ell)$ / МП к 2,4 /

Теорема доказана.

Пример 5. $(A \to (B \to C)) \vdash ((A \wedge B) \to C)$.

Для доказательства этого утверждения нужно применить правило дедукции к утверждению примера 4:

1. $(A \to (B \to C)),\ (A \wedge B) \vdash C$ / пример 4/
2. $(A \to (B \to C)) \vdash ((A \wedge B) \to C)$ / ПД /

Следствие 1. Если $A_1, A_2, \ldots, A_m \vdash B$, то $\vdash (A_1 \to (A_2 \to \ldots (A_m \to B)\ldots)$

Для доказательства нужно m раз применить правило дедукции.

В следующем пункте приводятся другие следствия теоремы 4.

3. Производные правила вывода.

В данном пункте мы доказываем некоторые вспомогательные правила вывода, облегчающие построение выводов в ИВ. Пусть A, B, C – произвольные формулы исчисления высказываний.

ТЕОРЕМА 5 / правило перестановки посылок/.

$$(A \to (B \to C)) \vdash (B \to (A \to C)) \qquad / \text{ППП} /$$

Доказательство. Сначала докажем следующее утверждение:

а/. $(A \to (B \to C)),\ B,\ A \vdash C$

1. A / гипотеза /
2. $(A \to (B \to C))$ / гипотеза /
3. $(B \to C)$ / МП к 1,3 /
4. B / гипотеза /
5. C / МП к 3,4 /

Теперь к доказанному утверждению а/ применим правило дедукции:

б/ $(A \to (B \to C)),\ B \vdash (A \to C)$ / ПД /

в/ $(A \to (B \to C)) \vdash (B \to (A \to C))$ / ПД /

Теорема доказана.

ТЕОРЕМА 6/правило соединения посылок/.

$$(A \to (B \to C)) \vdash ((A \wedge B) \to C)$$ / ПС[illegible]

Доказательство приведено в примере 5.

ТЕОРЕМА 7/правило разъединения посылок/.

$$((A \wedge B) \to C) \vdash (A \to (B \to C))$$ / [illegible]

Доказательство. Сначала докажем утверждение:

а/. $((A \wedge B) \to C,\ A,\ B \vdash C$

1. A /гип[illegible]/
2. B /гипо[illegible]/
3. $(A \to (B \to (A \wedge B)))$ / СА [illegible] /
4. $(B \to (A \wedge B))$ / МП к [illegible] /
5. $(A \wedge B)$ /МП к [illegible] /
6. $((A \wedge B) \to C)$ /гипо[illegible]/
7. C / МП к [illegible] /

Теперь, применяя дважды правило дедукции к а/, получим ис[illegible] утверждение.

Объединим все вспомогательные правила вывода в две группы правила введения и правила удаления.

ТЕОРЕМА 8 /правила введения/. Для любых формул

а/. $A, B \vdash (A \wedge B)$ / ПВ $\wedge$ /

б/. $A \vdash (A \vee B)$ / ПВ $\vee$ /

в/. $B \vdash (A \vee B)$ / ПВ $\vee$ /

г/. если $A \vdash B$, то $\vdash (A \to B)$ / ПВ $\to$ /

д/. $A \vdash \bar{\bar{A}}$ / ПВ $=$ /

е/. если $A \vdash B$ и $A \vdash \bar{B}$, то $\vdash \bar{A}$ / ПВ $^{-}$ /

Доказательство. Правила а/ – в/ легко следует из схем аксиом [illegible] П.1,2 и из теоремы 3; правило г/ есть П[illegible]; рассмотрим д/.е/.

д/. 1. A /гипотеза/

2. $(A \to (\bar{A} \to A))$ / СА 1.1 /

3. $(\bar{A} \to A)$ / МП к 1,2/

4. $((\bar{A}\to A)\to((\bar{A}\to\bar{\bar{A}})\to\bar{\bar{A}}))$ (Сх IV.1)

5. $((\bar{A}\to\bar{\bar{A}})\to\bar{\bar{A}})$ (МП к 3,4)

6. $(\bar{A}\to\bar{\bar{A}})$ (пример 3)

7. $\bar{\bar{A}}$ (МП к 5,6)

е). 1. $A\vdash B$ (условие теоремы)

2. $\vdash(A\to B)$ (ПД)

3. $\vdash((A\to B)\to((A\to\bar{B})\to\bar{A}))$ (Сх IV.1)

4. $\vdash((A\to\bar{B})\to\bar{A})$ (МП к 2,3)

5. $A\vdash\bar{B}$ (условие теоремы)

6. $\vdash(A\to\bar{B})$ (ПД)

7. $\vdash\bar{A}$ (МП к 4,6)

Правило введения отрицания е) представляет собой схему <u>доказательства от противного</u> или, иногда говорят: <u>правило сведения к противоречию.</u> Действительно, если необходимо доказать утверждение вида $\bar{A}$, мы предполагаем, что выполняется противоположное утверждение A и стараемся вывести противоречие: $(B\wedge\bar{B})$. Если $(B\wedge\bar{B})$ получено, то по правилу введения $\bar{\ }$ доказуемо искомое утверждение $\bar{A}$.

<u>ТЕОРЕМА 9.</u> (<u>правила удаления</u>).

а) $(A\wedge B)\vdash A$ (ПУ $\wedge$)

б) $(A\wedge B)\vdash B$ (ПУ $\wedge$)

в) $\bar{\bar{A}}\vdash A$ (ПУ $\bar{\bar{\ }}$)

г) если $A\vdash C$ и $B\vdash C$, то $(A\vee B)\vdash C$ (ПУ $\vee$)

д) если $\vdash A$ и $\vdash(A\to B)$, то $\vdash B$ (ПУ $\to$)

е) $A,\bar{A}\vdash B$

Доказательство. Правила а)–г) легко следуют из схем II.1,2,III.3,IV.2 и из теоремы 8; правило д) есть модус поненс.

Правило г) утверждает, что для доказательства суждения вида $(A\vee B)\vdash C$ достаточно доказать два суждения " $A\vdash C$ " и " $B\vdash C$ ", которые уже не содержат знака " $\vee$ ", т.е. действительно произошло удаление $\vee$. Это правило обосновывает такие доказательства, в которых приходится рассматривать несколько случаев. Например, в доказательстве признака делимости на 3 рассматриваются два случая: A — "данное число оканчивается на 0" и B - "данное число оканчивается на 5". В каждом из этих случаев "данное число делится на 5" = C, т.е. $A \vdash C$ и $B \vdash C$. Отсюда по правилу удаления $\vee : (A \vee B) \vdash C$.

При изложении производных правил вывода мы указываем минимальное число гипотез. Однако эти правила допускают обобщения на случаи, когда исходные множества гипотез более широкие. Например, правило введения отрицания и правило удаления дизъюнкции обобщается следующим образом:

Если $A_1, \ldots, A_m, B \vdash C$ и $A_1, \ldots, A_m, B \vdash \bar{C}$, то $A_1, \ldots, A_m \vdash \bar{B}$

Если $A_1, \ldots, A_m, B \vdash D$ и $A_1, \ldots, A_m, C \vdash D$, то $A_1, \ldots, A_m, (B \vee C) \vdash D$.

Пример 6. $A, \bar{A} \vdash B$

1. $A, \bar{A}, \bar{B} \vdash A$ (теорема 1)
2. $A, \bar{A}, \bar{B} \vdash \bar{A}$ (теорема 1)
3. $A, \bar{A} \vdash \bar{\bar{B}}$ (ПВ $^{-}$)
4. $\bar{\bar{B}} \vdash B$ (ПУ $^{=}$)
5. $A, \bar{A} \vdash B$ (ПС)

ТЕОРЕМА 10 (правило контрапозиции).

$A \vdash B$ тогда и только тогда, когда $\bar{B} \vdash \bar{A}$ (ПК)

Доказательство. а). Пусть $A \vdash B$, покажем, что $\bar{B} \vdash \bar{A}$

1. $\vdash \bar{B}$ (гипотеза)
2. $\vdash (\bar{B} \to (A \to \bar{B}))$ (СА 1.1)
3. $\vdash (A \to \bar{B})$ (МП к 1,2)
4. $A \vdash B$ (условие теоремы)
5. $\vdash (A \to B)$ (ПД)
6. $\vdash ((A \to B) \to ((A \to \bar{B}) \to \bar{A}))$ (СА 1У.1)
7. $\vdash ((A \to \bar{B}) \to \bar{A})$ (МП к 5,6)
8. $\vdash \bar{A}$ (МП к 3,7)

б). Пусть $\bar{B} \vdash \bar{A}$, тогда покажем, что $A \vdash B$. В силу первой части данного утверждения из $\bar{B} \vdash \bar{A}$ следует: $\bar{\bar{A}} \vdash \bar{\bar{B}}$. По правилу введения $^{=}$: $A \vdash \bar{\bar{A}}$ и по правилу удаления $^{=}$: $\bar{\bar{B}} \vdash B$. Применив к соотношениям $A \vdash \bar{\bar{A}}$, $\bar{\bar{A}} \vdash \bar{\bar{B}}$, $\bar{\bar{B}} \vdash B$ правило силлогизма, получим $A \vdash B$, что и требовалось доказать.

Правило контрапозиции дает исключительно удобный метод доказательства теорем. Оказывается, что теорема вида $(A \to B)$ равносильна теореме вида $(\bar{B} \to \bar{A})$ и потому вместо $A \vdash B$ можно доказывать $\bar{B} \vdash \bar{A}$. Например, утверждение "если функция дифференцируема, то она непрерывна" раносильно утверждению "если функция разрывна, то она недифференцируема".

<u>ТЕОРЕМА</u> 11. Пусть формула P содержит переменную A, и формула $S_B^A(P)$ получается из P в результате замены всех вхождений A на формулу B. Тогда если $\vdash P$, то $\vdash S_B^A(P)$.

Доказательство. Пусть $\vdash P$ и $Q_1, \ldots, Q_n$ - её вывод. Тогда $Q_n = P$ и каждая $Q_1, \ldots, Q_n$ либо аксиома, либо получается по МП из предыдущих формул. Рассмотрим формулы

$$S_B^A(Q_1), \ldots, S_B^A(Q_n),$$

получаемые из $Q_1, \ldots, Q_n$ заменой A на B. Они образуют вывод формулы $S_B^A(P)$. Действительно, если Q_i является аксиомой и получена подстановкой из некоторой схемы аксиом, то $S_B^A(Q_i)$ может быть получена из той же схемы подходящей подстановкой, т.е. $S_B^A(Q_i)$ аксиома. В частности, $S_B^A(Q_1)$ аксиома. Далее, применим математическую индукцию. Предположим, что все $S_B^A(Q_i)$ $(i<l)$ доказуемы в ИВ и рассмотрим $S_B^A(Q_l)$. Пусть Q_l получается по МП из предыдущих формул Q_i и $Q_j = (Q_i \to Q_l)$. Очевидно, что в этом случае $S_B^A(Q_j)$ имеет вид: $(S_B^A(Q_i) \to S_B^A(Q_l))$. Тогда $S_B^A(Q_l)$ получается по МП из $S_B^A(Q_i)$, $(S_B^A(Q_i) \to S_B^A(Q_l))$. Теорема доказана.

В заключение пункта мы рассмотрим несколько вспомогательных утверждений, иллюстрирующих применение доказанных правил.

<u>ЛЕММА</u> 1. В ИВ выполняются следующие соотношения:

а) $(\bar{A} \vee \bar{B}) \vdash \overline{(A \wedge B)}$

б) $(\bar{A} \wedge \bar{B}) \vdash \overline{(A \vee B)}$

в) $(\bar{A} \vee B) \vdash (A \to B)$

г) $(A \wedge \bar{B}) \vdash \overline{(A \to B)}$

д) $\vdash (A \vee \bar{A})$

$\vdash \overline{(A \wedge \bar{A})}$

Доказательство. а/. 1. $(A \wedge B) \vdash A$ / ПУ $\wedge$ /

2. $\overline{A} \vdash \overline{(A \wedge B)}$ / ПК /

3–4. $\overline{B} \vdash \overline{(A \wedge B)}$ / аналогично 1–2 /

5. $(\overline{A} \vee \overline{B}) \vdash \overline{(A \wedge B)}$ / ПУ $\vee$ /

б/. 1. $(\overline{A} \wedge \overline{B}) \vdash \overline{A}$ / ПУ $\wedge$ /

2. $\overline{\overline{A}} \vdash \overline{(\overline{A} \wedge \overline{B})}$ / ПК /

3. $A \vdash \overline{\overline{A}}$ / ПВ $\overline{}$ /

4. $A \vdash \overline{(\overline{A} \wedge \overline{B})}$ / ПС /

5–8. $B \vdash \overline{(\overline{A} \wedge \overline{B})}$ / аналогично 1–4 /

9. $(A \vee B) \vdash \overline{(\overline{A} \wedge \overline{B})}$ / ПУ $\vee$ /

10. $\overline{\overline{(\overline{A} \wedge \overline{B})}} \vdash \overline{(A \vee B)}$ / ПК /

11. $(\overline{A} \wedge \overline{B}) \vdash \overline{\overline{(\overline{A} \wedge \overline{B})}}$ / ПВ $\overline{}$ /

12. $(\overline{A} \wedge \overline{B}) \vdash \overline{(A \vee B)}$ / ПС /

в/. 1. $\vdash (B \to (A \to B))$ / СА 1 /

2. $B \vdash (A \to B)$ / ПУ $\to$ /

3. $\overline{A}, A \vdash B$ / схема 5 /

4. $\overline{A} \vdash (A \to B)$ / ПВ $\to$ /

5. $(\overline{A} \vee B) \vdash (A \to B)$ / ПУ $\vee$ /

г/. 1. $(A \wedge \overline{B}), (A \to B) \vdash \overline{B}$ / ПУ $\wedge$ /

2. $(A \wedge \overline{B}), (A \to B) \vdash A$ / ПУ $\wedge$ /

3. $(A \wedge \overline{B}), (A \to B) \vdash (A \to B)$ / теорема 1 /

4. $(A \wedge \overline{B}), (A \to B) \vdash B$ / МС к 2, 3 /

5. $(A \wedge \overline{B}) \vdash \overline{(A \to B)}$ / ПВ $\overline{}$ /

д/. 1. $A \vdash (A \vee \overline{A})$ / ПВ $\vee$ /

2. $\overline{(A \vee \overline{A})} \vdash \overline{A}$ / ПК /

3–4. $\overline{(A \vee \overline{A})} \vdash \overline{\overline{A}}$ / аналогично 1–2 /

5. $\vdash \overline{\overline{(A \vee \overline{A})}}$ / ПВ $\overline{}$ /

6. $\vdash (A \vee \overline{A})$ / ПУ $\overline{}$ /

е/. 1. $(A \wedge \overline{A}) \vdash A$ / ПУ $\wedge$ /

2. $(A \wedge \overline{A}) \vdash \overline{A}$ / ПУ $\wedge$ /

3. $\vdash \overline{(A \wedge \overline{A})}$ / ПВ $\overline{}$ /

Лемма доказана.

§ 4. Связь между алгеброй высказываний и исчислением высказываний.

Формулы исчисления высказываний можно рассматривать как формулы алгебры высказываний. При этом если высказывательным переменным в ИВ присваивать значения И и Л , а символы ($\neg, \wedge, \vee, \rightarrow$) считать символами соответствующих логических операций, то формулы ИВ будут принимать истинностные значения. Тогда можно будет говорить о тождественной истинности формул исчисления высказываний. Как было условлено в алгебре высказываний, тождественно истинные формулы выражают схемы правильных рассуждений в математике. В исчислении высказываний эту роль выполняют доказуемые формулы, поэтому особый интерес представляет сравнение тождественно истинных формул и доказуемых формул. В данном пункте мы покажем, что это одни и те же формулы.

ТЕОРЕМА 12. Всякая формула, доказуемая в ИВ, является тождественно истинной в алгебре высказываний.

Доказательство. Каждая доказуемая формула получается из аксиом с помощью правила модус поненс. По теоремам 4 и 5 раздела 1 каждая аксиома ИВ является тождественно истинной, и по той же теореме 4 применение модус поненс к тождественно истинным формулам дает вновь тождественно истинную формулу. Поэтому любая формула, получаемая из аксиом с помощью модус поненс, будет тождественно истинной. Теорема доказана.

Таким образом, мы установили, что формулы, доказуемые в ИВ , не выводят нас за пределы тождественно истинных формул . Этот факт свидетельствует о надежности рассмотренного формального подхода к изучению высказываний, т.е. о том, что выводы исчисления высказываний находятся в строгом соответствии с выводами алгебры высказываний. Рассмотрим обратную проблему: верно ли, что каждая тождественно истинная формула доказуема в ИВ? достаточен ли набор аксиом и правил вывода в ИВ для обоснования любых выводов алгебры высказываний?является ли ИВ достаточно полным? Эта проблема называется проблемой полноты исчисления высказываний. Ниже доказывается, что она решается положительно.

