Хаханян Валерий Христофорович

Элементы математической логики и теории алгоритмов

Учебное пособие

Предисловие

Данное учебное пособие имеет целью обеспечение учебной литературой курса «Математическая логика и теория алгоритмов», читаемого для специальности АКБ в IV семестре.Пособие состоит из введения и 4-х глав, в которые входят основные понятия математической логики: классические логика высказываний и логика предикатов с элементами теории моделей и теории доказательств и введение в теорию рекурсивных функций. Ряд необходимых фактов из других разделов математической логики упоминается лишь эпизодически.

Необходимость написания данного пособия вызвана тем, что достаточно богатая литература по математической логике содержит изучаемые сведения в разбросанном для курса виде (переводные учебники совсем не учитывают специфики и часов читаемого курса, отечественные же учебники и пособия не согласуются с часами, выделенными на изучение курса, т.к. их изложение рассчитано в первую очередь на на университеты и пединституты и также плохо соответствует программе читаемого курса). Всё это

вызывает серьёзные трудности у студентов специальности АКБ при изучении данного курса, вызванные ещё дополнительно и тем, что учебной литературы по математической логике в БУПе в достаточном количестве не имеется, а литература (тоже достаточно редкая по комплектации) из основных фондов могла бы служить лишь в качестве дополнительной при изучении курса, т.к. выдаётся на очень короткий для пользования срок.

Пособие сопровождается методической литературой по решению задач по данному курсу. Большое количество задач приводится прямо в тексте пособия. При написании пособия были использованы: учебник (переводной) Э.Мендельсона «Введение в математическую логику», М., Наука,1971г., «Вводный курс математической логики», изданный в 1991 г. в МГУ им. Ломоносова, авторы В.А.Успенский, Н.К.Верещагин, В.Е.Плиско, также переводная книга Р.Столла «Множества. Логика. Аксиоматические теории», М., Просвещение, 1968 г., учебное пособие Ю.М.Важенина «Множества. Логика. Алгоритмы», изданное в 1995 г. в УрГУ г. Екатеринбурга и замечательная книга Н.К.Верещагина и А.Шеня «Языки и исчисления», издание МЦНМО второе, стереотипное, 2002 г.

Введение

Скорее всего, логику можно определить как анализ правильных методов и способов рассуждений, т.е. когда из верных исходных положений получаются верные же выводы (при этом мы совершенно не поясняем термин «верный»?!). Логика, таким образом, интересуется в первую очередь только формой, а не содержанием используемых доводов. В качестве примеров можно привести конкретные рассуждения по одному из известных силлогизмов Аристотеля: а) все люди смертны; Сократ – человек; следовательно, Сократ смертен.; б) все кошки любят рыбу; Ряба – кошка; следовательно, Ряба любит рыбу. Приведённые рассуждения характеризуются одной и той же формой: все А суть В; С есть А; следовательно, С есть В. При этом удалось установить некий общий закон получения из верных посылок верного заключения. И если при таком получении (установлении) мы используем математический аппарат, то предмет такого рода изучения и может быть назван математической логикой.

Логика, безусловно, является одним из основных

элементов всех других наук (ситуация по выделению логики именно как единственной основы не верна: конечно, шасси автомобиля – один из его основных элементов, но не его основа (как единственный основной элемент): есть и другие, не менее основные, элементы автомобиля). Современная математическая логика, наряду с присущей ей фундаментальностью – обширный и разветвлённый раздел именно математики. Математическая логика должна быть, как и сама математика, точной наукой: иметь дело с точными понятиями и методами (здесь стоит отметить, что интерес к математической логике стал особо заметен в XIX столетии под влиянием строгого обоснования математического анализа, открытием неевклидовых геометрий, а затем и парадоксов в основаниях математики (хорошее описание и обсуждение парадоксов можно найти в книге С.К.Клини «Введение в метаматематику», издание 1957 г. и в упоминавнемся учебнике Э.Мендельсона)). В последние десятилетия интерес к математической логике в первую очередь связан с поисками наилучших алгоритмов при решении массовых задач и с программированием. Оставляя в стороне подробное обсуждение обеих тем отметим только, что поиск наилучших алгоритмов невозможен без описания и изучения свойств этих алгоритмов, т.е. без теории рекурсивных (вычислимых) функций.

Собственно курс состоит из трёх основных частей: классической логики высказываний, классической логики предикатов и элементов теории рекурсивных

функций, т.е. теории алгоритмов. При этом, особенно в последней части, ряд положений и фактов или даётся без доказательства или от изучающих изложение такого доказательства не обязательно в первом приближении.

Г Л А В А 1.

Исходные понятия математической логики.

1.1 Язык математической логики.

Основными понятиями математической логики являются высказывания, предикаты, логические связки и кванторы (конечно, мы не даем формального описания какого либо языка, но несколько ниже мы приведём примеры таких языков для исчисления высказываний и исчисления предикатов). Сейчас же мы изложим семантические аспекты понятий выше. Связка $\neg$ («не») называется отрицанием; связка $\wedge$ (иначе &) («и») называется конъюнкцией; связка $\vee$ («или», но не разделительное) называется дизъюнкцией; связка $\rightarrow$ («если…,то…») называется импликацией. Приведём пример. Пусть P – предложение «данное число делится на 2», Q – предложение «данное число делится на 5», R – предложение «данное число оканчивается нулём»; тогда предложение S «если данное число оканчивается нулём, то это число делится на 5 и делится на 2» может быть записано так: S © R $\rightarrow$

(P∧Q). Читатель может потренироваться в приведении примеров, подобных данному.