ТЕОРЕМА 13. Всякая тождественно истинная формула алгебры высказываний доказуема в исчислении высказываний.

Доказательству теоремы мы предпошлем некоторые вспомогательные понятия и утверждения.

Для произвольной формулы A определим следующие формулы:

$$A^{И} = A \quad , \quad A^{Л} = \bar{A} .$$

Далее, пусть $P(A_1, \dots, A_n)$ - формула ИВ и $\langle I_1, \dots, I_n \rangle$ - набор истинностных значений /т.е. каждое I_i равно $И$ или $Л$ /. Через I_P обозначим значение $P(I_1, \dots, I_n)$.

Ниже мы будем рассматривать формулы $A_1^{I_1}, \dots, A_n^{I_n}, P^{I_P}(A_1, \dots, A_n)$, поэтому приведем несколько примеров:

а/. Пусть $P(A_1, A_2) = (A_1 \wedge A_2)$ и $\langle I_1, I_2 \rangle = \langle Л, И \rangle$. Тогда $A_1^{I_1} = \bar{A}_1$, $A_2^{I_2} = A_2$, $I_P = (Л \wedge И) = Л$, $P^{I_P}(A_1, A_2) = (A_1 \wedge A_2)^{Л} = \overline{(A_1 \wedge A_2)}$,

б/. Пусть $P(A_1, A_2, A_3) = ((A_1 \vee A_2) \to A_3)$ и $\langle I_1, I_2, I_3 \rangle = \langle И, Л, Л \rangle$. тогда $A_1^{I_1} = A_1$, $A_2^{I_2} = \bar{A}_2$, $A_3^{I_3} = \bar{A}_3$, $I_P = Л$, $P^{I_P}(A_1, A_2, A_3) = \overline{((A_1 \vee A_2) \to A_3)}$.

в/. Пусть $P(A_1) = \bar{A}_1$ и $\langle I_1 \rangle = \langle Л \rangle$, тогда $A_1^{I_1} = \bar{A}_1$, $I_P = И$, $P^{I_P}(A_1) = \bar{A}_1$

ЛЕММА 2. Для любой формулы $P(A_1, \dots, A_n)$ и любого набора $\langle I_1, \dots, I_n \rangle$ выполняется соотношение:

$$A_1^{I_1}, \dots, A_n^{I_n} \vdash P^{I_P}(A_1, \dots, A_n) \qquad (1)$$

Доказательство / индукцией по длине формулы /. 1/. Пусть формула $P(A_1, \dots, A_n)$ не содержит логических символов. Тогда P совпадает с высказывательной переменной: $P = A_1$. Тогда в качестве набора истинностных значений нужно рассматривать $\langle I_1 \rangle$. В этом случае $I_P = P(I_1) = I_1$ и (1) примет вид $A_1^{I_1} \vdash A_1^{I_1}$. Это утверждение выполняется в силу теоремы 1 из 2.

2/. Пусть для формул $P(A_1, \dots, A_n)$ и $Q(A_1, \dots, A_n)$ утверждение леммы выполняется, т.е. для любого набора истинностных значений $\langle I_1, \dots, I_n \rangle$ выполняются соотношения:

$$A_1^{I_1}, \ldots ; A_n^{I_n} \vdash P^{I_P}(A_1, \ldots, A_n), \qquad (2)$$

$$A_1^{I_1}, \ldots, A_n^{I_n} \vdash Q^{I_q}(A_1, \ldots, A_n), \qquad (3)$$

где $I_p = P(I_1, \ldots, I_n)$, $I_q = Q(I_1, \ldots, I_n)$.

Пусть формула $R(A_1, \ldots, A_n)$ получается из $P(A_1, \ldots, A_n), Q(A_1, \ldots, A_n)$ с помощью одного из логических символов $^{-}$, $\vee$, $\wedge$.

а/. $R(A_1, \ldots, A_n) = \bar{P}(A_1, \ldots, A_n)$, тогда $I_2 = \bar{P}(I_1, \ldots, I_n) = \bar{I}_p$, и утверждение леммы примет вид:

$$A_1^{I_1}, \ldots, A_n^{I_n} \vdash \bar{P}^{\bar{I}_p}(A_1, \ldots, A_n) \qquad (4)$$

Если $I_p = \text{И}$, то $P^{I_p} = P$ и $\bar{P}^{\bar{I}_p} = \bar{\bar{P}}$. По правилу введения $=$: $P \vdash \bar{\bar{P}}$. Отсюда и из (2) по правилу силлогизма следует (4).

Если $I_p = \text{Л}$, то $P^{I_p} = \bar{P}$ и $\bar{P}^{\bar{I}_p} = \bar{P}$. По теореме 1 из 2: $\bar{P} \vdash \bar{P}$. Отсюда и из (2) по правилу силлогизма следует (4).

б/. $R = (P \vee Q)$. Тогда $I_2 = (I_p \vee I_q)$ и утверждение леммы примет вид:

$$A_1^{I_1}, \ldots, A_n^{I_n} \vdash (P \vee Q)^{I_p \vee I_q}. \qquad (5)$$

Если $I_p = \text{И}$, то $(I_p \vee I_q) = \text{И}$, $P^{I_p} = P$, $(P \vee Q)^{I_p \vee I_q} = (P \vee Q)$. По правилу введения $\vee$: $P \vdash (P \vee Q)$. Отсюда и из (2) следует (5).

Если $I_q = \text{И}$, то $(I_p \vee I_q) = \text{И}$, $Q^{I_q} = Q$, $(P \vee Q)^{I_p \vee I_q} = (P \vee Q)$. По правилу введения $\vee$: $Q \vdash (P \vee Q)$. Отсюда и из (3) следует (5).

Если $I_p = \text{Л}$ и $I_q = \text{Л}$, то $(I_p \vee I_q) = \text{Л}$, $P^{I_p} = \bar{P}$, $Q^{I_q} = \bar{Q}$, $(P \vee Q)^{I_p \vee I_q} = \overline{(P \vee Q)}$. По правилу введения $\wedge$: $\bar{P}, \bar{Q} \vdash (\bar{P} \wedge \bar{Q})$. Из леммы 1б/ имеем: $(\bar{P} \wedge \bar{Q}) \vdash \overline{(P \vee Q)}$. Отсюда и из (2), (3) по правилу силлогизма получаем (5).

в/. Пусть $R(P \wedge Q)$, тогда $I_2 = (I_p \wedge I_q)$ и утверждение леммы примет вид:

$$A_1^{I_1}, \ldots, A_n^{I_n} \vdash (P \wedge Q)^{I_p \wedge I_q}. \qquad (6)$$

Если $I_p = \text{И}$ и $I_q = \text{И}$, то $P^{I_p} = P$, $Q^{I_q} = Q$, $(P \wedge Q)^{I_p \wedge I_q} = (P \wedge Q)$. По правилу введения $\wedge$: $P, Q \vdash (P \wedge Q)$. Отсюда и из (2), (3) следует (6).

Если $I_p = \text{Л}$, то $P^{I_p} = \bar{P}$, $(P \wedge Q)^{I_p \wedge I_q} = \overline{(P \wedge Q)}$. По правилу введения $\vee$: $\bar{P} \vdash (\bar{P} \vee \bar{Q})$. Из леммы 1а/: $(\bar{P} \vee \bar{Q}) \vdash \overline{(P \wedge Q)}$. Из последних двух соотношений и из (2) следует (6).

Если $I_q = Л$, то $Q^{I_q} = \bar{Q}, (P \wedge Q)^{I_p \wedge I_q} = (\overline{P \wedge Q})$. По правилу введения $\vee$: $\bar{Q} \vdash (\bar{P} \vee \bar{Q})$. Из леммы 1е/: $(\bar{P} \vee \bar{Q}) \vdash (\overline{P \wedge Q})$. Тогда из этих двух утверждений и из (3) следует (6).

г/. Пусть $R = (P \to Q)$, тогда $I_R = (I_p \to I_q)$, и утверждение леммы примет вид:

$$A_1^{I_1}, \ldots, A_n^{I_n} \vdash (P \to Q)^{I_p \to I_q} \qquad (7)$$

Если $I_p = И$ и $I_q = Л$, то $P^{I_p} = P$, $Q^{I_q} = \bar{Q}$, $(P \to Q)^{I_p \to I_q} = (\overline{P \to Q})$. По правилу введения $\wedge$: $P, \bar{Q} \vdash (P \wedge \bar{Q})$. Из леммы 1г/: $(P \wedge \bar{Q}) \vdash (\overline{P \to Q})$. Из этих двух соотношений и из (2), (3) следует (7).

Если $I_p = Л$, то $P^{I_p} = \bar{P}$, $(P \to Q)^{I_p \to I_q} = (P \to Q)$. По правилу введения $\vee$: $\bar{P} \vdash (\bar{P} \vee Q)$. Из леммы 1в/: $(\bar{P} \vee Q) \vdash (P \to Q)$. Из этих двух соотношений и из (2) следует (7).

Если $I_q = И$, то $Q^{I_q} = Q$, $(P \to Q)^{I_p \to I_q} = (P \to Q)$. По правилу введения $\vee$: $Q \vdash (\bar{P} \vee Q)$. Из леммы 1в/: $(\bar{P} \vee Q) \vdash (P \to Q)$. Из этих двух соотношений и из (3) следует (7).

Нами рассмотрены все возможные случаи, и лемма доказана.

<u>Приступим к доказательству теоремы 13.</u> Пусть P тождественно истинная формула и зависит от переменных $A_1, \ldots, A_n$:

$$P = P(A_1, \ldots, A_n)$$

Тогда для любого набора $\langle I_1, \ldots, I_n \rangle$: $I_p = P(I_1, \ldots, I_n) = И$. Отсюда $P^{I_p}(A_1, \ldots, A_n) = P(A_1, \ldots, A_n)$ и по лемме 2 имеем:

$$A_1^{I_1}, \ldots, A_n^{I_n} \vdash P(A_1, \ldots, A_n) \qquad (8)$$

Возьмем два набора истинностных значений следующего вида: $\langle I_1, \ldots, I_{n-1}, И \rangle$ и $\langle I_1, \ldots, I_{n-1}, Л \rangle$. В силу (8) имеем:

$$A_1^{I_1}, \ldots, A_{n-1}^{I_{n-1}}, A_n \vdash P(A_1, \ldots, A_n),$$

$$A_1^{I_1}, \ldots, A_{n-1}^{I_{n-1}}, \bar{A}_n \vdash P(A_1, \ldots, A_n)$$

Отсюда по правилу удаления $\vee$ получаем:

$$A_1^{I_1}, \ldots, A_{n-1}^{I_{n-1}}, (A_n \vee \bar{A}_n) \vdash P(A_1, \ldots, A_n).$$

По лемме 1д/ $(A_n \vee \bar{A}_n)$ доказуема в ИВ, следовательно:

$$A_1^{I_1}, \ldots, A_{n-1}^{I_{n-1}} \vdash P(A_1, \ldots, A_n) \qquad (9)$$

Так как значения $I_1, \ldots, I_{n-1}$ выбирались произвольным образом, то соотношение (9) выполняется для любого набора $\langle I_1, \ldots, I_{n-1} \rangle$. Теперь аналогичными рассуждениями из (9) можно получить:

$$A_1^{I_1}, \ldots, A_{n-2}^{I_{n-2}} \vdash P(A_1, \ldots, A_n)$$

Продолжая подобные рассуждения, мы через $(n-2)$ шага получим искомое соотношение $\vdash P(A_1, \ldots, A_n)$. Теорема доказана.

Теоремы 12 и 13 дают хороший метод / алгоритм, см. с. 14 /для определения доказуемости формул исчисления высказываний. Чтобы проверить "доказуема ли данная формула P ?", достаточно проверить: "является ли P тождественно истинной формулой?" А последнее проверяется /эффективно/ с помощью таблицы истинности.

Пример 7. Доказуема ли формула $(A \to \bar{B}) \to (B \to \bar{A})$?

Чтобы проверить это, составим таблицу истинности:

A	B	$(A \to \bar{B}) \to (B \to \bar{A})$
И	И	И
И	Л	И
Л	И	И
Л	Л	И

Эта формула является тождественно истинной и по теореме 13 является доказуемой в ИВ.

Таким образом, отношение "быть доказуемой формулой в ИВ" является разрешимым /см. с. 13/.

Раздел 3. Логика предикатов

Алгебра высказываний и исчисление высказываний каждое утверждение анализирует с точки зрения логических связей, существующих между составляющими это утверждение высказываниями, структура составляющих высказываний не исследуется. В этом отношении такое исследование является ограниченным и не позволяет анализировать широкий класс математических рассуждений. Например, из посылок

"всякое рациональное число есть действительное число" (A)

" 1/3 есть рациональное число" (B)

конечно можно сделать заключение:

" 1/3 есть действительное число " (C)

Но в алгебре высказываний это рассуждение представимо следующей формулой: $((A \wedge B) \to C)$ Очевидно, что истинность этой формулы не может быть обоснована в алгебре высказываний. Для анализа этого утверждения необходимо в каждом составляющем высказывании выделить объекты рассуждения (подлежащие) и то, что о них говорится (сказуемые). Поэтому в данной главе мы расширяем наше исследование и вводим новые понятия: предметные переменные, константы, предикаты и кванторы, которые позволят нам анализировать структуру широкого класса суждений. Как и в случае изучения высказываний в первую очередь мы рассмотрим содержательный подход к исследованию этих понятий.

1. Переменные, предикаты, кванторы.

Напомним некоторые теоретико-множественные понятия и обозначения. Пусть M – произвольное непустое множество. Отдельные его элементы будем обозначать первыми буквами латинского алфавита: $a, b, c, a_1, a_2, \dots, a_n, c_1, c_2, \dots$. Сами буквы назовем предметными константами, обозначаемые ими элементы из M назовем их значениями. Латинскими буквами $x, y, z, x_1, x_2, \dots, x_n$ будем обозначать переменные, принимающие значения из множества M, и будем называть их предметными переменными. Букву t возможно с индексами будем использовать для обозначения как предметных констант, так и предметных переменных. Запись $x \in M$ означает, что значения x входят в M.

n-ой декартовой степенью множества M называется множество всевозможных кортежей длины n, составленных из элементов M. Обозначение: $M^n = M \times M \times \ldots \times M$. Например, если R - множество действительных чисел, то $R^2 = R \times R$ есть множество декартовых координат $\langle x, y \rangle$ точек плоскости, $R^3 = R \times R \times R$ - есть множество декартовых координат (x, y, z) точек пространства.

Произвольное подмножество P множества M^n ($P \subseteq M^n$) называется n-местным отношением на M. Так, в предыдущих примерах отношения неравенства чисел $x \leq y$, $x < y$ являются подмножествами $M \times M$, арифметические соотношения $x + y = z$, $x \cdot y = z$ также определяют некоторые отношения на множестве $M \times M \times M$.

Далее, если P - n-местное отношение на M и $a_1, \ldots, a_n$ элементы из M, то слова "кортеж $\langle a_1, \ldots, a_n \rangle$ удовлетворяет отношению P" означают, что $\langle a_1, \ldots, a_n \rangle$ принадлежит множеству P: $\langle a_1, \ldots, a_n \rangle \in P$. Отсюда следует, что любой кортеж $\langle a_1, \ldots, a_n \rangle$ из M^n либо удовлетворяет P, либо нет. В математической логике с каждым отношением $P \subseteq M^n$ связывают истинностные значения. А именно, если кортеж $\langle a_1, \ldots, a_n \rangle$ удовлетворяет P, то говорят, что отношение P истинно на $\langle a_1, \ldots, a_n \rangle$ (обозначение: $P(a_1, \ldots, a_n) = И$), в противном случае P ложно на $\langle a_1, \ldots, a_n \rangle$ ($P(a_1, \ldots, a_n) = Л$). Тем самым, n-местное отношение рассматривается как высказывательная функция, которая каждому кортежу $\langle a_1, \ldots, a_n \rangle \in M^n$ сопоставляет значение И или Л. В этом случае n-местное отношение называют n-местным предикатом, определенным на M. Для обозначения предикатов будем использовать заглавные латинские буквы P, R, S, T с верхними и нижними индексами. Для указания местности предиката используются верхние индексы или выписываются переменные. Например, $P^n(x_1, \ldots, x_n)$,

$R^n(y_1,\ldots,y_n)$, $S^n_m(t_1,\ldots,t_n)$ n - местные предикаты.