Аналог понятия предикат есть понятие группы слов, характеризующих некий предмет, т.е. есть сказуемое, характеризующее подлежащее. Здесь часто используется так называемая функциональная запись: $f(x_1, \ldots, x_n)$, где f – обозначение свойства, которым характеризуется набор предметов $x_1, \ldots, x_n$. С этой точки зрения предикат ставит в соответствие элементам $x_1, \ldots, x_n$ символы И (истина) или Л (ложь), которые далее всегда будут заменяться 1 и 0 соответственно. Итак $f : M^n \Rightarrow \{0,1\}$, где M – объектная область, т.е. область, которую «пробегают» переменные $x_1, \ldots, x_n$. Рассмотрим пример: P(x) = «x – пионер» (это – одноместный предикат «быть пионером»). Если данное лицо A является пионером, то P(A) = 1; в противном случае P(A) = 0. В качестве M здесь выступает всё человечество. Другой пример: Q(x,y) = «x делится на y» (в качестве M выступает множество всех натуральных чисел). Теперь Q – двухместный предикат. Если A=28 и B=2, то Q(A,B)=1; если же A=13, а B=4, то Q(A,B)=0. Если мы зафиксируем первую переменную числом 28, то получим предикат Q(28,y)=R(y) и R – уже одноместный предикат, выражающий делимость числа 28 на все остальные числа. Однако есть другой способ получения одних предикатов из других и такой способ связан с применением кванторов. Пусть P(x) и Q(x,y) – рассмотренные выше предикаты. Тогда ∀xP(x) («для всякого x из области M (M – всегда

подразумеваемая область) P(x)=1») и ∃yQ(x,y)=H(x) («для данного x из области M найдётся y из области M такой, что Q(x,y)=1») – новые предикаты (первый из них есть нульместный предикат или просто высказывание), полученные применением кванторов ∀ (для всякого или всеобщности (for all)) и ∃ (существования (exist)) к предикатам P и Q. В первом случае мы получим функцию-константу или высказывание (в нашем случае – ложное), во втором случае – одноместный предикат, который всегда истинен (например, в качестве y нужно просто взять x), а тогда утверждение ∀x∃yQ(x,y) – также истинное утверждение. Думается, что изложенного выше достаточно для уяснения понятия «квантор». Ниже, при изложении исчисления предикатов, мы вернёмся к этому понятию.

Перейдём теперь к более формальному изложению понятия «язык» в математической логике. При введении понятий «высказывание», «связка», «предикат» и «квантор» мы опирались на семантическую сторону или смысл (неточный, вообще говоря) этих понятий. Но теперь мы перейдём к синтаксической (формальной) стороне вопроса.

1.2 Высказывания и высказывательные формы. Логические операции над высказываниями.

В пункте 1.1 мы уже получили представление о логических связках (операторах) и кванторах. Теперь

мы обратимся к высказываниям. Под высказыванием мы понимаем суждение, характеризующееся тем, что оно обязательно является либо истинным, либо ложным (последние слова – это истинностностные значения суждения или высказывания).

Высказывание $7\times3=21$ является истинным (его истинностное значение есть 1), а высказывание $7\times7=47$ – ложным (его истинностное значение есть 0). Однако бывают суждения, которые не являются высказываниями. Например, суждение «натуральное число n, умноженное на 5, всегда оканчивается (в десятичной записи) нулём» является неопределенным в том смысле, что его истинностное значение зависит от того, какое значение принимает натуральное число n, которое в данной записи носит характер переменной. Переменная n принимает значения из вполне определенного множества объектов: натуральных чисел и такая переменная называется «свободная». Но бывают и такие переменные, которые не допускают подстановок описанного рода, например $\sum_{i=1}^{3}(i+1)$ (сравни с действиями кванторов из примеров выше; ещё пример с кванторами: $\neg\exists x(x^2+1=0)$). Такие переменные называют «связанная». Ещё пример связанной переменной: $\int_0^t tdt$; здесь верхнее вхождение переменной t является свободным, а два других вхождения – связанными. Таким образом, нужно говорить не просто о свободных и связанных переменных, а об их

вхождениях в суждение. Итак, наряду с высказываниями (в которых нет свободных вхождений ни одной переменной) существуют и суждения, в которых есть вхождения свободных переменных. Суждения такого вида называют высказывательными формами.

Задача. Приведите 5 примеров высказываний и 5 примеров высказывательных форм.

Обратимся теперь к введённым выше логическим операциям (связкам); к ним мы ещё добавим логическую операцию (бинарную) «≡» («тогда и только тогда» или «эквиваленция»). Представим сводную логическую таблицу всех введённых операций.

A	B	$A \wedge B$	$A \vee B$	$A \to B$	$A \equiv B$	$\neg A$
1	1	1	1	1	1	0
1	0	0	1	0	0	0
0	1	0	1	1	0	1
0	0	0	0	1	1	1

Эти логические операции можно рассматривать как функции, например, $\wedge$ есть отображение из $\{0,1\}^2$ в $\{0,1\}$. Применять эти операции можно как к высказываниям, так и к высказывательным формам.

Г Л А В А 2.

Классическое исчисление высказываний

2.1 Истинностные таблицы.

Придадим всему сказанному выше более формальное описание. Пропозициональной переменной (пп) называется переменная, пробегающая над множеством высказывательных форм (в том числе и высказываний). Пропозициональная форма (пф) получается с помощью следующего индуктивного определения (математическая логика очень часто использует определения объектов с помощью индуктивной процедуры, часто явно не указывая индуктивную переменную, которая обычно есть натуральное число; доказательства также часто проводятся с использованием математической индукции, с помощью которой уже были построены объекты, являющиеся предметом доказательства; поэтому рекомендуем читателю повторить метод математической индукции):

(i) любая пп есть пф; (ii) если A и B – пф, то $(\neg A)$, $(A \wedge B)$, $(A \vee B)$, $(A \rightarrow B)$, $(A \equiv B)$ есть пф; (iii) только те выражения есть пф, для которых это следует из пунктов (i) и (ii).

Понятно, что любому распределению истинностных значений пп, входящих в ту или иную пф, соответствует некоторое (определяемое с помощью истиностных таблиц) истинностное значение этой пф. Поэтому всякая пф определяет некоторую истинностную функцию и м.б. функционально представлена таблицей. Например, форма $A \vee B \rightarrow C$ может быть представлена такой таблицей:

A	B	C	$A \vee B$	$A \vee B \rightarrow C$

0	0	0	0	1
0	0	1	0	1
0	1	0	1	0
0	1	1	1	1

1	0	0	1	0
1	0	1	1	1
1	1	0	1	0
1	1	1	1	1

Задача. Составьте таблицы истинностных функций для следующих пф: а) $(A \to B) \vee (\neg A)$; в) $((A \to B) \to C) \to D$.

Введём ряд соглашений о более экономном употреблении скобок в записях пф (внимательный читатель уже заметил, что две последних пф записаны неправильно, тем не менее воспринимаются эти записи как правильные). Внешнюю пару скобок в записи будем опускать. Если форма содержит вхождения только одной бинарной связки, то для любого вхождения этой связки опускаем внешние скобки у той из двух форм, соединяемых этим вхождением, которая стоит слева. Далее, связки упорядочим так: $\equiv$, $\to$, $\vee$, $\wedge$, $\neg$ и будем опускать все те пары скобок, без которых возможно восстановление пф по правилу: $\neg$ относится к наименьшей пф, следующей за ним, $\wedge$ связывает наименьшие формы, его окружающие; затем всякое вхождение $\vee$ действует аналогичным образом (но после применения

правила к $\neg$ и $\wedge$ и т.д., включая $\rightarrow$, а затем $\equiv$). Пример: $A\rightarrow B\rightarrow C$ есть $((A\rightarrow B)\rightarrow C)$; $A\vee\neg B\rightarrow C\equiv A$ есть $(((A\vee(\neg B))\rightarrow C)\equiv A)$. Сами потренируйтесь в восстановлении и опускании скобок по правилу, приведённому выше.

Отметим теперь, что если в пф имеется n различных пп, то возможны 2^n различных распределений истинностнх значений для этих пп. Истинностная таблица для пф будет содержать столько же строк. Всего же различных пф, содержащих n пп, может быть только 2^{2^n}.

2.2 Тавтологии.

Пф, которая истинна независимо от того, какие значения принимают входящие в неё пп, называется тавтологией. Таким образом, функция истинности тавтологии принимает только значение 1. Говорят, что A логически влечет B, если пф $A\rightarrow B$ является тавтологией и что A логически эквивалентно B, если пф $A\equiv B$ – тавтология. Каждая тавтология есть пример какого-либо логического закона. Например, $A\vee\neg A$ – закон исключённого третьего, $(A\rightarrow B)\rightarrow(\neg B\rightarrow\neg A)$ – закон контрапозиции и т.д. Отметим еще, что $A\wedge(A\rightarrow B)$ логически влечёт B. Ясно, что таблицы истинностности дают эффективную процедуру для решения вопроса о том, является ли данная пф тавтологией.

Задача. Определить, являются ли следующие пф

тавтологиями.

1. $((A \to B) \to B) \to B$. 2. $(A \equiv B) \equiv (A \equiv (B \equiv A))$.

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

Отрицание тавтологии называется противоречием (т.е., если А – тавтология, то $\neg A$ – противоречие). Ясно, что противоречие есть пф, которой соответствует истинностная, всюду ложная, функция.

Задача. Приведите пять примеров пф, которые являются противоречиями.

Высказывание (в любом естественном языке), которое м.б. получено из какой-либо тавтологии подстановкой любых высказываний вместо входящих в тавтологию пп (при этом, конечно, вместо одной и той же пп подставляется одно и то же высказавание), называется логически истинным и в этом случае истинность этого высказывания связана только с функциональным строением той пф, из которой это высказывание получено. Высказывание, которое получается аналогичным способом, но из противоречия, называется логически ложным. Установим теперь некоторые общие факты о тавтологиях.

Утверждение 2.2.1 Если А и $A \to B$ – тавтологии, то В – тавтология.

Замечание. Вы уже вероятно заметили, что в тексте все время не различаются собственно пп и пф и вместо тех и других используются одни и те же обозначения.

Доказательство: если А и $A \to B$ – тавтологии, то при любом распределении (фиксированном)

истинностных значений входящих в них пп они принимают значение 1. Если бы В принимала при этом значение 0, то пф $A \to B$ принимала бы значение 0 также и мы получаем противоречие.
Следовательно, В принимает значение 1.
Замечание. Не лучшее доказательство. Попробуйте рассудить «более логично».
Утверждение 2.2.2 Если А – тавтология с пп $A_1,\ldots,A_n$ и пф В получается из пф А подстановкой пф $B_1,\ldots,B_n$ вместо пп выше, то пф В – также тавтология (подстановка в тавтологию приводит снова к тавтологии).
Докажите это Утверждение самостоятельно. Приведите подтверждающие и опровергающие примеры (например, может ли быть так, когда в не тавтологию что-то подставляют и получается тавтология?)
Утверждение 2.2.3 Если пф B_1 получается из пф A_1 подстановкой пф В вместо одного или большего числа вхождений пф А, то $(A \equiv B) \to (A_1 \equiv B_1)$ есть тавтология, т.е. из логической эквивалентности пф А и В следует логическая эквивалентность пф A_1 и B_1.
Это Утверждение также докажите самостоятельно. Рассмотрите какое-либо произвольное, но фиксированное, распределение пп, входящих в А и В.

2.3 Полные системы связок

Материал подобного сорта должен быть рассмотрен (обычно) в курсе «Дискретная

математика», но иногда (а раньше – почти всегда) рассматривался и в курсе «Математическая логика». Поэтому мы будем кратки.