В анализе суждения предикаты выполняют роль сказуемых, а роль подлежащего выполняют предметные переменные и константы, входящие в предикаты. Логические операции $\bar{\ }$, $\vee$, $\wedge$, $\rightarrow$ по-прежнему выполняют роль связок между высказываниями. Теперь высказывания могут содержать предметные переменные и константы, и потому мы вводим еще две логические операции - операции навешивания кванторов на предметные переменные.

Пусть формула $A(x)$ содержит предметную переменную x. Сопоставим $A(x)$ две формулы: $\forall x\, A(x)$ и $\exists x\, A(x)$

Символы $\forall$, $\exists$ называются соответственно квантором общности и квантором существования. Процедура перехода от формулы $A(x)$ к формулам $\forall x\, A(x)$ и $\exists x\, A(x)$ называется операцией навешивания кванторов $\forall$ и $\exists$ на переменную x.

Поясним, что означают кванторы содержательно. Для этого в качестве $A(x)$ возьмем одноместный предикат $P(x)$, определенный на множестве M. Для каждого значения x предикат $P(x)$ является истинным или ложным. И мы полагаем, что формулы $\forall x\, P(x)$ и $\exists x\, P(x)$ являются высказываниями, принимающими следующие истинностные значения:

$\forall x\, P(x) = И \longleftrightarrow$ для любого значения x из M: $P(x) = И$

$\exists x\, P(x) = И \longleftrightarrow$ существует такое значение x из M, что $P(x) = И$

В разговорном языке формула $\forall x\, A(x)$ читается как " для всех x $A(x)$" или "для любых x $A(x)$"; формула $\exists x\, A(x)$ читается "существует x $A(x)$" или "для некоторого x $A(x)$".

Пример 1. Пусть $D(x)$ обозначает предикат " x - действительное число" и $R(x)$ - " x рациональное число ". Очевидно, что высказывание (A) на с.46 можно пересказать следующим образом:

"для любого x, если x -рациональное число, то x является действительным числом".

Это высказывание, а также высказывания (B) и (C) могут быть записаны в следующем виде:

$$\forall x\,(R(x) \longrightarrow \mathcal{D}(x)) \qquad (A)$$

$$R(1/3) \qquad (B)$$

$$\mathcal{D}(1/3) \qquad (C)$$

Тогда высказывание $((A \wedge B) \longrightarrow C)$ примет вид:

$$[(\forall x\,(R(x) \longrightarrow \mathcal{D}(x)) \wedge R(1/3)) \longrightarrow \mathcal{D}(1/3)]$$

Истинность этого высказывания легко обосновывается в логике предикатов. Тем самым, введенные понятия предикатов, констант ,переменных и кванторов расширили возможности анализа рассуждений.

Произвольные формулы логики предикатов образуются из предикатных символов с помощью логических операций $\neg, \vee, \wedge, \longrightarrow$ и навешивания кванторов $\forall$, $\exists$ на предметные переменные. Однако для изучения логики предикатов нам необходимо более строгое определение языка логики предикатов. Ниже это определение будет дано с помощью индукции по числу логических символов, но вначале необходимо ввести понятие сигнатуры.

ОПРЕДЕЛЕНИЕ 1. Пусть $P_1^{n_1}, \dots, P_k^{n_k}, \dots$ - символы предикатов и $a_1, \dots, a_m$ символы предметных констант. Множество

$$\sigma = \{P_1^{n_1}, \dots, P_k^{n_k}, \dots; a_1, \dots, a_m, \dots$$

называется сигнатурой.

Зафиксируем некоторую сигнатуру σ и определим язык сигнатуры σ

ОПРЕДЕЛЕНИЕ 2. 1). Алфавит языка сигнатуры σ содержит следующие символы:

$a_1, \dots, a_m,$	-	символы предметных констант из σ,
$x_1, \dots, x_n, y, z$	-	символы предметных переменных,
$P_1^{n_1}, \dots, P_k^{n_k},$	-	предикатные символы из ,
$\neg, \wedge, \vee, \longrightarrow, \forall, \exists$	-	логические символы,
$(\ ,\ )$	-	скобки.

2). Формулы. а) Если R^n - n-местный предикатный символ и $t_1, \dots, t_n$ символы предметных переменных или констант из σ , то $R^n(t_1, \dots, t_n)$ есть формула. Такие формулы назовем атомными.

б). Если A и B ранее построенные формулы языка сигнатуры σ, то $\bar{A}$, $(A \wedge B)$, $(A \vee B)$, $(A \rightarrow B)$ – также являются формулами сигнатуры σ.

в). Если B формула сигнатуры σ и x предметная переменная, то $\forall x B$, $\exists x B$ являются формулами сигнатуры σ.

г). Других формул сигнатуры σ нет.

Пример 2. Пусть $\sigma = \{P^1, Q^2, 0, 1\}$. Тогда

а). $(\forall x\, P^1(x) \rightarrow Q^2(y, z))$, $(P^1(x) \rightarrow \exists y\, Q^2(0, y))$,

$\forall x_1 (Q^2(x_1, x_2) \vee P^1(x_1))$, $\exists y\, \forall x\, Q^2(y, 0)$,

$\forall x (P^1(y) \wedge P^1(x))$, $P^1(0)$, $Q^2(1,1)$, –

эти слова являются формулами сигнатуры σ;

б). $P^1(x,y)$, $Q^2(x)$, 0, x, $(x \rightarrow y)$, $(P^1 \wedge Q^2)$,

$P^1(y) \wedge Q^2(x,y) \vee P^1(y)$, $0 1 x P^1$, –

не являются формулами сигнатуры σ.

Формулы сигнатуры σ имеют смысл только тогда, когда имеется какая-нибудь интерпретация символов сигнатуры σ. Определим это понятие.

Пусть M непустое множество и сигнатура σ содержит символы предметных констант $a_1, \dots, a_m, \dots$ и символы предикатов $P_1^{n_1}, \dots, P_k^{n_k}, \dots$. Каждой константе a_m сопоставим некоторый элемент $\tilde{a}_m$ из M; каждому символу $P_k^{n_k}$ сопоставим n_k-местное отношение (предикат) $\tilde{P}_k^{n_k}$, определенное на множестве M. Условимся также, что предметные переменные принимают значения из множества M. Тогда будем говорить, что задана интерпретация формул языка сигнатуры σ на множестве M. Моделью сигнатуры σ называется тройка, состоящая из непустого множества M, сигнатуры σ и интерпретации формул языка сигнатуры σ на M.

Обозначение: $\langle M, \sigma \rangle$.

Иногда в математике возникает ситуация, при которой формула содержит некоторую переменную, но не зависит от значения этой переменной. Например, формула суммы $\sum\limits_{n=0}^{k} \frac{x^n}{n!}$ содержит переменную n, однако величина, определяемая этой формулой, не зависит от n. Более того, мы можем вместо n написать m, при этом смысл этой формулы не изменится. В таких случаях о переменной n говорят, что она связанная в данной формуле. С другой стороны, в той же формуле переменная x является свободной переменной. В логике предикатов в связи с введением кванторов тоже встречаются связанные и свободные предметные переменные. Введем это понятие с помощью индукции по длине формулы.

Определение 5. Пусть A формула языка логики предикатов некоторой сигнатуры. 1). Если $A = P^n(t_1, \ldots, t_n)$ атомная формула то все вхождения ее предметных переменных являются свободными, связанных вхождений переменных A не имеет.

2). Пусть для формул B и C определено какие вхождения переменных в B, C являются свободными и какие - связанными. Тогда

а). если A имеет один из следующих видов:

$$\bar{B},\ (B \wedge C),\ (B \vee C),\ (B \to C),$$

то вхождения любой переменной в A являются такими же, какими они были в формулах B и C;

б) если A имеет вид $\forall x\, B$ или $\exists x\, B$, то каждое вхождение переменной x в B является связанным, а вхождения остальных переменных являются такими же, какими они были в формуле B. При этом формула B называется областью действия кванторов $\forall$, $\exists$.

Переменная x называется свободной в A, если в A имеется хотя бы одно свободное вхождение x, в противном случае x называется связанной в A. Формула, не содержащая свободных переменных, называется замкнутой или предложением.

Пример 5. а). В формулах $\forall x_1 (Q^2(x_1, x_2) \vee P^1(x_1))$, $\exists x_1\, R(x_1)$ переменная x_1 - связанная, а x_2 - свободная.

б). В формулах $\forall x\, \exists y\, Q^2(x,y)$, $\forall x\, R^2(x,x)$ обе переменные x, y связаны.

в). $(P^1(x) \rightarrow \exists x\, Q^1(x))$ здесь первое вхождение x является свободным, а второе связанным.

2. Истинность.

Введенные понятия предметных переменных, констант, предикатов и кванторов позволяют произвести строгий математический анализ понятия истинности утверждения. Для этого мы фиксируем некоторую сигнатуру σ и произвольную модель $\langle M, \sigma \rangle$ данной сигнатуры. Используя индукцию по построению формулы, мы дадим строгое определение истинности формулы A сигнатуры σ в модели $\langle M, \sigma \rangle$.

Произвольная формула A сигнатуры σ может содержать символы предметных переменных и констант. Если проинтерпретировать A в модели $\langle M, \sigma \rangle$, то символам констант будут сопоставлены определенные значения из множества M. Кроме того, всем свободным переменным в A мы сопоставим произвольные фиксированные значения из M. Тогда если A содержит некоторые символы констант и свободных переменных $t_1, \dots, t_n$, то им будут сопоставлены некоторые значения из множества M : $t_1 = a_1, \dots, t_n = a_n$. И в дальнейшем истинность или ложность формулы A будет определяться относительно этих фиксированных значений.

ОПРЕДЕЛЕНИЕ 4. 1). Если $A = R^n(t_1, \dots, t_n)$ - атомная формула, то будем говорить, что $A = И$ при $t_1 = a_1, \dots, t_n = a_n$ тогда и только тогда, когда кортеж $\langle a_1, \dots, a_n \rangle$ удовлетворяет отношению $\tilde{R}^n$, которое интерпретирует символ предиката R^n :

$$R^n(a_1, \dots, a_n) = И \longleftrightarrow \langle a_1, \dots, a_n \rangle \in \tilde{R}^n$$

2). Пусть формулы B и C имеют определенные истинностные значения при $t_1 = a_1, \dots, t_n = a_n$. Тогда истинностные значения формул $\bar{B}$, $(B \wedge C)$, $(B \vee C)$, $(B \rightarrow C)$ определяются по соответствующим таблицам истинности:

B	C	$\bar{B}$	$(B \wedge C)$	$(B \vee C)$	$(B \to C)$
И	И	Л	И	И	И
И	Л	Л	Л	И	Л
Л	И	И	Л	И	И
Л	Л	И	Л	Л	И

3). Пусть $A = \exists x\, B(x)$ и для любого $a_0 \in M$ определено истинностное значение $B(x)$ при $x = a_0, t_1 = a_1, \dots, t_n = a_n$. Тогда

($\exists x\, B(x)$ = И при $t_1 = a_1, \dots, t_n = a_n$) $\longleftrightarrow$ существует $a_0 \in M$ такое, что $B(x)$ = И при $x = a_0, t_1 = a_1, \dots, t_n = a_n$

4). Пусть $A = \forall x\, B(x)$ и для любого $a_0 \in M$ определено истинностное значение $B(x)$ при $x = a_0, t_1 = a_1, \dots, t_n = a_n$. Тогда

($\forall x\, B(x)$ = И при $t_1 = a_1, \dots, t_n = a_n$) $\longleftrightarrow$ для любого $a_0 \in M$ $B(x)$ = И при $x = a_0, t_1 = a_1, \dots, t_n = a_n$.

ПРИМЕР 4. Пусть $N = \{0, 1, 2, \dots\}$ – множество натуральных чисел, сигнатура $\mathfrak{S} = \{S^3, P^3, 0, 1\}$. Символы $0, 1$ интерпретируем как $0, 1$, соответственно; символы S^3, P^3 интерпретируем посредством следующих соотношений:

$$S^3(x, y, z) = \text{И} \longleftrightarrow x + y = z,$$

$$P^3(x, y, z) = \text{И} \longleftrightarrow x \cdot y = z$$

Тогда $\langle N; S^3, P^3, 0, 1 \rangle$ является моделью арифметики натуральных чисел, а следующие формулы выражают соответствующие математические суждения:

а). $\forall x\, \forall y\, \exists z\, S^3(x, y, z)$ – существует сумма произвольных чисел x, y.

б). $\exists y\, \forall x\, S^3(x, y, x)$ – существует число нуль,

в). $\exists x\, S^3(x, 1, 0)$ – существуют отрицательные числа,

г). $\forall x\, \forall y\, \exists z\, P^3(x, z, y)$ – существует частное от деления y на x.

О приведенных формулах можно судить истинны они или ложны в модели $\langle N, \mathfrak{S} \rangle$: а), б) – истинны, в), г) – ложны.

В следующей теореме мы показываем, что введенные понятия истинности и ложности формулы обладают естественными свойствами интуитивных понятий истинности и ложности.

ТЕОРЕМА 1. Каждая замкнутая формула $\mathcal{A}$ сигнатуры σ в любой модели $\langle M, \sigma \rangle$ является либо истинной, либо ложной, и не может быть одновременно истинной и ложной.

Доказательство теоремы непосредственно следует из определения 4.

ЗАМЕЧАНИЕ 1. В определении 4 непосредственно указано в каком случае формулы вида $\forall x B$, $\exists x B$ являются истинными. Полезно также запомнить случаи, в которых эти формулы ложны. А именно, пусть $\langle M, \sigma \rangle$ модель для этих формул, и в формуле B зафиксированы все свободные переменные, кроме x. Тогда

$$(\forall x B = Л) \longleftrightarrow \text{существует } a \in M, \text{ для которого } B = Л \text{ при } x = a,$$
$$(\exists x B = Л) \longleftrightarrow \text{для любого } a \in M : B = Л \text{ при } x = a.$$

3. Тождественно истинные формулы, эквивалентность.

ОПРЕДЕЛЕНИЕ 5. Пусть $\mathcal{A}$ - формула сигнатуры σ и $x_1, \ldots, x_n$ - ее свободные переменные. Формула $\mathcal{A}$ называется выполнимой, если существует модель $\langle M, \sigma \rangle$, в которой $\mathcal{A}$ истинна при некоторых фиксированных значениях переменных $x_1, \ldots, x_n$ из M. Формула $\mathcal{A}$ называется тождественно истинной или тавтологией, если она истинна в любой модели $\langle M, \sigma \rangle$ при любой фиксации ее свободных переменных значениями из множества M.

Условимся писать $M \models \mathcal{A}$, если формула $\mathcal{A}$ истинна в модели $\langle M, \sigma \rangle$ при любой фиксации ее свободных переменных значениями из M; и будем писать $\models \mathcal{A}$, если $\mathcal{A}$ тождественно истинная формула.

Как и в алгебре высказываний мы отождествляем схемы правильных рассуждений с тождественно истинными формулами. Отметим, что все тавтологии алгебры высказываний будут тавтологиями логики предикатов. Это легко следует из пункта 2/ определения 4. Истинностные значения формул, образованных с помощью логических символов $\neg$, $\wedge$, $\vee$, $\longrightarrow$, вычисляются по тем же таблицам истинности, что и в алгебре высказываний.

Такое же замечание можно сделать по отношению к теоремам, доказанным в алгебре высказываний. Поэтому в дальнейшем мы подразумеваем, что теоремы 1,2,4,5 из раздела 1 выполняются в логике предикатов.

Рассмотрим новые тавтологии и правила их образования в логике предикатов.

ТЕОРЕМА 2. Пусть $A(x)$ - формула логики предикатов и $A(y)$ получается из $A(x)$ заменой всех свободных вхождений x на y. Тогда если все новые вхождения переменной y свободны в $A(y)$, то следующие формулы тождественно истинны:

$$(\forall x\, A(x) \longrightarrow A(y)), \qquad (A(y) \longrightarrow \exists x\, A(x)) \qquad (1)$$

Доказательство. Пусть выполняется условие теоремы и $\langle M, \sigma\rangle$ - произвольная модель для формул (1). Для проверки тождественной истинности формул (1) мы фиксируем в них все свободные переменные значениями из M. В частности, если формула $A(x)$ содержит свободные вхождения x, то $A(y)$ будет содержать свободные вхождения y и этим вхождениям будет сопоставлено фиксированное значение $y_0 \in M$.

Рассмотрим формулу $\forall x A(x) \longrightarrow A(y_0)$. Если $A(x)$ не содержит свободных вхождений x, то $\forall x A(x) \to A(y_0)$ примет вид $A \to A$ и в силу примера 9 из главы 1 эта формула тождественно истинна. Пусть $A(x)$ содержит свободные вхождения x и $\forall x A(x) = И$ в $\langle M, \sigma\rangle$. Тогда для всех $x_0 \in M$ $A(x) = И$ при $x = x_0$. В формуле $A(y)$ переменная y является свободной и в силу предыдущего $A(y) = И$ при $y = y_0$. Если же $\forall x A(x) = Л$, то сразу выполняется $(\forall x A(x) \to A(y_0)) = И$.