Утверждение 2.3.1 Всякая истинностная функция порождается некоторой пф, содержащей только связки $\neg$, $\wedge$, $\vee$. Это верно в силу того факта, что по данной истинностной функции можно написать совершенную конъюнктивную (или дизъюнктивную) нормальную форму (которая и есть требуемая пф).

Следствие 2.3.2 Для любой из трёх пар связок $(\neg,\wedge)$, $(\neg,\vee)$ и $(\neg,\rightarrow)$ и для любой истинностной функции найдётся пф, содержащая только связки из заданной пары и порождающая данную функцию.

Для доказательства достаточно заметить, что любая из связок $\wedge$, $\vee$, $\rightarrow$ выражается через любую из остальных и $\neg$.

Однако можно ввести и одну связку, с помощью которой можно добиться такого же эффекта.

Утверждение 2.3.3 Единственными бинарными связками, каждой из которых достаточно для построения всех истинностных функций, являются связки $\downarrow$ и $|$. Напишем таблицы истинностности для этих связок и предоставим остальное читателю в качестве полезного упражнения.

A	B	$\downarrow$	$\mid$
0	0	1	0
0	1	0	1
1	0	0	1

1 1 0 1

Задача. Доказать, что ни одна из пар связок ($\rightarrow$,$\vee$) и ($\neg$,$\equiv$), не является достаточной для выражения всех истинностных функций.

2.4 Система аксиом для исчисления высказываний

Истинностные таблицы позволяют ответить на очень многие важные вопросы, возникающие в исчислении высказываний. Однако (как, например, в геометрии Евклида) часто недостаточно просто аксиоматизировать тот или иной раздел математики, а необходимо применить метод полной формализации, который поможет ответить на ряд важных вопросов, ответить на которые, не применяя метода полной формализации, не удаётся. Пример применения мы увидим несколько ниже в виде исчисления предикатов, т.к. исчисление высказываний ввиду своей простоты таким примером служить не может. Однако общие черты метода формальных теорий (метаматематики), введённого Д.Гильбертом, опишем сразу и применим этот метод и для исчисления высказываний.

Формальная аксиоматическая теория T задана, если выполнены следующие условия (читатель найдёт в других учебниках несколько иные условия, но все они оказываются «эквивалентными»; в 4-ой части («Элементы теории алгоритмов») можно будет привести другое описание как пример):

а) задано счётное число исходных символов – алфавит теории Т; конечные последовательности (слова) этих символов называются выражениями теории Т;
в) имеется подмножество выражений теории Т, называемых формулами теории Т; часто имеется эффективная (мы уже несколько раз употребили этот термин, не поясняя его и считая его интуитивно понятным) процедура, позволяющая по данному выражению определить, является оно формулой или нет;
с) выделено некоторое множество формул, называемых аксиомами теории Т; здесь также часто имеется эффективная процедура, позволяющая выяснить, является ли данная формула аксиомой (эффективно аксиоматизируемая теория);
d) имеется конечное множество отношений $R_1,\ldots,R_n$ между множествами формулами, называемых правилами вывода; для каждого R_i и для каждого натурального j можно эффективно определить, является данное множество, состоящее из j формул, и данная формула А в отношении R_i, и если да, то формула А называется непосредственным следствием из данных j формул по правилу R_i.

Выводом в теории Т называется любая последовательность формул $A_1,\ldots,A_n$ такая, что для всякого i формула A_i есть либо аксиома теории Т, либо непосредственное следствие каких-либо предыдущих формул по одному из правил вывода.

Формула А есть теорема теории Т, если существует вывод в Т, последней формулой которого

является A; такой вывод называется выводом формулы A в теории T.

Понятие теоремы не обязательно является эффективным (часто, как правило, не является эффективным), даже если сама теория эффективно аксиоматизируема. Если множество теорем является эффективно заданным, то теория T называется разрешимой; в противном случае – неразрешимой. Разрешимая теория такова, что подразумевает существование эффективной процедуры, позволяющей определить по любой формуле, выводима эта формула в T или нет.

Формула A называется следствием в T множества формул Г, если в теории T+Г существует вывод формулы A (теория T+Г получается из теории T добавлением всех формул из Г в виде аксиом). Иногда говорят о выводе в T формулы A из множества формул Г. Члены Г называют гипотезами или посылками. Формальные записи таковы: $\vdash_T A$ – в теории T выводима формула A (формула A есть теорема теории T); $Г \vdash_T A$ – в теории T формула A выводима из множества формул Г (далее индекс T будем часто опускать).

Простейшие свойства выводимости:
а) если $Г \subseteq \Delta$ и $Г \vdash A$, то $\Delta \vdash A$; в) $Г \vdash A$ тогда и только тогда, когда в Г существует конечное подмножество Δ такое, что $\Delta \vdash A$; с) если $\Delta \vdash A$ и $Г \vdash B$ для любого B из Δ, то $Г \vdash A$. Все приведённые свойства имеют простое толкование, связанное с понятием вывода (попробуйте

самостоятельно «перевести» эти свойства на обычный язык).

Теперь мы готовы ввести формальную аксиоматическую теорию L для исчисления высказываний.

1) символами L (далее символ L иногда опускаем) являются $\neg$, $\rightarrow$, (,) и буквы A_i, где индексы есть натуральные числа, A_i – пропозициональные буквы (пб), остальные – примитивные связки (пс) и скобки.

2) а) все пб есть формулы (фл); в) если A и B – фл, то $(\neg A)$ и $(A \rightarrow B)$ – также фл; с) других фл, кроме полученных по пунктам а) и в), нет.

3) следующие фл суть аксиомы теории L:

A1) $(A \rightarrow (B \rightarrow A))$; A2) $((A \rightarrow (B \rightarrow C)) \rightarrow ((A \rightarrow B) \rightarrow (A \rightarrow C)))$; A3) $((\neg B \rightarrow \neg A) \rightarrow ((\neg B \rightarrow A) \rightarrow B))$, где A,B и C – любые фл.

4) правило вывода (modus ponens (MP)): B есть непосредственное следствие A и $A \rightarrow B$.

Замечание. Как всегда, при записи фл будем придерживаться соглашений относительно исключения скобок.

Отметим, что собственно аксиом – бесконечное множество, которое задано с помощью трёх схем аксиом. Наше множество аксиом задано эффективно, т.к. относительно любой формулы можно проверить, является она аксиомой или нет.

Наша цель такова: построить систему L так, чтобы множество её теорем совпадало с классом всех тавтологий. Для этого сначала введём остальные связки таким образом: $(A \wedge B)$ есть $\neg(A \rightarrow \neg B)$;

$(A \vee B)$ есть $(\neg A) \to B$; $(A \equiv B)$ есть $(A \to B) \wedge (B \to A)$.

Приведём пример вывода и его записи в теории L.

Утверждение 2.4.1 Для любой фл A $\vdash_L A \to A$ (далее нижний символ L опускаем).

Построим требуемый вывод:

(1) $(A \to ((A \to A) \to A)) \to ((A \to (A \to A)) \to (A \to A))$ аксиома A2 (какие фл подставлены вместо A,B и C?);

(2) $A \to ((A \to A) \to A)$ аксиома A1 (тот же вопрос);

(3) $(A \to (A \to A)) \to (A \to A)$ из 1 и 2 по MP;

(4) $A \to (A \to A)$ аксиома A4;

(9) $A \to A$ из 3 и 4 по MP. Вывод завершен.

Задача Постройте выводы в L для следующих фл: $(\neg A \to A) \to A$; $A \to C$ из гипотез $A \to B$ и $B \to C$; $B \to (A \to C)$ из гипотезы $A \to (B \to C)$; $(\neg B \to \neg A) \to (A \to B)$.

Теперь докажем одну из важнейших теорем – теорему о дедукции, которая является важным вспомогательным правилом вывода и часто применяется в неформальных математических доказательствах.

2.4.2 Теорема о дедукции. Если Г – множество фл, A и B – фл и $\Gamma, A \vdash B$, то $\Gamma \vdash A \to B$ (Эрбран, 1930 г.).

Доказательство. Пусть $B_1,\ldots,B_n$ – вывод из $\Gamma \cup \{A\}$ и $B=B_n$. Индукцией по длине вывода докажем, что $\Gamma \vdash A \to B$. Основание индукции. Тогда $B=B_1$ есть либо элемент Г, либо B=A, либо B – аксиома. В первом и третьем случаях, используя аксиому $B \to (A \to B)$, получаем $\Gamma \vdash A \to B$ по MP. Во втором случае в силу Утверждения 2.4.1 имеем также $\Gamma \vdash A \to B$ и

основание индукции завершено (более детально проверьте основание). Индукционный шаг. Пусть для всякого $i< n$ наше утверждение доказано, т.е. $\Gamma \vdash A\to B_i$. Для B_n есть четыре возможности: B_n – аксиома, $B_n\in\Gamma$, $B_n=A$ или B_n получено по правилу MP из B_j и B_m, где j и $m < n$, причём B_m имеет вид $B_j\to B_n$. В первых трёх случаях $\Gamma \vdash A\to B$ доказывается так же, как в случае с основанием индукции. В последнем случае применяем индукционное предположение, согласно которому $\Gamma \vdash A\to B_j$, $\Gamma \vdash A\to B_m$, т.е. $\Gamma \vdash A\to(B_i\to B_n)$. По схеме аксиом A2) имеем $\vdash(A\to(B_j\to B_n))\to((A\to B_i)\to(A\to B_n))$. Теперь по правилу MP $\Gamma \vdash (A\to B_j)\to(A\to B_n)$ и снова по MP $\Gamma \vdash(A\to B_n)$. Доказательство индукционного шага и всей теоремы о дедукции завершено. Отметим, что доказательство носит конструктивный характер: оно позволяет по данному выводу B из Γ и A построить вывод $A\to B$ из Γ. Также, при доказательстве были использованы только аксиомы A1) и A2).

Следствие 2.4.3 $A\to B,\ B\to C \vdash A\to C$; $A\to(B\to C),\ B \vdash A\to C$. Докажите Следствие 2.4.3 самостоятельно, используя Теорему о дедукции.

Утверждение 2.4.4 Следующие фл являются теоремами L для любых фл A и B:

(a) $\neg\neg B \to B$; (b) $B \to \neg\neg B$; c) $\neg A\to(A\to B)$;

(d) $(\neg B\to\neg A)\to(A\to B)$; (e) $(A\to B)\to(\neg B\to\neg A)$;

(f) $A\to(\neg B\to\neg(A\to B))$; (g) $(A\to B)\to((\neg A\to B)\to B)$.

(h) $((A\to B)\to A)\to A$; (k) $A\to(B\to(A\wedge B))$.

(вспомните, что пс $\wedge$ есть сокращение!)

Задача. Докажите Утверждение 2.4.4 (т.е. постройте в L соответствующие выводы).

В качестве примера докажем (а):

1)$(\neg B\to\neg\neg B)\to((\neg B\to\neg B)\to B)$ схема аксиом A3) (укажите, что в этой аксиоме есть фл A и фл B);

2) $\neg B\to\neg B$ Утверждение 2.4.1;

3) $(\neg B\to\neg\neg B)\to B$ из 1) и 2), Следствие 2.4.3 (вторая фл);

4) $\neg\neg B\to(\neg B\to\neg\neg B)$ схема аксиом A1);

5) $\neg\neg B \to B$ из 3) и 4), Следствие 2.4.3 (первая фл).