Рассмотрим формулу $A(y_0) \longrightarrow \exists x A(x)$. Если $A(x)$ не содержит свободных вхождений x, то $A(y_0) \to \exists x A(x)$ примет вид $A \to A$ и потому будет истинной. Пусть $A(x)$ содержит свободные вхождения x и эти вхождения заменены на y. Если $A(y) = И$ при $y = y_0 \in N$, то $A(x)$ будет истинной при $x = y_0$. Действительно, если $A(x)$ содержит свободные вхождения y, то после фиксации всех свободных переменных в формуле $A(y) \to \exists x A(x)$ эти вхождения в формулы $A(x)$ и $A(y)$ одновременно примут одинаковое значение $y_0 \in M$. Поэтому $A(x)$ и $A(y)$ имеют одинаковые истинностные значения при $x = y_0$ и $y = y_0$ соответственно. Далее, если $A(x) = И$ при $x = y_0$, то формула $\exists x A(x)$ так же будет истинной в $\langle M, \sigma \rangle$, и потому $(A(y_0) \to \exists x A(x)) = И$. Если же $A(y_0) = Л$ в $\langle M, \sigma \rangle$, то сразу выполняется: $(A(y_0) \to \exists x A(x)) = И$. Теорема доказана.

Замечание 2. В теореме 2 на формулы (1) было наложено специальное условие на переменные x и y. Приведем пример, показывающий, что без этого условия формулы (1) не будут тождественно истинными.

Пример 5. Пусть $P(x,y)$ обозначает отношение равенства: $x = y$. В качестве модели возьмем $\langle N; P(x,y) \rangle$, где $N = \{1, 2, 3, \dots\}$. Пусть $A(x) = \exists y\, P(x,y)$ и $B(x) = \forall y\, P(x,y)$. Тогда следующие формулы являются ложными в $\langle N; P(x,y) \rangle$:

$$(\forall x A(x) \to A(y)), \quad (B(y) \to \exists x B(x))$$

Действительно, содержательно первая формула означает:

$$[\forall x \exists y (x \neq y) \to \exists y (y \neq y)]$$

вторая формула означает:

$$[\forall y (y = y) \to \exists x \forall y (x = y)]$$

Легко видеть, что посылки в этих импликациях истинны, а заключения ложны. Подчеркнем, что рассмотренные формулы имеют вид (1), но не удовлетворяют дополнительному условию теоремы 2. В формуле $A(x) = \exists y \overline{P(x,y)}$ переменная x входит свободно, но после замены x на y новое вхождение переменной y попало в область действия квантора $\exists y$ и стало связанным в формуле $\exists y \overline{P(y,y)}$. Возникла неестественная ситуация: свободное вхождение переменной после переименования стало связанным. Выделим подобные ситуации с помощью специального понятия.

Определение 6. Пусть $A(x)$ формула логики предикатов и $A(y)$ получается из $A(x)$ заменой всех свободных вхождений x на y. Тогда если все новые вхождения y свободны в $A(y)$, то переменная y

называется свободной для x в $A(x)$.

ТЕОРЕМА 3. Пусть $B(x)$, C формулы логики предикатов и C не содержит свободных вхождений переменной x. Тогда

а/. Если $\models (C \to B(x))$, то $\models (C \to \forall x\, B(x))$;

б/. Если $\models (B(x) \to C)$, то $\models (\exists x\, B(x) \to C)$.

Доказательство. а/. Пусть $\models (C \to B(x))$. Возьмем произвольную модель $\langle M, \sigma \rangle$ для формулы $(C \to \forall x\, B(x))$ и зафиксируем все свободные переменные в $(C \to \forall x\, B(x))$ значениями из M. Тогда в формуле $B(x)$ останется свободной только переменная x, а формула C не будет иметь свободных переменных, и потому $C = И$ или $C = Л$. Если $C = Л$, то вся формула $(C \to \forall x\, B(x)) = И$.

Пусть $C = И$. По условию для любого $\tilde{x} \in M$ формула $(C \to B(x))$ истинна при $x = \tilde{x}$, поэтому по теореме 4 из главы 1 формула $B(x)$ должна также принимать значение истина при любых $x = \tilde{x}$. Это означает, что $\forall x\, B(x)$ истинна в модели $\langle M, \sigma \rangle$, а вместе с ней истинна формула $(C \to \forall x\, B(x))$.

б/. Аналогично, пусть $\models (B(x) \to C)$ и $\langle M, \sigma \rangle$ модель той же сигнатуры, что и $(\exists x\, B(x) \to C)$. Зафиксируем все свободные переменные в $(\exists x\, B(x) \to C)$ некоторыми значениями из M. Если $\exists x\, B(x) = Л$, то сразу выполняется $(\exists x\, B(x) \to C) = И$. Пусть $\exists x\, B(x) = И$, тогда для некоторого значения $x_0 \in M$ формула $B(x)$ истинна при $x = x_0$. Так как $(B(x) \to C)$ тавтология, то $(B(x) \to C) = И$ при $x = x_0$. Отсюда по теореме 4 из главы 1 следует, что $C = И$ в $\langle M, \sigma \rangle$. Следовательно, формула $(\exists x\, B(x) \to C)$ также истинна в $\langle M, \sigma \rangle$. Теорема доказана.

ОПРЕДЕЛЕНИЕ 8. Формулы A и B сигнатуры σ называются эквивалентными /обозначение: $A \sim B$ /, если в любой модели $\langle M, \sigma \rangle$ при любых фиксированных значениях из M своих свободных переменных формулы A и B принимают одинаковые истинностные значения.

Пример 4. $\forall x\, \forall y\, P(x,y) \sim \forall y\, \forall x\, P(x,y)$,

$\exists x\, \exists y\, Q(x,y) \sim \exists y\, \exists x\, Q(x,y)$; $\forall x\, P'(x) \sim \forall y\, P'(y)$.

Чтобы доказать эквивалентность некоторых формул $\mathcal{A}$ и $\mathcal{B}$ необходимо показать, что в любой модели соответствующей сигнатуры формулы $\mathcal{A}$ и $\mathcal{B}$ принимают одинаковые истинностные значения при одинаковой фиксации свободных переменных. Это можно осуществить несколькими способами.

1. Прямой способ: фиксируем произвольную модель $\langle M, \sigma \rangle$ той же сигнатуры, что формулы $\mathcal{A}, \mathcal{B}$, и доказываем два утверждения:

а/. если $\mathcal{A} = И$ в $\langle M, \sigma \rangle$, то $\mathcal{B} = И$ в $\langle M, \sigma \rangle$;

б/. если $\mathcal{B} = И$ в $\langle M, \sigma \rangle$, то $\mathcal{A} = И$ в $\langle M, \sigma \rangle$

В этом способе вместо утверждений а/ и б/ можно рассматривать соответственно эквивалентные им утверждения а$'$/ и б$'$/:

а$'$/. если $\mathcal{B} = Л$ в $\langle M, \sigma \rangle$, то $\mathcal{A} = Л$ в $\langle M, \sigma \rangle$;

б$'$/. если $\mathcal{A} = Л$ в $\langle M, \sigma \rangle$, то $\mathcal{B} = Л$ в $\langle M, \sigma \rangle$.

2. Способ от противного: предполагаем, что в некоторой модели $\langle M, \sigma \rangle$ формулы $\mathcal{A}$ и $\mathcal{B}$ принимают неодинаковые значения, и рассматриваем два случая:

а$''$/. Пусть $\mathcal{A} = И$ и $\mathcal{B} = Л$ в $\langle M, \sigma \rangle$,

б$''$/. Пусть $\mathcal{A} = Л$ и $\mathcal{B} = И$ в $\langle M, \sigma \rangle$.

В каждом из этих случаев необходимо получить противоречие. Полученное противоречие показывает, что в любой модели $\langle M, \sigma \rangle$ формулы $\mathcal{A}$ и $\mathcal{B}$ не могут принимать различные значения, т.е. $\mathcal{A} \sim \mathcal{B}$.

3. Если же необходимо опровергнуть эквивалентность некоторых формул, то строится модель, в которой одна формула истинна, а другая ложна.

В следующей теореме мы демонстрируем указанные способы доказательства эквивалентностей.

ТЕОРЕМА 4. Если $\mathcal{B}$ не содержит свободных вхождений x, то верны следующие эквивалентности:

1/. $(\overline{\forall x\, \mathcal{A}(x)}) \sim \exists x\, \overline{\mathcal{A}(x)}$;

$(\overline{\exists x\, \mathcal{A}(x)}) \sim \forall x\, \overline{\mathcal{A}(x)}$;

2/. $(\forall x\, \mathcal{A}(x) \wedge \mathcal{B}) \sim \forall x\, (\mathcal{A}(x) \wedge \mathcal{B})$;

$(\exists x\, \mathcal{A}(x) \wedge \mathcal{B}) \sim \exists x\, (\mathcal{A}(x) \wedge \mathcal{B})$;

3/. $(\forall x\, A(x) \vee B) \sim \forall x(A(x) \vee B)$,

$(\exists x\, A(x) \vee B) \sim \exists x\, (A(x) \vee B)$,

4/. $(\forall x\, A(x) \longrightarrow B) \sim \exists x\, (A(x) \longrightarrow B)$,

$(\exists x\, A(x) \longrightarrow B) \sim \forall x\, (A(x) \longrightarrow B)$

5/. $(B \longrightarrow \forall x\, A(x)) \sim \forall x\, (B \longrightarrow A(x))$

$(B \longrightarrow \exists x\, A(x)) \sim \exists x\, (B \longrightarrow A(x))$

Доказательство. 1/. Пусть $\langle M,\sigma\rangle$ произвольная модель той же сигнатуры, что и формулы $A(x)$, B . Зафиксируем некоторыми значениями из M все свободные переменные в этих формулах, кроме x, и рассмотрим два случая.

а/. Пусть $\overline{\forall x\, A(x)} = \text{И}$ в $\langle M,\sigma\rangle$, тогда $\forall x\, A(x) = \text{Л}$ в $\langle M,\sigma\rangle$. Последнее означает, что существует $x_0 \in M$ такой, что $A(x) = \text{Л}$ при $x = x_0$. Для такого $x_0 \in M$: $\overline{A(x)} = \text{И}$ при $x = x_0$. Это влечет: $\exists x\, \overline{A(x)} = \text{И}$ в $\langle M,\sigma\rangle$.

б/. Пусть $\overline{\forall x\, A(x)} = \text{Л}$ в $\langle M,\sigma\rangle$, тогда $\forall x\, A(x) = \text{И}$ в $\langle M,\sigma\rangle$ и следовательно, для любого $x_0 \in M$: $A(x_0) = \text{И}$ и $\overline{A(x_0)} = \text{Л}$. Последнее означает, что $\exists x\, \overline{A(x)} = \text{Л}$.

4/. Предположим, от противного, что существует модель $\langle M,\sigma\rangle$ той же сигнатуры, что и формулы B, $A(x)$, в которой эквивалентность $(\forall x\, A(x) \to B) \sim \exists x (A(x) \to B)$ не верна.

а/. Пусть $(\forall x\, A(x) \longrightarrow B) = \text{И}$ и $\exists x (A(x) \longrightarrow B) = \text{Л}$ в $\langle M,\sigma\rangle$. Из последнего соотношения имеем: для любого $x_0 \in M$: $(A(x_0) \longrightarrow B) = \text{Л}$ или $A(x_0) = \text{И}$ и $B = \text{Л}$. Таким образом, для каждого $x_0 \in M$: $A(x_0) = \text{И}$, что означает: $\forall x\, A(x) = \text{И}$ в $\langle M,\sigma\rangle$. Тогда импликация $(\forall x\, A(x) \longrightarrow B) = \text{Л}$ в $\langle M,\sigma\rangle$, что противоречит первоначальному допущению.

б/. Пусть $(\forall x\, A(x) \longrightarrow B) = \text{Л}$ и $\exists x (A(x) \longrightarrow B) = \text{И}$ в $\langle M,\sigma\rangle$. Импликация $(\forall x\, A(x) \longrightarrow B)$ ложна только в случае, когда $\forall x\, A(x) = \text{И}$ и $B = \text{Л}$. Это означает, что для любого $x_0 \in M$: $A(x) = \text{И}$ при $x = x_0$ и независимо от x_0 $B = \text{Л}$. Тогда $(A(x_0) \longrightarrow B) = \text{Л}$ для всех $x_0 \in M$. С другой стороны, равенство $\exists x (A(x) \longrightarrow B) = \text{И}$ влечет: существует $x_0 \in M$, для которого $(A(x) \longrightarrow B) = \text{И}$ при $x = x_0$. Это противоречит предыдущему заключению.

Доказательство остальных эквивалентностей предоставляется читателю в качестве упражнения.

В логике предикатов , как и в алгебре высказываний , эквивалентные формулы можно заменять друг на друга. Этот факт мы доказываем в следующем разделе, используя средства формального исчисления. А сейчас, учитывая этот факт, отмечаем, что эквивалентности теоремы 4 описывают способы внесения и вынесения кванторов $\forall, \exists$ под знаки логических операций $^{-}, \wedge, \vee, \rightarrow$. Например, под знаки конъюнкции и дизъюнкции кванторы $\forall, \exists$ вносятся без изменения, а при внесении под знак отрицания происходит изменение кванторов: квантор $\forall$ меняется на $\exists$, и квантор $\exists$ меняется на $\forall$.

Пример 7. Преобразовать формулу $(\forall z\, B(y,z) \rightarrow \overline{\exists x\, P(x)})$, где $B(y,z)$ не содержит свободных вхождений x .

$$(\forall z\, B(y,z) \rightarrow \overline{\exists x\, P(x)}) \sim (\forall z\, B(y,z) \rightarrow \forall x\, \overline{P(x)}) \sim$$
$$\sim \forall x\, (\forall z\, B(y,z) \rightarrow \overline{P(x)}) \sim \forall x\, \exists z\, (B(y,z) \rightarrow \overline{P(x)}).$$

Раздел 4. Исчисление предикатов.

В данном разделе рассматривается формальный подход к изучению предикатов. Мы полностью отвлекаемся от соображений, связанных с содержанием формул, и строим формальную систему, которая называется исчислением предикатов / ИП /. Основные свойства предикатов описываются с помощью доказуемых формул. В последних параграфах доказывается равносильность содержательного и формального подходов, и приводятся основные теоремы теории моделей и исчисления предикатов.

1. Аксиомы и правила вывода.

Язык исчисления предикатов полностью совпадает с языком логики предикатов, описанным в предыдущем разделе. Единственная особенность языка исчисления предикатов состоит в том, что мы заранее фиксируем некоторое множество предикатных символов и констант

$$P_1^{n_1},\ P_2^{n_2},\ \ldots,\ P_k^{n_k},\ \ldots;\ a_1,\ \ldots,\ a_m,\ \ldots \qquad (6)$$

и в дальнейшем используем только эти предикатные символы. Другими словами, мы строим исчисление предикатов заданной сигнатуры σ

Правила построения формул, данные в определении 2 / с.49 /, остаются прежними. Кроме того, мы по-прежнему используем понятия свободной и связанной переменных, и понятие переменной y, свободной для x в формуле $A(x)$ / см. определение 4 на с. 56 /.

Исчисление предикатов содержит бесконечное число аксиом, каждая из которых образуется по одной из схем I.1 - IV.2 исчисления высказываний а также по следующим двум схемам:

V.1. $\forall x\, A(x) \longrightarrow A(y)$,

2. $A(y) \longrightarrow \exists x\, A(x)$,

где формула $A(y)$ получается из $A(x)$ заменой всех свободных вхождений x на y, и y является свободной для x в $A(x)$.

Конечно применять эти схемы надо для нового понятия формулы ИП.

Пример 1. а/. $\forall x\, P^1(x) \longrightarrow P^1(y)$ - аксиома V.1;

б/. $P^1(y) \longrightarrow \exists x\, P^1(x)$ - аксиома V.2,

в/. $\forall x\, \exists y\, R^2(x,y) \longrightarrow \exists y\, R^2(y,y)$ не является аксиомой, ибо y не свободна для x в формуле $\exists y R^2(x, y)$,

в/ $\forall z \exists y_2 R^2(x, y) \to \exists y R^2(z, y)$ - аксиома, здесь роль y выполняет z в У.1;

д/. $\forall y Q^2(x, y) \to \exists x \forall y Q^2(x, y)$ - аксиома, здесь роль y в У.2 выполняет сам x.

Правилами вывода в ИП являются модус поненс / см. с. 2* / и два новых правила: $\forall$ -правило и $\exists$ -правило.

Определение 1. $\forall$-правило - это правило перехода от формулы вида $(C \to A(x))$ к формуле $C \to \forall x A(x)$, где формула C не содержит свободных вхождений x. Символически это правило записывается следующим образом:

$$\frac{C \to A(x)}{C \to \forall x A(x)} \qquad (\forall\text{-пр})$$

$\exists$-пр. это правило перехода от формулы вида $A(x) \to C$ к формуле $\exists x A(x) \to C$, где формула C не содержит свободных вхождения x. Символически:

$$\frac{A(x) \to C}{\exists x A(x) \to C} \qquad (\exists\text{-пр})$$

Формула A называется доказуемой или выводимой в ИП, если существует конечная последовательность формул $B_1, B_2, \ldots, B_k$ / называемая выводом /, в которой $B_k = A$ и каждая B_i есть либо аксиома, либо получается из предыдущих формул этой последовательности по одному из правил вывода ИП. Обозначение: $\vdash A$.

Пример 2. а/. $\vdash \forall x P^1(x) \to \forall y P^1(y)$ Вывод этой формулы состоит из двух формул:

1. $\forall x P^1(x) \to P^1(y)$ — / См У.1 /
2. $\forall x P^1(x) \to \forall y P^1(y)$ — / $\forall$-пр. к 1 /

б/. $\vdash \exists x P(x) \to \exists y P(y)$

1. $P(x) \to \exists y P(y)$ — / См У.2 /
2. $\exists x P(x) \to \exists y P(y)$ — / $\exists$ -пр. к 1/

в/. Следующая последовательность формул не является выводом в ИП:

1. $\forall x \exists \omega P^3(x, \omega, y) \longrightarrow \exists \omega P^3(y, \omega, y)$ /СА V.1/

2. $\forall x \exists \omega P^3(x, \omega, y) \longrightarrow \forall y \exists \omega P^3(y, \omega, y)$

Вторая формула получена из первой с помощью $\forall$-правила, примененного к переменной y. Но y свободна в формуле $(= \forall x \exists \omega P^3(x, \omega, y))$ и потому $\forall$-правило нельзя применять к y.

Теперь введем понятие выводимости из гипотез в исчислении предикатов. Основной смысл этого понятия заключается в том, чтобы формулы выводимые из истинных гипотез, также были истинными. Гипотезами являются произвольные формулы ИП, которые могут содержать свободные переменные. Истинность гипотез в логике предикатов определяется путем задания определенной модели $\langle M, \sigma \rangle$ и фиксации в гипотезах всех свободных переменных некоторыми значениями из M. И, коль скоро, при такой фиксации гипотезы $A_1, \ldots, A_m$ истинны в $\langle M, \sigma \rangle$, то формула B, выводимая из $A_1, \ldots, A_m$, должна быть истинной в $\langle M, \sigma \rangle$ при той же фиксации в M свободных переменных. Отсюда следует, что свободные переменные в гипотезах должны рассматриваться как символы констант и потому применять $\forall$-правило и $\exists$-правило к этим переменным нельзя.

Определение 2. Пусть $A_1, \ldots, A_m$ формулы ИП, свободные переменные которых суть $x_1, \ldots, x_n$. Формула B называется выводимой из гипотез $A_1, \ldots, A_m$, если существует конечная последовательность формул $B_1, \ldots, B_k$ в которой $B_k = B$, каждая $B_1, \ldots, B_k$ является либо аксиомой, либо одной из гипотез $A_1, \ldots, A_m$, либо получается по правилам вывода из предыдущих формул, причем $\forall$-правило и $\exists$-правило не применяются к переменным $x_1, \ldots, x_n$.

Пример 3. а/. $\forall y (R \longrightarrow P(y)) \vdash (R \longrightarrow \forall y P(y))$

1. $\forall y (R \rightarrow P(y))$ /гипотеза/
2. $(\forall y (R \rightarrow P(y)) \longrightarrow (R \rightarrow P(y)))$ /СА V.1/
3. $(R \longrightarrow P(y))$ /МП к 1,2/
4. $(R \longrightarrow \forall y P(y))$ /$\forall$-пр. к 3/

б/. $\forall x \forall y\, A(x,y) \vdash A(x,y)$

1. $\forall x \forall y\, A(x,y)$ /гипотеза/
2. $(\forall x \forall y\, A(x,y) \to \forall y\, A(x,y))$ / СА У.1/
3. $\forall y\, A(x,y)$ / МП к 1,2/
4. $(\forall y\, A(x,y) \to A(x,y))$ / СА У.1/
5. $A(x,y)$ / МП к 3,4/

в/. Не верно, что $(R \to P(x)) \vdash (R \to \forall x P(x))$. Здесь $\forall$ -правило применяется к переменной x, которая свободна в $(R \to P(x))$. Заметим, что легко придумать модель, в которой формула $(R \to P(x))$ истинна при некотором значении x, а формула $(R \to \forall x P(x))$ ложна.

Если сравнивать исчисление предикатов с исчислением высказываний, то легко увидеть, что последнее полностью вкладывается в исчисление предикатов. Действительно: аксиомы ИВ являются аксиомами ИП, модус поненс является правилом вывода и для ИП. Формулы ИВ образуются из простейших высказываний, но простейшие высказывания можно рассматривать как предикатные символы, не имеющие переменных, т.е. нульместные предикаты. Поэтому можно считать, что простейшие высказывания ИВ включены в исходную сигнатуру (б). После такого соглашения формулы ИВ будут формулами ИП, и все доказательства и выводы в ИВ будут являться доказательствами и выводами в ИП. Поэтому большая часть результатов, установленных в ИВ, автоматически переносится на исчисление предикатов. Например, мы будем предполагать, что в ИП выполняются теоремы 1,2,3 из раздела 2 пункт 2.

Однако в исчислении предикатов кроме МП имеются новые правила вывода по сравнению с ИВ. Поэтому некоторые теоремы требуют нового доказательства. В частности, это относится к правилу дедукции, в доказательстве которого фигурировало понятие выводимости. Из того, что правило дедукции: если $A \vdash B$, то $\vdash (A \to B)$ – верно в исчислении высказываний /теорема 4, с.31/, нельзя еще заключить, что это правило верно в исчислении предикатов; можно лишь заключить, что если $A \vdash B$ в исчислении высказываний, то $\vdash (A \to B)$ в исчислении предикатов.

следующей теореме правило дедукции будет доказано для исчисления предикатов. При этом нам потребуются вспомогательные правила вывода:

$(A \to (B \to C)) \vdash (B \to (A \to C))$ /перестановка посылок/

$(A \to (B \to C)) \vdash ((A \wedge B) \to C)$ /соединение посылок/

$((A \wedge B) \to C) \vdash (A \to (B \to C))$ /разъединение посылок/

Эти правила были доказаны в ИВ, и в силу предыдущего замечания они автоматически выполняются в ИП.

ТЕОРЕМА 1. Если $A_1, \dots, A_m \vdash B$, то $A_1, \dots, A_{m-1} \vdash (A_m \to B)$

Доказательство. Пусть $A_1, \dots, A_{m-1}, A_m \vdash B$ и $B_1, \dots, B_k$ - вывод формулы B из $A_1, \dots, A_{m-1}, A_m$. Рассмотрим последовательность формул:

$$(A_m \to B_1),\ (A_m \to B_2),\ \dots\ (A_m \to B_k) \qquad (1)$$

Так как $B_k = B$, то последняя формула в (1) есть искомая. Поэтому для доказательства теоремы достаточно дополнить (1) несколькими формулами так, чтобы получился вывод $(A_m \to B)$ из $A_1, \dots, A_{m-1}$. Дополнение (1) до вывода будем производить индукцией по $i = 1, \dots, k$

$i = 1$ $(A_m \to B_1)$. Возможны случаи: B_1 - аксиома, B_1 - одна из гипотез $A_1, \dots, A_{m-1}, A_m$. Во всех этих случаях поступаем так же как при доказательстве теоремы 4 в главе 2. Читателю предлагается рассмотреть это самостоятельно; обратим только внимание на то, что на этом шаге $\forall$-пр. и $\exists$-пр. не применяются и потому все свободные переменные из $A_1, \dots, A_m$ остаются свободными в формуле $(A_m \to B_1)$

$i < j$: $(A_m \to B_i)$ Предположим, что формулы $(A_m \to B_1), \dots, (A_m \to B_{j-1})$ из (1) дополнены до вывода из $A_1, \dots, A_{m-1}$, так, что $\forall$-пр. и $\exists$-пр. не применялись к переменным, свободным в $A_1, \dots, A_{m-1}, A_m$. Рассмотрим формулу $(A_m \to B_j)$.

а/. Если B_j - аксиома, или гипотеза, то вывод $(A_m \to B_j)$ получается так же как вывод $(A_m \to B_1)$.

б/. Пусть B_j получена из B_k, B_g по МП, где $k, g < j$. Тогда B_g имеет вид $(B_k \to B_j)$. По предположению $(A_m \to B_k)$ и $(A_m \to (B_k \to B_g))$ уже выводимы из $A_1, \dots, A_{m-1}$, и мы имеем:

1. $((A_m \to B_k) \to ((A_m \to (B_k \to B_j)) \to (A_m \to B_j)))$ / СА 1.2/
2. $((A_m \to (B_k \to B_j)) \to (A_m \to B_j))$ / МП к 1 и $(A_m \to B_k)$ /
3. $(A_m \to B_j)$ / МП к 2 и $(A_m \to (B_k \to B_j))$ /

в/. B_j получается из B_k $(k<j)$ с помощью $\forall$-пр. Тогда B_k, B_j имеют вид: $B_k = (C \to A(x))$, $B_j = (C \to \forall x\, A(x))$, где x не свободна в C. По определению 2 при выводе B из $A_1, \dots, A_m$ $\exists$-пр. и $\forall$-пр. не применялись к переменным, свободным в $A_1, \dots, A_m$. Поэтому переменная x не свободна в формулах A_m, C. Кроме того, $(A_m \to (C \to A(x)))$ уже выводима из $A_1, \dots, A_{m-1}$. Применим к ней правило соединения посылок: $((A_m \wedge C) \to A(x))$. Затем применим $\forall$-пр., ибо x не свободна в $(A_m \wedge C)$: $((A_m \wedge C) \to \forall x\, A(x))$ /подчеркнем, что здесь $\forall$-пр. не применяется к переменным, свободным в $A_1, \dots, A_m$ /. Последний шаг получается с помощью правила разъединения посылок:

$$(A_m \to (C \to \forall x\, A(x))) = (A_m \to B_j)$$

г/. B_j получено из B_k $(k<j)$ с помощью $\exists$-пр. Тогда B_k, B_j имеют вид: $B_k = (A(x) \to C)$, $B_j = (\exists x\, A(x) \to C)$. Как и в случае в/ обосновывается то, что A_m, C не содержат свободных вхождений x. По предположению формула $(A_m \to (A(x) \to C))$ выводима из $A_1, \dots, A_{m-1}$. Тогда имеем:

1. $(A(x) \to (A_m \to C))$ /перестановка посылок/
2. $(\exists x\, A(x) \to (A_m \to C))$ / $\exists$-пр. к 1/
3. $(A_m \to (\exists x\, A(x) \to C))$ /перестановка посылок/

Теорема доказана.

<u>СЛЕДСТВИЕ</u> / <u>правило контрапозиции</u>/. $A \vdash B$ тогда и только тогда, когда $\bar{B} \vdash \bar{A}$ / ПК /

Доказательство совпадает с доказательством этого правила в [illegible]

<u>Пример 4</u>. а/. $\forall x \bar{B} \vdash \overline{\exists x B}$. / сл. У.1 /

1. $\vdash \forall x \bar{B} \to \bar{B}$ /теорема 3 из раздела 2/
2. $\forall x \bar{B} \vdash \bar{B}$ / ПК /
3. $B \vdash \overline{\forall x \bar{B}}$ / ПД /
4. $\vdash B \to \overline{\forall x \bar{B}}$ / $\exists$-пр./
5. $\vdash \exists x B \to \overline{\forall x \bar{B}}$ /теорема 3 из раздела 2/
6. $\exists x B \vdash \overline{\forall x \bar{B}}$ / [illegible] /
7. $\forall x \bar{B} \vdash \overline{\exists x B}$ [illegible]

е/. $\exists x \bar{B} \vdash \overline{\forall x B}$

1. $\vdash \forall x B \rightarrow B$ / СА У.1 /
2. $\forall x B \vdash B$ /теорема 5 из раздела 2/
3. $\bar{B} \vdash \overline{\forall x B}$ / ПК /
4. $\vdash \bar{B} \longrightarrow \overline{\forall x B}$ / ПД /
5. $\vdash \exists x \bar{B} \longrightarrow \overline{\forall x B}$ / $\exists$ -пр. /
6. $\exists x \bar{B} \vdash \overline{\forall x B}$ /теорема 6 из раздела 2/

2. Производные правила вывода. Приведенная нормальная форма.

Коль скоро правило дедукции доказано в ИП, то мы без всякой оговорки можем использовать все правила введения и удаления, доказанные в ИВ /теоремы 8, 9, с. 36–37/. Добавим к этим правилам еще два правила введения и удаления кванторов.

ТЕОРЕМА 2. 1/. Введение $\forall$: если $C \vdash A(x)$ и C не имеет свободных вхождений x , то $C \vdash \forall x A(x)$

2/. Введение $\exists$: $A(y) \vdash \exists x A(x)$ при условии, что y свободна для x в $A(x)$.

3/. Удаление $\forall$: $\forall x A(x) \vdash A(y)$ при условии, что y свободна для x в $A(x)$.

4/. Удаление $\exists$: если $A(x) \vdash C$ и C не имеет свободных вхождений x , то $\exists x A(x) \vdash C$.

Доказательство. Правила 1/ и 4/ получаются из $\forall$-пр. и $\exists$-пр. с помощью теоремы 3 из главы 2 ; правила 2/ и 3/ получаются аналогично из аксиом У.1 и У.2.

Следующая теорема дает правило, позволяющее в некоторых случаях переобозначать свободные переменные в формуле. Напомним, что $A(y)$ получается из $A(x)$ заменой всех свободных вхождений x на y .

ТЕОРЕМА 3. Пусть y свободна для x в $A(x)$ и x не входит свободно в формулы $A_1, \ldots, A_m$. Тогда если $A_1, \ldots, A_m \vdash A(x)$, то $A_1, \ldots, A_m \vdash A(y)$.

Доказательство. 1. $A_1, \ldots, A_m \vdash A(x)$ /условие теоремы/

2. $A_1, \ldots, A_m \vdash \forall x A(x)$ / ВВ $\forall$ /
3. $\forall x A(x) \vdash A(y)$ / УД $\forall$ /
4. $A_1, \ldots, A_m \vdash A(y)$ / ПС /

В предыдущем разделе было введено содержательное понятие эквивалентности формул: $A \sim B$. В ИП это понятие дается в терминах выводимости: A и B называются эквивалентными в ИП, если выполняются соотношения $A \vdash B$ и $B \vdash A$ одновременно. Обозначение $A \equiv B$.

В терминах вновь введенного понятия мы продолжим описание свойств предикатов и кванторов. Докажем теорему о замене эквивалентных формул, о которой упоминалось на с. 60.

ТЕОРЕМА 4. Пусть C_A некоторая формула, в которой выделено вхождение подформулы A , и C_B получается из C_A заменой этого вхождения на формулу B . Тогда если $A \equiv B$, то $C_A \equiv C_B$.

Доказательство / индукцией по длине формулы C_A /.

1/ $C_A = P^n(x_1, \dots, x_n)$. В этом случае роль A играет символ предиката $P^n(x_1, \dots, x_n)$ и поэтому $C_B = B$. Тогда если выполняется соотношение $P^n \equiv B$, то оно же является соотношением $C_A \equiv C_B$ и утверждение теоремы автоматически выполнено.

2/. Пусть теорема выполняется для всех формул D_A , E_A , имеющих длину меньше, чем C_A , т.е. если

$$\text{если } A \equiv B \text{ , то } D_A \equiv D_B \text{ и } E_A \equiv E_B \qquad /2/$$

3/. Пусть $A \equiv B$ и C_A имеет один из следующих видов:

$$\overline{D}_A,\ (D_A \wedge E_A),\ (D_A \vee E_A),\ (D_A \to E_A),\ \forall x D_A,\ \exists x D_A$$

Тогда доказательство эквивалентности $C_A \equiv C_B$ основывается на следующих утверждениях:

а/ если $A \equiv B$, то $\overline{A} \equiv \overline{B}$;

б/ если $A \equiv B$, то $(A \wedge C) \equiv (B \wedge C)$, $(C \wedge A) \equiv (C \wedge B)$;

в/ если $A \equiv B$, то $(A \vee C) \equiv (B \vee C)$, $(C \vee A) \equiv (C \vee B)$;

г/ если $A \equiv B$, то $(C \to A) \equiv (C \to B)$, $(A \to C) \equiv (B \to C)$;

д/ если $A \equiv B$, то $\forall x A \equiv \forall x B$;

е/ если $A \equiv B$, то $\exists x A \equiv \exists x B$;

ж/ если $A \equiv B$ и $B \equiv C$, то $A \equiv C$.