Теперь мы докажем, что фл теории L является теоремой тогда и только тогда, когда эта фл есть тавтология.

Утверждение 2.4.5 Всякая теорема теории L является тавтологией. Мы оставляем доказательство этого Утверждения читателю (нужно убедиться, что любая аксиома есть тавтология и что правило MP по тавтологиям даёт тавтологию, см. Утверждение 2.2.1).

Утверждение 2.4.6 Пусть A – фл и $B_1,\ldots,B_n$ – пб, входящие в A. Пусть задано некоторое распределение истинностных значений для этих пб. Пусть $B_i`$ есть фл $B_i$, если $B_i$ принимает значение 1 и фл $\neg B_i$, если $B_i$ принимает значение 0; пусть A` есть фл A, если при заданном распределении истинностных значений пб фл A принимает значение 1 и $\neg$A, если фл A принимает значение 0.

Тогда $B_1`,\ldots,B_n` \vdash A`$.

Дадим краткое пояснение в виде примера. Пусть фл $A = \neg B_1\to B_2$. Пусть B_1 принимает значение 1, а B_2

– значение 0. Тогда фл А принимает значение 1 и утверждается , что $B_1, \neg B_2 \vdash \neg B_1 \rightarrow B_2$.

Доказазательство 2.4.6. Индукция по числу n вхождений пс в А. Основание индукции: n=0 и А есть просто пб B_1. Утверждение сводится к доказательству $\neg B_1 \vdash \neg B_1$ или $B_1 \vdash B_1$ (см. Утверждение 2.4.1 и примени теорему о дедукции).

Индукционный шаг: пусть Утверждение 2.4.5 верно при любом к< n. 1 случай: А = ¬В и число вхождений пс в В меньше n. Если при заданном распределении истинностных значений пб В принимает значение 1, тогда А принимает значение 0 и В`=В, а А`= ¬А. По предположению индукции имеем $B_1`,\ldots,B_к` \vdash B$. Но тогда по Утверждению 2.4.4 (b) и МР $B_1`,\ldots,B_к` \vdash \neg\neg B$, которое и есть А. Пусть теперь В принимает значение 0, тогда А принимает значение 1 и В`= ¬В и А`=А. По предположению индукции $B_1`,\ldots,B_к` \vdash \neg B$, а это и есть А. 2 случай: А=В→С. Число вхождений пс в В и С меньше n и по индукционному предположению $B_1`,\ldots,B_к` \vdash B`$ и $B_1`,\ldots,B_к` \vdash C`$. Если В принимает значение 0, то А принимает значение 1 и В`= ¬В и А`=А. Но тогда $B_1`,\ldots,B_к` \vdash \neg B$ и по Утверждению 2.4.4 (c) $B_1`,\ldots,B_к` \vdash B \rightarrow C$, т.е. А. Если С принимает значение 1, то А принимает значение 1 и С`= С, А`=А. Т.к. $B_1`,\ldots,B_к` \vdash C(=C`)$, то по схеме аксиом А1) $B_1`,\ldots,B_к` \vdash B \rightarrow C(=A`)$. Пусть, наконец, В принимает значение 1 и С принимает значение 0, тогда А принимает значение 0 и А`= ¬А, В`=В и С`= ¬С. По предположению индукции имеем

B_1`,…,$B_к$` □ B и B_1`,…,$B_к$` □ ¬C. Тогда по Утверждению 2.4.4 (f) получаем, что B_1`,…,$B_к$` □ ¬(B→C), что и есть A. Индукционный шаг, а с ним и Утверждение 2.4.6 доказаны.

Утверждение 2.4.7 (Теорема о полноте). Если фл. A теории L является тавтологией, то она есть теорема теории L.

Доказательство (Кальмар). Пусть A есть тавтология и B_1,…,$B_к$ - пб, входящие в A. В силу Утверждеия 2.4.6 при всяком распределении истинностных значений пб имеем B_1`,…,$B_к$` □ A (т.к. A – тавтология). Отсюда получаем, что если $B_к$ принимает значение 1, то B_1`,…,$B`_{к-1}$,$B_к$ □ A, а если $B_к$ принимает значение 0, то B_1`,…,$B`_{к-1}$,¬$B_к$ □ A. А тогда по теореме о дедукции и по Утверждению 2.4.4 (g) B_1`,…,$B`_{к-1}$ □ A. Продолжая этот процесс исключения пб, мы получим □ A. Теорема о полноте доказана.

Следствие 2.4.8 Если выражение B содержит все пропозициональные связки и является сокращением для некоторой фл A теории L, то B является тавтологией тогда и только тогда, когда A есть теорема теории L. Докажите Следствие 2.4.8 самостоятельно.

Формальная теория T называется непротиворечивой, если не существует формулы A такой, чтобы A и ¬A были теоремами теории T.

Утверждение 2.4.9 Система L непротиворечива.

Для доказательства достаточно заметить, что отрицание тавтологии не есть тавтология.

Из непротиворечивости L следует, что есть фл, не являющаяся теоремой L. Но непротиворечивость теории L можно вывести непосредственно из факта существования фл, не выводимой в L. Действительно, т.к. по Утверждению 2.4.4 (c) □ ¬A→(A→B), то из противоречивости L и правила MP в L была бы выводима любая фл B (этот факт был бы верен в любой теории с правилом MP, в которой выполнено Утверждение 2.4.4 (c)). Теорию, в которой не все фл выводимы, иногда называют абсолютно непротиворечивой и такое определение применимо к теориям, не содержащим пс отрицания.

Утверждение 2.4.10 Теория L разрешима, т.е. существует эффективная процедура, применимая ко всем формулам L, которая по всякой формуле решает, выводима эта формула в L или нет. Доказательство проведите самостоятельно и опишите неформально искомую процедуру.