Доказательства утверждений а/ – г/ представляют собой несложные упражнения в ИВ, доказательства д/, е/ аналогичны примерам

Полное доказательство теоремы мы оставляем читателю в качестве самостоятельного упражнения, а для примера разберем только один случай.

Пусть $A = B$ и $C_A = (\mathcal{D}_A \wedge E_A)$. Тогда из предположения (=) и утверждения б/ следует: $(\mathcal{D}_A \wedge E_A) \equiv (\mathcal{D}_B \wedge E_A)$, $(\mathcal{D}_B \wedge E_A) \equiv (\mathcal{D}_B \wedge E_B)$ откуда в силу ж/ имеем: $(\mathcal{D}_A \wedge E_A) \equiv (\mathcal{D}_B \wedge E_B)$, т.е. $C_A \equiv C_B$

В дополнение к эквивалентностям теоремы 4 из главы 3 мы приводим еще несколько важных эквивалентностей, позволяющих преобразовывать формулы с кванторами.

<u>ТЕОРЕМА 5.</u> 1/. Пусть переменная y не встречается в формуле $A(x)$. Тогда $\forall x\, A(x) \equiv \forall y\, A(y)$, $\exists x\, A(x) \equiv \exists y\, A(y)$

2/. Для любых формул $A(x)$, $B(x)$:

$$(\forall x\, A(x) \wedge \forall x\, B(x)) \equiv \forall x\, (A(x) \wedge B(x))$$

$$(\exists x\, A(x) \vee \exists x\, B(x)) \equiv \exists x\, (A(x) \vee B(x))$$

$$\overline{\forall x\, A(x)} \equiv \exists x\, \overline{A(x)}$$

$$\overline{\exists x\, A(x)} \equiv \forall x\, \overline{A(x)}$$

Доказательство. 1/. Если y не встречается в $A(x)$, то мы можем применять правила введения и удаления кванторов $\forall$, $\exists$ и доказательство первых эквивалентностей будет полностью совпадать с рассуждениями примеров 2 а/,б/ на с. 62.

2/. а/ $\forall x\, A(x) \wedge \forall x\, B(x) \vdash \forall x\, (A(x) \wedge B(x))$

1. $\forall x\, A(x) \wedge \forall x\, B(x) \vdash \forall x\, A(x)$ / ПУ $\wedge$ /
2. $\forall x\, A(x) \vdash A(x)$ / ПУ $\forall$ /
3. $\forall x\, A(x) \wedge \forall x\, B(x) \vdash A(x)$ / ПС /

4-6. Аналогично получаем: $\forall x\, A(x) \wedge \forall x\, B(x) \vdash B(x)$

7. $\forall x\, A(x) \wedge \forall x\, B(x) \vdash A(x) \wedge B(x)$ / ПВ $\wedge$ /
8. $\forall x\, A(x) \wedge \forall x\, B(x) \vdash \forall x\, (A(x) \wedge B(x))$ / ПВ $\forall$ /

б/. $\forall x\, (A(x) \wedge B(x)) \vdash \forall x\, A(x) \wedge \forall x\, B(x)$

1. $\forall x\, (A(x) \wedge B(x)) \vdash A(x) \wedge B(x)$ / ПУ $\forall$ /
2. $A(x) \wedge B(x) \vdash A(x)$ / ПУ $\wedge$ /
3. $\forall x\, (A(x) \wedge B(x)) \vdash A(x)$ / ПС /
4. $\forall x\, (A(x) \wedge B(x)) \vdash \forall x\, A(x)$ / ПВ $\forall$ /

5–7. Аналогично получаем $\forall x\,(A(x) \wedge B(x)) \vdash \forall x\, B(x)$

8. $\forall x\,(A(x) \wedge B(x)) \vdash \forall x\, A(x) \wedge \forall x\, B(x)$ / ПВ $\wedge$ /

в/. $\exists x\, A(x) \vee \exists x\, B(x) \vdash \exists x\,(A(x) \vee B(x))$

1. $A(x) \vdash A(x) \vee B(x)$ / ПВ $\vee$ /
2. $A(x) \vee B(x) \vdash \exists x\,(A(x) \vee B(x))$ / ПВ $\exists$ /
3. $A(x) \vdash \exists x\,(A(x) \vee B(x))$ / ПС /
4. $\exists x\, A(x) \vdash \exists x\,(A(x) \vee B(x))$ / ПУ $\exists$ /

5–7. Аналогично получаем $\exists x\, B(x) \vdash \exists x\,(A(x) \vee B(x))$

8. $\exists x\, A(x) \vee \exists x\, B(x) \vdash \exists x\,(A(x) \vee B(x))$ / ПУ $\vee$ /

г/. $\exists x\,(A(x) \vee B(x)) \vdash \exists x\, A(x) \vee \exists x\, B(x)$

1. $A(x) \vdash \exists x\, A(x)$ / ПВ $\exists$ /
2. $\exists x\, A(x) \vdash \exists x\, A(x) \vee \exists x\, B(x)$ / ПВ $\vee$ /
3. $A(x) \vdash \exists x\, A(x) \vee \exists x\, B(x)$ / ПС /

4–6. Аналогично получаем $B(x) \vdash \exists (x)\, A(x) \vee \exists x\, B(x)$

7. $A(x) \vee B(x) \vdash \exists x\, A(x) \vee \exists x\, B(x)$ / ПУ $\vee$ /
8. $\exists x\,(A(x) \vee B(x)) \vdash \exists x\, A(x) \vee \exists x\, B(x)$ / ПУ $\exists$ /

д/. $\overline{\exists x\, A(x)} \vdash \forall x\, \overline{A(x)}$

1. $A(x) \vdash \exists x\, A(x)$ / ПВ $\exists$ /
2. $\overline{\exists (x)\, A(x)} \vdash \overline{A(x)}$ / ПК /
3. $\overline{\exists (x)\, A(x)} \vdash \forall x\, \overline{A(x)}$ / ПВ $\forall$ /

е/. $\forall x\, \overline{A(x)} \vdash \overline{\exists x\, A(x)}$

1. $\forall x\, \overline{A(x)} \vdash \overline{A(x)}$ / ПУ $\forall$ /
2. $A(x) \vdash \overline{\forall x\, \overline{A(x)}}$ / ПК /
3. $\exists x\, A(x) \vdash \overline{\forall x\, \overline{A(x)}}$ / ПУ $\exists$ /
4. $\forall x\, \overline{A(x)} \vdash \overline{\exists x\, A(x)}$ / ПК /

Теорема доказана.

Определение 3. Формула A называется приведенной нормальной формой, если она имеет вид:

$$A = Q_1 x_1 \ldots Q_k x_k\, C(x_1, \ldots, x_k),$$

где $Q_1, \ldots, Q_k$ – кванторы $\forall$ или $\exists$, а формула $C(x_1, \ldots, x_k)$ не содержит кванторов и имеет среди своих свободных переменных $x_1, \ldots, x_k$. Если формула B эквивалентна A, то говорят, что A есть приведенная нормальная форма для B.

<u>Пример 5.</u> $\forall x_1 \exists x_2 \forall x_3 (P(x_1) \vee Q(x_2, x_3))$, $\exists x \forall y \forall z (A(x) \to (B(y,z) \vee C(x)))$ — приведенная нормальная форма,

$\forall x (A(x) \to \exists y B(y))$ — не является приведенной нормальной формой.

<u>ТЕОРЕМА 6.</u> Всякая формула B в ИП имеет приведенную нормальную форму.

Доказательство / индукцией по длине формулы B /. 1/. Если $B = P^n(x_1, \ldots, x_n)$ - предикат, то B уже находится в приведенной нормальной форме.

2/. Предположим, что формулы D и E имеют приведенные нормальные формы:

$$D = Q'_1 x_1 \ldots Q'_m x_m C_1(x_1, \ldots, x_m)$$

$$E = Q''_1 y_1 \ldots Q''_k y_k C_2(y_1, \ldots, y_k)$$

$\forall x A(x) \equiv \forall y A(y)$

$\exists x A(x) \equiv \exists y A(y)$

В силу эквивалентностей 1/ теоремы 5 мы можем переименовать связанные переменные в формулах D и E так, что $x_1, \ldots, x_m$ не будут встречаться в $C_2(y_1, \ldots, y_k)$ и $y_1, \ldots, y_k$ не будут встречаться в $C_1(x_1, \ldots, x_m)$.

Пусть некоторая формула B имеет один из следующих видов:

$$\overline{D},\ (D \wedge E),\ (D \vee E),\ (D \to E),\ \underline{\forall x D,\ \exists x D}.$$

В последних двух случаях B будет эквивалентна одной из следующих приведенных нормальных форм: $\forall x Q'_1 x_1 \ldots Q'_m x_m C_1(x_1, \ldots, x_m)$,

$\exists x Q'_1 x_1 \ldots Q'_m x_m C_1(x_1, \ldots, x_m)$.

В оставшихся случаях формула B будет эквивалентна одной из следующих формул: $\overline{Q'_1} x_1 \ldots \overline{Q'_m} x_m \overline{C_1}(x_1, \ldots, x_m)$,

$Q'_1 x_1 \ldots Q'_m x_m C_1(x_1, \ldots, x_m) \wedge Q''_1 y_1 \ldots Q''_k y_k C_2(y_1, \ldots, y_k)$,

$Q'_1 x_1 \ldots Q'_m x_m C_1(x_1, \ldots, x_m) \vee Q''_1 y_1 \ldots Q''_k y_k C_2(y_1, \ldots, y_k)$,

$Q'_1 x_1 \ldots Q'_m x_m C_1(x_1, \ldots, x_m) \to Q''_1 y_1 \ldots Q''_k y_k C_2(y_1, \ldots, y_k)$.

Учитывая замечание о переименовании переменных и используя основные эквивалентности ИП, мы соответствующим образом вынесем кванторы из-под знаков логических операций $^-$, $\wedge$, $\vee$, $\to$. В результате получим приведенную нормальную форму для B.

<u>Пример 6.</u> $(\forall x P(x,y) \to \exists x R(x)) \equiv \exists x (P(x,y) \to \exists x R(x)) \equiv$

$\equiv \exists z (P(z,y) \to \exists x R(x)) \equiv \exists z \exists x (P(z,y) \to R(x))$.

3. Непротиворечивые и полные множества формул.

ОПРЕДЕЛЕНИЕ 4. Пусть S произвольное множество предложений сигнатуры σ. Тогда

а/. S называется выполнимым, если существует такая модель $\langle M, \sigma \rangle$ в которой истинны все предложения из S, в противном случае S называется невыполнимым.

б/. S называется противоречивым, если существует такое предложение A сигнатуры σ, что $S \vdash A \wedge \bar{A}$, в противном случае S называется непротиворечивым.

Пусть множество предложений S выполнимо. Это значит, что мы можем придать S такое содержание, при котором все предложения из S будут истинными. В таком случае в разговорном языке часто говорят, что рассуждения, проведенные в S, имеет смысл. И наоборот, если некоторое рассуждение S кажется неправдоподобным, то говорят, что оно бессмысленно. Поэтому понятие выполнимого множества предложений является математическим определением содержательно правильного рассуждения.

В этом отношении понятие непротиворечивого множества предложений является математическим определением формально правильного рассуждения. Действительно, если в процессе некоторого рассуждения S получено противоречие $(A \wedge \bar{A})$, то это рассуждение считается неправильным. А если же рассуждение непротиворечиво, то естественно считать его правильным, т.е. что-то означающим.

Например, многочисленные попытки вывести постулат Евклида о параллельных прямых из остальных аксиом геометрии привели к созданию неевклидовой геометрии. Н.И. Лобачевский предположил, что через точку, не лежащую на прямой, можно провести несколько прямых линий, параллельных данной прямой. Опираясь на это предположение, Лобачевский стремился получить противоречие. Но не смотря на огромные усилия, ему не удалось получить противоречие. Тогда Лобачевский сделал заключение, что аксиомы геометрии с измененным постулатом о параллельных прямых образуют непротиворечивое множество суждений, а соответствующую им геометрию назвал "воображаемой". Позднее были построены модели "воображаемой" геометрии, и тем самым, рассуждения Лобачевского приобрели определенное содержание. Построение модели доказывало также непротиворечивость аксиом геометрии Лобачевского. Последнее обстоятельство обосновывается следующим утверждением.

ТЕОРЕМА 7. Если множество предложений S выполнимо, то оно непротиворечиво.

Доказательство. Пусть S имеет модель $\langle M, \sigma \rangle$, в которой истинны все предложения из S. Предположим от противного, что S противоречиво, т.е. существует предложение A данной сигнатуры такое, что $S \vdash (A \wedge \bar{A})$.

По теореме 5 из раздела 1 /с.22/ и по теореме 2 из раздела 3/с.55/ все аксиомы ИП являются тождественно истинными и потому истинны в модели $\langle M, \sigma \rangle$. Далее, из доказательства теоремы 4 раздела 1 /с.22/ и из доказательства теоремы 3 раздела 3 /с.56/ видно, что правила вывода МП, $\forall$-пр. и $\exists$-пр., примененные к формулам, тождественно истинным в некоторой модели, дают формулы, снова тождественно истинные в рассматриваемой модели. Предложения из S истинны в модели $\langle M, \sigma \rangle$, следовательно, предложения, выводимые из S, также будут истинными в $\langle M, \sigma \rangle$. В частности: $(A \wedge \bar{A}) = И$ в $\langle M, \sigma \rangle$. Но это противоречит теореме 1 из раздела 3 /с.53/. Теорема доказана.

Таким образом, мы доказали, что содержательное понятие правильности рассуждения полностью согласуется с формальным. Представляет интерес обратная проблема: верно ли, что всякое формально правильное рассуждение является содержательно правильным? Другими словами, верно ли, что каждое непротиворечивое множество предложений выполнимо? Наша дальнейшая цель - доказать, что эта проблема решается положительно. Для этого введем необходимые понятия и докажем вспомогательные факты.

ОПРЕДЕЛЕНИЕ 5. Множество M называется счетным, если существует взаимно однозначное соответствие между M и множеством натуральных чисел.

Примером счетного множества может служить любое бесконечное множество целых чисел.

ЛЕММА 1. Если сигнатура σ счетна, то множество всех формул сигнатуры σ также счетно.

Доказательство. Каждая формула исчисления предикатов сигнатуры σ есть конечный набор символов языка /см. с. 49/. Сопоставим символам сигнатуры натуральные числа с помощью следующей функции:

$$g(\neg)=2,\ g(\wedge)=3\quad g(\vee)=5,\ g(\rightarrow)=7,\ g(\forall)=11,\ g(\exists)=13,$$

$$g(()=17,\ g())=19,\ g(a_m)=29+8\cdot m,\ g(,)=23,$$

$$g(x_i)=31+8\cdot i,\ g(P_k^{n_k})=37+8\cdot(2^k 3^{n_k})$$

Теперь произвольной формуле, составленной из некоторых символов $u_1, u_2, \ldots, u_s$ рассматриваемой сигнатуры, сопоставим число

$$2^{g(u_1)}\cdot 3^{g(u_2)}\cdot\ldots\cdot p_s^{g(u_s)},$$

где p_j есть j-ое простое число / $j=1,2,\ldots,s$ /. Это число назовем **номером** данной формулы. При такой нумерации, очевидно, что разные формулы получат разные номера, поэтому формул не более, чем счетное множество. С другой стороны множество всех формул счетной сигнатуры бесконечно, и потому счетно.

Пример 7. Формула $\forall x_1 \exists x_2 P_2^3(x_3, x_2, x_1)$ имеет следующий номер:

$$N=2^{11}\cdot 3^{39}\cdot 5^{13}\cdot 7^{47}\cdot 11^{901}\cdot 13^{17}\cdot 17^{55}\cdot 19^{23}\cdot 23^{47}\cdot 29^{23}\cdot 31^{39}\cdot 37^{19}$$

Доказываемые ниже утверждения выполняются для множеств предложений произвольной сигнатуры σ. Но мы ограничимся рассмотрением только счетных сигнатур, и потому полагаем, что рассматриваемые ниже сигнатуры счетны.

ЛЕММА 2. Пусть $S_0, S_1, S_2, \ldots$ – непротиворечивые множества предложений и $S_0 \subseteq S_1 \subseteq S_2 \subseteq \ldots$ Тогда множество $T=\bigcup_{i=0}^{\infty} S_i$ непротиворечиво.