Замечание. В пункте 2.7 будет приведена (со ссылками на литературу) вторая форма теоремы о полноте для исчисления L).

Задача. Пусть A – пф, не являющаяся тавтологией. Построим теорию L+, которая получается из L добавлением к последней в качестве аксиом всех формул, которые можно получить из фл A, подставляя вместо пб из A произвольные фл (но на место всех вхождений одной и той же пб подставляется одна и та же фл!). Докажите, что теория L+ противоречива.

2.5 Другие аксиоматизации для исчисления высказываний.

Приведём здесь только один, самый распространённый, пример аксиоматизации исчисления высказываний (ряд других можно найти в упоминавшейся книге Э. Мендельсона). Обозначим эту систему через L_4.

Пс служат $\to$, $\wedge$, $\vee$, $\neg$ и упоминавшиеся в формализации для L скобки и пб. Единственное правило вывода – MP. Класс аксиом задаётся следующими схемами:

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

Для $\equiv$ применяется обычное сокращение. Этот пример аксиоматизации использован в учебнике Клини.

Задача. Докажите, что системы L и L_4 имеют одно и то же множество теорем (с точностью до принятых сокращений).

Следующий материал до Главы 3 можно при первом чтении пропустить.

2.6 Независимость. Многозначные логики.

Подмножество X аксиом данной формальной теории (аксиоматической) называется независимым, если какая-либо формула из этого множества не может быть выведена с помощью правил вывода из остальных аксиом теории, не входящих в X.

Сейчас будет изложен один из методов доказательства независимости с помощью многозначных логик (рассмотренное нами пропозициональное исчисление есть частный случай двузначной логики).

Пусть числа 0,1, … , n являются «истинностными значениями» и выберем какое-либо число m такое, чтобы $1 \leq m \leq n$. Числа 0, … , m назовём «выделенными истинностными значениями». Выберем некоторое число «истинностных таблиц», которые представляют функции, отображающие множество $\{0,1,\ldots,n\}^к$ в $\{0,1,\ldots,n\}$. Для каждой такой таблицы введем знак, который будем называть соответствующей этой таблице связкой. С помощью этих связок и пб можно строить пф (многозначные!). Всякая такая пф определяет некоторую «истинностную» функцию из множества $\{0,1,\ldots,n\}^к$ в множество $\{0,1,\ldots,n\}$. Пф называется выделенной, если она принимает только выделенные значения. В описанной ситуации говорят, что задана многозначная логика M. Аксиоматическая теория, содержащая пб и связки логики M называется подходящей для логики M в том и только в том случае, если множество теорем этой теории совпадает с множеством выделенных пф логики M (ясно, что все эти понятия можно обобщить и на случай логики с

бесконечным числом истинностных значений). В этом случае аксиоматическая теория называется полной

относительно логики М. Выше была изучена двузначная логика, соответствующая случаю n=1 и m=0, соответствующие связки были определены в пункте 1.2. Выделенные пф назывались тавтологиями. Утверждения 2.4.5 и 2.4.7 говорили, что теория L является подходящей для этой логики аксиоматической теорией. Используя технику многозначных логик, докажем, что все три схемы аксиом теории L являются независимыми.

Утверждение 2.6.1 Схема аксиом А1 является независимой. Доказательство. Рассмотрим таблицы:

A	$\neg$A	A	B	A$\rightarrow$B
0	1	0	0	0
1	1	1	0	2
2	0	2	0	0
		0	1	2
		1	1	2
		2	1	0
		0	2	2
		1	2	0
		2	2	0

Ясно, что при всяком распределении значений 0,1,2 для букв, входящих в какую-либо фл А, эти таблицы позволяют найти соответствующее значение А. Если А принимает всегда значение 0, то она будет

называться выделенной (трёхзначная логика с одним выделенным значением). Можно убедиться (убедитесь!), что правило MP сохраняет свойство выделенности. Нетрудно также проверить (и это тоже упражнение), что всякая аксиома, получающаяся по схемам A2) или A3), также является выделенной. Ясно также, что любая фл, выводимая из A2) и A3) по правилу MP, будет выделенной. Но фл $A\to(B\to A)$ не является выделенной (эта формула, а точнее пф, принимает значение 2, когда A принимает значение 1 и B принимает значение 2). Это и доказывает независимость схемы A1).

Задача. Докажите независимость схем аксиом A2) и A3), придумав подходящие таблицы для связок $\to$ и $\neg$ в отмеченной трёхзначной логике (при этом задача может быть решена совершенно различными способами). Отметим также, что в случае доказательства независимости нам не нужно доказывать полноту аксиоматики относитель но многозначной логики, а только так называемую корректность, т.е. аналог Утверждения 2.4.5.

Продемонстрируем другой способ доказательства независимости схемы аксиом A3) (общий подход в деле доказательства независимости таков: для аксиоматической теории T нужно построить модель (ниже мы определим понятие модели в некотором частном случае; в общем случае этим занимается специальная ветвь математической логики – теория моделей), в которой бы все аксиомы были «истинны», а аксиома, чья независимость должна

быть доказана – нет). Если A – произвольная фл теории L, то пусть фл P(A) получается из фл A стиранием в ней всех знаков отрицания. Нетрудно теперь заметить, что P(A1)) и P(A2)) – тавтологии (почему?). Также, правило MP сохраняет свойство A иметь в качестве P(A) также тавтологию (почему?). Теперь достаточно взять частный случай A3): B = (¬A→¬A)→((¬A→A)→A), вычислить P(B) (вычислите!) и убедиться, что P(B) не является тавтологией. Таким образом, схема аксиом A3) является независимой от схем A1) и A2).

2.7 Интуиционистское исчисление высказываний.