Доказательство. Предположим, что T противоречиво. Тогда существует такое предложение A, что $T \vdash (A \wedge \bar{A})$. Вывод $(A\wedge\bar{A})$ из T представляет собой конечный набор формул и потому использует конечное число гипотез из T . Все эти гипотезы войдут в некоторое S_i из данной последовательности, и потому $S_i \vdash (A \wedge \bar{A})$, что противоречит непротиворечивости множества S_i . Лемма доказана.

ЛЕММА 3. Если S непротиворечивое множество предложений и A произвольное предложение, то хотя бы одно из множеств $S \cup \{A\}$, $S \cup \{\bar{A}\}$ является непротиворечивым.

Доказательство. Допустим, что оба множества $S \cup \{A\}$, $S \cup \{\bar{A}\}$ противоречивы. Тогда существуют такие предложения B и C , что $S, A \vdash (B \wedge \bar{B})$; $S, \bar{A} \vdash (C \wedge \bar{C})$. Согласно примеру 6 на с.38: $(B \wedge \bar{B}) \vdash (C \wedge \bar{C})$. Из приведенных соотношений по правилу силлогизма получаем: $S, A \vdash (C \wedge \bar{C})$ и $S, \bar{A} \vdash (C \wedge \bar{C})$. Отсюда по правилу удаления $\vee$: $S, (A \vee \bar{A}) \vdash (C \wedge \bar{C})$. Но $(A \vee \bar{A})$ доказуема в ИП, следовательно, $S \vdash (C \wedge \bar{C})$, что противоречит непротиворечивости S .

ОПРЕДЕЛЕНИЕ 8. Множество предложений T сигнатуры σ называется полным в σ , если для каждого предложения A сигнатуры σ выполняется: $T \vdash A$ или $T \vdash \bar{A}$.

ТЕОРЕМА ЛИНДЕНБАУМА. Всякое непротиворечивое множество предложений S содержится в непротиворечивом и полном множестве T сигнатуры σ .

Доказательство. Пусть S непротиворечивое множество предложений сигнатуры σ ; занумеруем все предложения сигнатуры σ :

$$A_1, A_2, \ldots, A_n, A_{n+1}, \ldots \quad . \qquad (3)$$

Используя эту нумерацию, построим последовательность множеств

$$S_0, S_1, \ldots, S_n, S_{n+1}, \ldots , \qquad (4)$$

которая даст искомое множество $T = \bigcup_{n=0}^{\infty} S_n$.

а/. $S_0 = S$.

б/. Пусть S_n определено, тогда полагаем:

$$S_{n+1} = \begin{cases} S_n \cup \{A_{n+1}\}, & \text{если } S_n \cup \{A_{n+1}\} \text{ непротиворечиво,} \\ S_n \cup \{\bar{A}_{n+1}\}, & \text{в остальных случаях.} \end{cases}$$

Каждое множество S_n / $n > 0$ / получается из предыдущего S_{n-1} добавлением одного из предложений A_n или $\bar{A}_n$. Поэтому $S_0 \subseteq S_1 \subseteq \ldots \subseteq S_n \subseteq S_{n+1} \subseteq \ldots$ для каждого n : $A_n \in S_n$ или $\bar{A}_n \in S_n$.

Докажем, что S_n непротиворечивы. а/. $S_0 = S$ непротиворечиво по условию.

б/. Предположим, что S_n непротиворечиво и рассмотрим S_{n+1}. Если $S_n \cup \{A_{n+1}\}$ непротиворечиво, то $S_{n+1} = S_n \cup \{A_{n+1}\}$ тоже непротиворечиво. Если же $S_n \cup \{A_{n+1}\}$ противоречиво, то по лемме 3 $S_n \cup \{\bar{A}_{n+1}\}$ непротиворечиво, а в этом случае $S_{n+1} = S_n \cup \{\bar{A}_{n+1}\}$, и потому оно непротиворечиво.

Таким образом, (4) удовлетворяет условию леммы 2, и тогда множество $T = \bigcup_{n=0}^{\infty} S_n$ искомое. Действительно, во-первых, оно непротиворечиво, и во-вторых, оно полно в σ: каждое предложение A сигнатуры σ совпадает с некоторым предложением A_n из (3), и поэтому $A \in S_n$ или $\bar{A} \in S_n$. Это влечет: $A \in T$ или $\bar{A} \in T$, следовательно, $T \vdash A$ или $T \vdash \bar{A}$. Теорема доказана.

4. Теорема Геделя.

<u>ТЕОРЕМА ГЕДЕЛЯ</u>. Если множество предложений S непротиворечиво, то оно выполнимо.

Доказательство теоремы мы разбиваем на три части: в первой части строится специальное множество предложений T, содержащее S; во второй части доказывается, что это множество T непротиворечиво и полно в данной сигнатуре; в третьей части строится модель, в которой истинны все предложения из множества T и, в частности, в этой модели истинны предложения из S. Это и завершает доказательство теоремы.

1. <u>Построение множества T</u>. Пусть S непротиворечивое множество сигнатуры σ. Добавим к σ счетное множество символов констант, не встречавшихся в S: $M = \{c_0, c_1, \ldots, c_m, \ldots\}$. Сигнатура $\sigma' = \sigma \cup M$ будет содержательнее, чем σ, и потому множество формул сигнатуры σ' будет содержать все формулы сигнатуры σ и кроме того, - всевозможные формулы вида:

$$A(c_1, \ldots, c_i, x_{i+1}, \ldots, x_n),$$

которые получаются из некоторых формул прежней сигнатуры σ заменой свободных переменных символами констант из M. Сигнатура σ' счетна, и мы можем занумеровать все предложения сигнатуры σ' в следующую последовательность:

$$A_1, A_2, \ldots, A_n, \ldots \qquad (5)$$

Искомое множество T будет полным в сигнатуре σ' и его построение аналогично конструкции в теореме Линденбаума. Индукцией по n строим следующую последовательность множеств предложений:

$$S_0, S_1, \ldots, S_n, \ldots \qquad (6)$$

1/. $S_0 = S$;

2/. Предположим, что S_n построено. Тогда S_{n+1} определяется следующим образом:

а/ Если $S_n \cup \{A_{n+1}\}$ непротиворечиво, и A_{n+1} не начинается с квантора $\exists$, то $S_{n+1} = S_n \cup \{A_{n+1}\}$

б/ Если $S_n \cup \{A_{n+1}\}$ непротиворечиво и для некоторой формулы $B(x)$ $A_{n+1} = \exists x\, B(x)$, то $S_{n+1} = S_n \cup \{A_{n+1}\} \cup \{B(C_{i_n})\}$,

где C_{i_n} – первый символ константы из M, который не входит в $S_n \cup \{A_{n+1}\}$.

в/ Если $S_n \cup \{A_{n+1}\}$ противоречиво, то $S_{n+1} = S_n \cup \{\bar{A}_{n+1}\}$.

Теперь искомое множество T полагаем равным $T = \bigcup\limits_{n=0}^{\infty} S_n$.

2. Непротиворечивость и полнота множества T. По построению каждое множество S_n $(n > 0)$ получается из предыдущего добавлением некоторых предложений сигнатуры σ', среди которых едино предложение A_n или $\bar{A}_n$. Поэтому $S_0 \subseteq S_1 \subseteq \ldots \subseteq S_n \subseteq \ldots$ и для каждого n: либо $A_n \in S_n$, либо $\bar{A}_n \in S_n$. Покажем, что S_n непротиворечивы.

1/. $S_0 = S$ непротиворечиво по условию.

2/. Предположим, что S_n непротиворечиво и рассмотрим S_{n+1}.

По лемме 3: $S_n \cup \{A_{n+1}\}$ или $S_n \cup \{\bar{A}_{n+1}\}$ непротиворечивое множество.

в/. Если $S_n \cup \{A_{n+1}\}$ противоречиво, то $S_n \cup \{\bar{A}_{n+1}\}$ непротиворечиво, в этом случае $S_{n+1} = S_n \cup \{\bar{A}_{n+1}\}$, и потому S_{n+1} непротиворечиво.

а/. Если $S_n \cup \{A_{n+1}\}$ непротиворечиво и A_{n+1} не начинается с квантора $\exists$, то $S_{n+1} = S_n \cup \{A_{n+1}\}$ и также непротиворечиво.

б/. Пусть $S_n \cup \{A_{n+1}\}$ непротиворечиво и $A_{n+1} = \exists x\, B(x)$. Тогда

$$S_{n+1} = S_n \cup \{A_{n+1}\} \cup \{B(c_{i_n})\},$$

где c_{i_n} первый символ константы из M, не входящий в S_n, A_{n+1}. Предположим, что S_{n+1} противоречиво, тогда существует такое предложение $\mathfrak{D}$ сигнатуры σ', что $S_{n+1} \vdash (\mathfrak{D} \wedge \overline{\mathfrak{D}})$. Распишем это соотношение подробнее:

$$S_n,\ A_{n+1},\ B(c_{i_n}) \vdash (\mathfrak{D} \wedge \overline{\mathfrak{D}})$$

Отсюда по правилу контрапозиции: $S_n, A_{n+1}, \overline{(\mathfrak{D} \wedge \overline{\mathfrak{D}})} \vdash \overline{B(c_{i_n})}$ но $\overline{(\mathfrak{D} \wedge \overline{\mathfrak{D}})}$ доказуема в ИП, следовательно: $S_n, A_{n+1} \vdash \overline{B(c_{i_n})}$. Так как c_{i_n} не встречается в S_n, A_{n+1}, то символ c_{i_n} в выводе $\overline{B(c_{i_n})}$ из S_n, A_{n+1} играет пассивную роль в том смысле, что вместо c_{i_n} в этом выводе можно было бы вставить символ переменной t, не встречающейся в S_n, A_{n+1}. В результате был бы получен вывод $\overline{B(t)}$ из S_n, A_{n+1}. Поэтому считаем, что $S_n, A_{n+1} \vdash \overline{B(t)}$, где t не встречается в S_n, A_{n+1}. Применим правило введения $\forall$:

$$S_n, A_{n+1} \vdash \forall t\, \overline{B(t)} \qquad (7)$$

По теореме 5: $\forall t\, \overline{B(t)} \equiv \overline{\exists t\, B(t)}$ и $\exists x\, B(x) \equiv \exists t\, B(t)$. ?

Тогда из (7) и из последних эквивалентностей получаем:

$$S_n, A_{n+1} \vdash \overline{\exists t\, B(t)} \quad \text{и} \quad S_n, A_{n+1} \vdash \exists t\, B(t)$$

Это противоречит тому, что $S_n \cup \{A_{n+1}\}$ непротиворечиво. Таким образом, S_{n+1} непротиворечиво, (6) удовлетворяет условию леммы 2, и множество $T = \bigcup\limits_{n=0}^{\infty} S_n$ будет непротиворечивым. Кроме того, каждое предложение A сигнатуры σ' совпадает с некоторым предложением A_n из (5), и поэтому $A_n \in T$ или $\overline{A_n} \in T$. Это влечет: $T \vdash A$ или $T \vdash \overline{A}$, т.е. T полно в сигнатуре σ'.

3. <u>Построение модели</u> $\langle M, \sigma' \rangle$. В качестве основного множества возьмем $M = \{c_0, c_1, \ldots, c_m, \ldots\}$. Предикатные символы $\langle P_1^{n_1}, P_2^{n_2}, \ldots \rangle$ из σ интерпретируются на M следующим образом:

для каждого j и произвольных $c_{i_1}, \ldots, c_{i_k} \in M$

$$P_j^k(c_{i_1}, \ldots, c_{i_k}) = \begin{cases} И, & \text{если } T \vdash P_j^k(c_{i_1}, \ldots, c_{i_k}), \\ Л, & \text{если } T \vdash \overline{P_j^k}(c_{i_1}, \ldots, c_{i_k}). \end{cases}$$

Так как множество T непротиворечиво и полно в σ', то либо

$T \vdash P_j^k(c_{i_1}, \dots, c_{i_k})$, либо $T \vdash \overline{P_j^k}(c_{i_1}, \dots, c_{i_k})$, а это означает, что либо $P_j^k(c_{i_1}, \dots, c_{i_k}) = И$, либо $\overline{P}_j^k(c_{i_1}, \dots, c_{i_k}) = И$, т.е. данная интерпретация корректна. Покажем, что в полученной модели $\langle M, \sigma' \rangle$ истинны все предложения множества T . Для этого докажем, что для любого предложения A сигнатуры σ' верно:

$$A = И \longleftrightarrow T \vdash A$$

Доказательство будем вести индукцией по длине построения A .

1/. Пусть A атомная формула : $A = P_j^k(c_{i_1}, \dots, c_{i_k})$. Тогда согласно интерпретации предикатных символов имеем:

$$A = И \longleftrightarrow P_j^k(c_{i_1}, \dots, c_{i_k}) = И \longleftrightarrow T \vdash P_j^k(c_{i_1}, \dots, c_{i_k}),$$

т.е. A удовлетворяет (8).

2/. Предположим, что предложения B и C удовлетворяют соотношению (8), т.е.

$$B = И \longleftrightarrow T \vdash B \qquad (9)$$

$$C = И \longleftrightarrow T \vdash C \qquad (10)$$

Рассмотрим предложение A , имеющее один из следующих видов:

$$\overline{B}, \quad (B \wedge C), \quad (B \vee C), \quad (B \to C).$$

1-й случай: $A = \overline{B}$. T - непротиворечивое множество, поэтому если $T \vdash \overline{B}$, то B не выводимо из T , а так как B удовлетворяет (9), то $B = Л$. Тогда $\overline{B} = И$ в M .

Обратно, если $\overline{B} = И$, то $B = Л$ и в силу предположения (9) B не выводимо из T . В силу полноты T имеем: $T \vdash \overline{B}$. Таким образом, $A = \overline{B}$ удовлетворяет (8).

2-й случай: $A = (B \wedge C)$ Если $T \vdash (B \wedge C)$, то по правилу удаления $\wedge$ имеем: $T \vdash B$ и $T \vdash C$. Тогда по предположению $(9), (10)$: $B = И$ и $C = И$, т.е. $A = (B \wedge C) = И$.

Обратно, если $(B \wedge C) = И$, то $B = И$ и $C = И$, в силу $(9), (10)$: $T \vdash B$ и $T \vdash C$. Отсюда по правилу введения $\wedge$: $T \vdash (B \wedge C)$. Таким образом, для $A = (B \wedge C)$ выполняется (8).

3-й случай: $A = (B \vee C)$. Если $(B \vee C) = И$, то $B = И$ или $C = И$. Тогда по предположению $(9), (10)$: $T \vdash B$ или $T \vdash C$. Но в обоих случаях по правилу введения $\vee$ выполняется: $T \vdash (B \vee C)$.

Обратно, пусть $T \vdash (B \vee C)$ и от противного $(B \vee C) = \text{Л}$. Тогда $B = \text{Л}$ и $C = \text{Л}$, отсюда в силу (9), (10) : B и C не выводимы из T . Но так как T полно в G', то $T \vdash \bar{B}$ и $T \vdash \bar{C}$. Отсюда по правилу введения $\wedge$: $T \vdash (\bar{B} \wedge \bar{C})$, что $(\bar{B} \wedge \bar{C}) \vdash (\overline{B \vee C})$, следовательно: $T \vdash (\overline{B \vee C})$ - это невозможно, ибо T непротиворечиво.

Таким образом, $A = (B \vee C)$ удовлетворяет (8).

<u>4-й случай:</u> $A = (B \to C)$. Если $(B \to C) = \text{И}$, то $B = \text{Л}$ или $C = \text{И}$. Если $B = \text{Л}$, то в силу (9) B не выводимо из T и , следовательно, $T \vdash \bar{B}$. Отсюда по правилу введения $\vee$: $T \vdash (\bar{B} \vee C)$. Но $(\bar{B} \vee C) \vdash (B \to C)$, и потому $T \vdash (B \to C)$. Пусть $C = \text{И}$, тогда из (9) получим: $T \vdash C$. Из последнего по правилу введения $\vee$ имеем: $T \vdash (\bar{B} \vee C)$, и аналогично предыдущему рассуждению получаем: $T \vdash (B \to C)$. Таким образом, в обоих случаях $T \vdash (B \to C)$.

Обратно, пусть $T \vdash (B \to C)$, и предположим, что $(B \to C) = \text{Л}$. Тогда $B = \text{И}$ и $C = \text{Л}$, и в силу предположения (9), (10) : $T \vdash B$ и C не выводимо из T . Последнее влечет $T \vdash \bar{C}$. Применяя правило введения $\wedge$, получим $T \vdash (B \wedge \bar{C})$. Что $(B \wedge \bar{C}) \vdash (\overline{B \to C})$, отсюда следует, что $T \vdash (\overline{B \to C})$, а это противоречит $T \vdash (B \to C)$. Поэтому $(B \to C) = \text{И}$ и $A = (B \to C)$ удовлетворяет (8).

3/. Пусть $B(x)$ содержит одну переменную x и для каждого $c \in M$ предложение $B(c)$ удовлетворяет (8), т.е.

$$B(c) = \text{И} \longleftrightarrow T \vdash B(c) \qquad (11)$$

Рассмотрим предложения вида $\exists x\, B(x)$ и $\forall x\, B(x)$.

<u>5-й случай:</u> $A = \exists x\, B(x)$. Пусть $T \vdash \exists x\, B(x)$, тогда A совпадает с некоторой формулой A_n из (5) и при этом $S_n = S_{n-1} \cup \{A_n\} \cup \{B(c)\}$, где c - некоторый символ из M . Это означает, что $B(c) \in T$, и потому $T \vdash B(c)$, тогда в силу предположения (11) : $B(c) = \text{И}$. Последнее влечет: $\exists x\, B(x) = \text{И}$.

Обратно, пусть $\exists x\, B(x) = \text{И}$. Тогда для некоторого $c \in M$: $B(c) = \text{И}$ и по предположению $T \vdash B(c)$. Применяя правило введения $\exists$: $B(c) \vdash \exists x\, B(x)$, получим $T \vdash \exists x\, B(x)$. Следовательно, $A = \exists x\, B(x)$ удовлетворчет (8).

4-й случай: $A = \forall x\, B(x)$. Пусть $T \vdash \forall x\, B(x)$ и $\forall x\, B(x) = Л$ в M. Тогда для некоторого $c \in M$: $B(c) = Л$ и в силу (11) : $T \vdash \overline{B(c)}$.

c – символ константы, и потому в формуле $\overline{B(x)}$, получаемой из $\overline{B(c)}$ заменой c на x, отсутствуют кванторы по c. Это значит, что c свободна для x в $\overline{B(x)}$. По правилу введения $\exists$: $\overline{B(c)} \vdash \exists x\, \overline{B(x)}$. Тогда отсюда и из предыдущего соотношения получаем: $T \vdash \exists x\, \overline{B(x)}$. По теореме 1 из 2 имеем: $\exists x\, \overline{B(x)} \vdash \overline{\forall x\, B(x)}$, и поэтому $T \vdash \overline{\forall x\, B(x)}$, что противоречит предположению $T \vdash \forall x\, B(x)$. Следовательно, $\forall x\, B(x) = И$.

Обратно, пусть $\forall x\, B(x) = И$ и $\forall x\, B(x)$ не выводима из T. В силу полноты множества T : $T \vdash \overline{\forall x\, B(x)}$. По теореме 5: $\overline{\forall x\, B(x)} \vdash \exists x\, \overline{B(x)}$. Из этих соотношений по правилу силлогизма получаем: $T \vdash \exists x\, \overline{B(x)}$. Последняя формула является предложением данной сигнатуры и потому имеет некоторый номер в (5) : $A_n = \exists x\, \overline{B(x)}$. Рассмотрим соответствующее множество S_n из (6). По построению $S_n = S_{n-1} \cup \{A_n\} \cup \{\overline{B(c)}\}$, где $c \in M$. Тогда $\overline{B(c)} \in T$ и потому $T \vdash \overline{B(c)}$. Отсюда в силу непротиворечивости T следует: $B(c)$ не выводима из T. Тогда по предположению (11) : $B(c) = Л$, что противоречит допущению $\forall x\, B(x) = И$. Полученное противоречие доказывает, что $T \vdash \forall x\, B(x)$.

Соотношение (8) доказано, из него следует, что любое предложение из T истинно в $\langle M, \sigma' \rangle$, так как оно выводимо из T. Теорема доказана.

Произвольная формальная система помимо логических аксиом содержит нелогические аксиомы. Например, аксиомы геометрии описывают свойства геометрических фигур, аксиомы алгебры описывают свойства алгебраических операций и отношений, аксиомы математического анализа описывают свойства действительных чисел и функций, и т.д. Но все логические рассуждения в таких системах осуществляются в рамках исчисления предикатов или логики предикатов. Тем самым, формулы исчисления предикатов охватывают всевозможные схемы рассуждений в формальных системах, а доказуемые фор[мулы] ИП охватывают всевозможные схемы правильных рассуждения. Возникает вопрос: достаточно ли средств исчисления предикатов для того, чтобы доказать любое утверждение, которое вытекает из данной системы аксиом? Эта проблема носит название проблемы полноты исчисления предикатов.

ТЕОРЕМА О ПОЛНОТЕ. Предложение $\mathcal{A}$ доказуемо в ИП тогда и только тогда, когда $\mathcal{A}$ тождественно истинно.

Доказательство. Если $\mathcal{A}$ доказуемо в ИП, то оно получается из аксиом с помощью правил вывода. Как отмечалось в доказательстве теоремы 7, аксиомы ИП являются тождественно истинными, и правила вывода не выводят нас за пределы тождественно истинных формул. Поэтому доказуемые формулы суть тождественно истинные.

Обратно, пусть $\mathcal{A}$ тождественно истинное предложение, тогда $\bar{\mathcal{A}}$ является тождественно ложным предложением, и следовательно: множество предложений $\{\bar{\mathcal{A}}\}$ не может быть выполнимым. Тогда по теореме Геделя $\{\bar{\mathcal{A}}\}$ не может быть непротиворечивым, ибо в противном случае $\{\bar{\mathcal{A}}\}$ было бы выполнимым. Следовательно, $\{\bar{\mathcal{A}}\}$ противоречиво, и потому существует B такое, что $\bar{\mathcal{A}} \vdash (B \wedge \bar{B})$. Применяя правило контрапозиции, получим $\overline{(B \wedge \bar{B})} \vdash \mathcal{A}$. Но $\overline{(B \wedge \bar{B})}$ доказуема в ИП, следовательно, $\mathcal{A}$ доказуемо в ИП. Теорема доказана.

Предыдущие теоремы являются основными теоремами теории моделей. Более того, они были первыми крупными теоремами теории моделей. Кроме них мы докажем еще две важные теоремы этой теории. Каждая из этих теорем была получена в свое время независимо от теоремы Геделя, и каждая из них обогатила математическую логику ценными методами доказательств, позволившими в дальнейшем получить ряд крупных результатов. В данном курсе мы сводим доказательства этих теорем к теореме Геделя.

ТЕОРЕМА ЛЕВЕНГЕЙМА-СКОЛЕМА. Если множество предложений S имеет модель, то оно имеет счетную модель.

Доказательство. Если S имеет модель, то по теореме 7 оно непротиворечиво. Тогда к S применим конструкцию теоремы Геделя и получим модель $\langle M, \sigma' \rangle$ для S, в которой основное множество M счетно.

ЛОКАЛЬНАЯ ТЕОРЕМА А.И.МАЛЬЦЕВА. Пусть S множество предложений, и каждое его конечное подмножество имеет модель. Тогда всё множество S имеет модель.

Доказательство. Пусть каждое конечное подмножество $S_1 \subseteq S$ имеет модель. Тогда каждое такое S_1 непротиворечиво. Предположим, что само множество S противоречиво и потому существует B такое, что $S \vdash (B \wedge \bar{B})$. Вывод $(B \wedge \bar{B})$ из S содержит конечное число гипотез из S. Обозначим это множество гипотез через S_1. Тогда $S_1 \vdash (B \wedge \bar{B})$, но это противоречит условию теоремы. Полученное противоречие доказывает, что S непротиворечиво. Тогда по теореме Геделя S имеет модель. Теорема доказана.

Раздел 5. Элементы теории алгоритмов.

Центральным понятием современной математики является понятие алгоритма. Начиная с древнейших времен, алгоритмами называют определенные процедуры или наборы правил и инструкций, механическое выполнение которых позволяет решить любую задачу некоторого данного класса. Класс задач, для которого подобные процедуры существуют, называется алгоритмически разрешимым или просто разрешимым. Проблема разыскания алгоритма называется алгоритмической проблемой или проблемой разрешимости для этого класса задач. Например, существует процедура нахождения наибольшего общего делителя двух натуральных чисел a, b / Н.О.Д. (a, b) /, называемая алгоритмом Евклида. Она заключается в выполнении следующей последовательности делений:

1/. Пусть $a > b$, тогда делим a на b и находим остаток r_1. Если $r_1 = 0$, то $b = $(Н.О.Д. (a, b))

2/. Пусть $r_1 > 0$, тогда делим b на r_1 и находим остаток r_2. Если $r_2 = 0$, то $r_1 = $(Н.О.Д. (a, b))

3/. Пусть $r_2 > 0$, тогда делим r_1 на r_2 и т.д.

Процедура прекращается как только некоторый остаток окажется равным 0, при этом последний делитель является искомым Н.О.Д. (a, b).

Из других числовых алгоритмов укажем еще алгоритмы разложения натурального числа на простые множители, алгоритм извлечения квадратного корня, алгоритмы распознавания делимости чисел на 2,3,4,5, и. В предыдущих главах нами рассматривались некоторые процедуры, которые также являются алгоритмами для решения определенных задач математической логики. Например, в доказательстве теоремы 6 раздела 1 был описан алгоритм построения СДНФ и СКНФ для формул алгебры высказываний. Метод построения сокращенных таблиц истинности /с. 27/ является одним из алгоритмов упрощения формул алгебры высказываний. В конце раздела 2 указан алгоритм, позволяющий выяснить "является ли доказуемой данная формула A исчисления высказываний".

В этих примерах мы имеем уже готовые алгоритмы, и нам остается только проверить их правильность. Но в тех случаях, когда искомый алгоритм не удается построить, возникает вопрос: существует ли вообще данный алгоритм? Например, существует ли алгоритм, позволяющий выяснить доказуемость или недоказуемость данной формулы исчисления предикатов?

Чтобы ответить на этот вопрос, мы должны иметь строгое математическое определение алгоритма. Приведенное в начале главы определение этого понятия не является точным математическим определением, оно лишь поясняет содержание алгоритма. Поэтому в тридцатых годах нашего века производится анализ понятия алгоритма, и в работах Геделя, Черча, Клини, Тьюринга, Поста и несколько позже в работах Маркова разрабатываются различные математические определения алгоритма. В дальнейшем оказалось, что эти определения описывают один и тот же класс алгоритмических процедур. Это обстоятельство позволяет считать, что мы действительно имеем математические определения алгоритма. В данном разделе мы рассматриваем строгое определение алгоритма, данное в терминах "машин Тьюринга".

1. Машина Тьюринга.

Машина Тьюринга представляет собой абстрактную вычислительную машину, состоящую из конечной ленты, читающей головки, управляющего устройства и конечной программы.

Конечная лента разбита на одинаковые ячейки, в каждой ячейке может быть записан один символ из данного конечного множества $A = \{a_1, \ldots, a_m\}$. Это множество называется внешним алфавитом, сама лента часто называется внешней памятью. Для удобства описания мы считаем, что пустые ячейки содержат "пустой символ" – " Λ ", который включаем в алфавит каждой машины Тьюринга.

В каждый момент времени на ленте записано конечное число символов алфавита, включая пустой символ:

Λ	a_{i_1}	a_{i_2}	a_{i_3}	Λ	Λ	a_{i_4}	a_{i_5}	a_{i_6}	a_{i_4}	Λ	Λ	Λ

но в процессе работы машина может неограниченно достраивать пусть
ячейки с левого и правого краев ленты, - мы говорим, что лента
потенциально неограничена в обе стороны.

Читающая головка - это некоторое устройство, которое может перемещаться вдоль ленты так, что в каждый дискретный момент времени $t = 0, 1, 2, \ldots$ оно обозревает определенную ячейку. Читающая голов[ка в] каждый момент находится в некотором внутреннем состоянии. Число в[нут]ренних состояний конечно, их множество $Q = \{q_0, q_1, \ldots, q_n\}$ называется внутренним алфавитом или внутренней памятью.

$\boxed{q_j}$

Λ	Λ	Λ	a_{i_1}	a_{i_2}	a_{i_3}	a_{i_4}	Λ	Λ	Λ	Λ	Λ	Λ

Одно из внутренних состояний объявляется заключительным. Условимся в дальнейшем обозначать заключительное состояние символом « ! ».

Управляющий механизм на каждом такте работы в зависимости от символа обозреваемой ячейки и от внутреннего состояния головки может одновременно выполнять следующие операции:

а/ стереть символ обозреваемой ячейки и записать вместо него друг[ой] символ из внешнего алфавита,

б/ изменить внутреннее состояние головки на любое состояние внутреннего алфавита,

в/ сдвинуть головку вправо или влево на одну ячейку. Если при э[том] головка находилась на краю ленты, то при соответствующем сдвиге [она] автоматически достраивает одну пустую ячейку. Если головка прихо[дит в] заключительное состояние « ! », то управляющий механизм останавл[и]вает работу машины. Если же головка никогда не приходит в заключи[тель]ное состояние, то считается, что машина работает бесконечно.

Программа машины Тьюринга представляет собой конечный набор команд следующего вида

$$q_j a_i \longrightarrow a_r q_s, \quad q_j a_i \longrightarrow a_r q_s R, \quad q_j a_i \longrightarrow a_r q_s L$$

при этом программа не содержит различных команд с одинаковыми ле[выми] частями $q_j a_i$.

каждая такая команда означает, что если читающая головка машины находится в состоянии q_j и обозревает символ a_i, то в следующий момент времени головка переходит в состояние q_s и изменяет символ a_i на a_r; если же команда содержит символы R или L, то дополнительно головка сдвигается соответственно вправо или влево на одну ячейку. Мы говорим, что машина Тьюринга выполнила один такт работы. Условимся программу машины Тьюринга записывать в виде следующей таблицы:

	q_0	q_1	q_2	.	q_n
a_0					
a_1					
a_m					$a_r q_s R$
Λ					

В такой таблице, если программа машины содержит команду $q_j a_i \to a_r q_s R$, то на пересечении столбца q_j и строки a_i записывается $a_r q_s R$.

Пусть в ячейках машины M записаны символы $a_{i_1}, a_{i_k}, \dots, a_{i_l}$, включая пустой символ; читающая головка находится в состоянии q_j и обозревает ячейку с номером k. Тогда слово

$$a_{i_1} a_{i_2} \dots q_j a_{i_k} \dots a_{i_l} \qquad (1)$$

называется машинным словом или состоянием машины M. Предполагается, что мы можем любую машину M с соответствующим алфавитом привести в любое состояние вида (1) и запустить работать. Работа M будет заключаться в переходе из одного состояния в другое согласно своей программе.

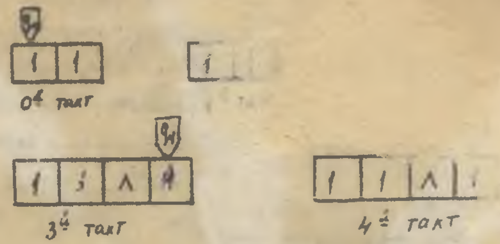
Пример 1. Пусть машина M_1 имеет внешний алфавит $A=\{\Lambda, 1\}$, внутренний алфавит $Q=\{q_0, q_1, !\}$ и программу:

M_1	q_0	q_1
Λ	$\Lambda q_1 R$	$1\,!$
1	$1 q_0 R$	$1 q_1 R$

Тогда если в начальный момент / 0-й такт / на ленте M_1 запи-

… головк…

…жет происходить следу…



Пример 2. Следующая машина Тьюринга M_2 переводит унарн…

число n в десятичную:

$A = \{\Lambda, 1, 0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$

$Q = \{q_0, q_1, q_2, !\}$

M_2	q_0	[illegible]	[illegible]
1	$\Lambda q_1 L$	$1 q_1 L$	
Λ		$1 q_2$	$\Lambda q_0 L$
0	!	[illegible] $q_2 R$	$0 q_2 R$
1	!	[illegible] $q_2 R$	$1 q_2 R$
2	!	$3 q_2 R$	$2 q_2 R$
3	!	$4 q_2 R$	$3 q_2 R$
4	!	$5 q_2$ [illegible]	$4 q_2 R$
5	!	$6 q_2$ [illegible]	$5 q_2 R$
6	!	$7 q_2 R$	$6 q_2 R$
7	!	$8 q_2 R$	$7 q_2 R$
8		$9 q$ [illegible]	$8 q_2 R$
9		$0 q$ [illegible]	9 [illegible] R

Если на ленте машины M_2 запи… …ряд n … …ка в сос…янии q_0 обозревает …йнюю правую палочку, конечн… число тактов запишет число n в де…

Например, при $n = 5$ работа M_2 …