Пусть система L_1 получается из системы L_4 заменой схемы аксиом 10 из пункта 2.5 схемой аксиом 10`: ¬A→(A→B). Система L_1 называется интуиционистским исчислением высказываний и была введена А.Гейтингом в 1927-30 гг. Совершенно очевидно, что система L_1 – непротиворечивая теория. Далее, для L_1 также имеет место теорема о дедукции (докажите два последних факта самостоятельно). Не очень трудно также проинтерпретировать исчисление L_4 в исчислении L_1 (для этого (Гливенко, 1929 г.) нужно каждой формуле языка исчисления высказываний приписать впереди двойное отрицание (т.е.формула A будет иметь вид ¬¬A) и после этого доказать такой факт: L_4 ⊢ A ⇔ L_1 ⊢ ¬¬A). Теперь видно, что интуиционистское

исчисление высказываний является подсистемой системы классического исчисления высказываний, но и классическое исчисление высказываний может быть проинтерпретировано в интуиционистском исчислении высказываний. Хорошо известно, что в классическом исчислении высказываний система связок не является независимой (т.е. некоторые связки выражаются через другие (см. пункт 2.3)). Однако в интуиционистском исчислении высказываний все связки являются независимыми (для доказательства см. книгу А.Драгалина «Математический интуиционизм. Введение в теорию доказательств», стр. 98, пункт 3.2). Этот результат принадлежит К.Гёделю, который также доказал, что система L_1 не полна относительно любой конечнозначной логики. Для систем L_1 и L_4 Г.Генцен построил секвенциальные варианты этих исчислений. С помощью техники Г.Генцена можно дать другое доказательство полноты исчисления L_4 (см. упоминавшуюся в Предисловии книгу Н.К.Верещагина и А.Шеня, стр.58). Доказательство теоремы о полноте для исчисления L_1 (которое также можно найти в той же книге, стр. 79) уже не является столь же простым, как для классического исчисления высказываний (оказывается, L_1 полно относительно так называемых «конечных моделей Крипке»). Этот результат о полноте позволяет доказать ещё и разрешимость системы L_1. Еще одним интересным свойством, которым система L_1 отличается от системы L_4, является так называемое свойство

дизъюнктивности. Говорят, что формальная система T со связкой $\vee$ («или») обладает дизъюнктивным свойством, если из того, что в системе выводима формула $A \vee B$ следует, что в системе выводима формула A или в системе выводима формула B (система L_4 таким свойством не обладает, т.к. для любой пп p в L_4 выводима формула $p \vee \neg p$, но в L_4 не выводимы ни формула p, ни формула $\neg p$). Мы приведем доказательство свойства дизъюнктивности полностью и на этом наш экскурс в интуиционистское исчисление высказываний будет завершён.

Утверждение 2.7.1 Интуиционистское исчисление высказываний обладает свойством дизъюнктивности.

Технически удобнее работать в интуиционистском исчислении высказываний, в языке которого есть константа $\bot$ («ложь») и нет связки «отрицание», которая определяется так: $\neg A \Leftrightarrow (A \to \bot)$. Наше исчисление теперь содержит следующие постулаты (обозначим его L_1'): все схемы аксиом из L_1 остаются, но схема 9) есть частный случай 2) и не нужна, а схема 10′ заменяется схемой 10″: $\bot \to A$.

Задача Докажите, что схема 10′ выводима из 10″ и правила MP в L_1'.

Определим теперь понятие rA (формула A реализуема) индукцией по построению формулы A:

а) $rp \Leftrightarrow \Box p$ (здесь и далее $\Box$ означает выводимость в L_1'; p - пп); б) не верно, что $r\bot$; в) $r(A \wedge B) \Leftrightarrow rA$ и rB; г) $r(A \vee B) \Leftrightarrow [rA$ и $\Box A]$ или $[rB$ и $\Box B]$; д) $r(A \to B) \Leftrightarrow [rA$ и $\Box A \Rightarrow rB]$.

Утверждение 2.7.2 Если □A, то rA.

Доказательство Утверждения 2.7.1 Пусть □A∨B. Тогда r(A∨B) по Утверждению 2.7.2, т.е. [rA и □A] или [rB и □B]. В первом случае □A, во втором - □B. Свойство дизъюнктивности L_1', а с ним и L_1, доказано.

Следствие 2.7.3 Следующие формулы не выводимы в исчислении L_1 : p∨¬p (закон исключенного третьего), ¬¬p→p (закон снятия двойного отрицания), ¬(p∧q) → (¬p∨¬q) (один из двух законов де Моргана).

Задача Докажите Следствие 2.7.3 самостоятельно, а также тот факт, что если L_1□A и если вместо некоторых пп, входящих в A, подставить любые формулы (но вместо одной и той же переменной – одну и ту же формулу), то новая формула B, полученная из A таким образом, также выводима в L_1.

Доказательство Утверждения 2.7.2. Применяем индукцию по выводу формулы A. Нужно проверить, что все схемы аксиом реализуемы и что правило MP по реализуемым формулам даёт реализуемую формулу. Мы проверим реализуемость схем 2) и 8).

2) Предположим, что r(A→(B→C)), т.е. если rA, □A, rB и □B, то rC. Тогда нужно доказать, что если r(A→B) и □A→B, то r(A→C), т.е. из того, что (rA и □A влечёт rB) и □A→B и rA и □A следует rC. Но это действительно так (если заметить, что □A и □A→B даёт □B) , ибо следует из замечания в скобках и посылок выше. Реализуемость схемы 2) доказана.

8) По аналогии со схемой 2), пусть r(A→C), т.е. rA и □A даёт rC. Нужно доказать, что реализуемо

заключение схемы, т.е. если □B→C и r(B→C), , то в предположении r(A∨B) и □A∨B будем иметь rC. Т.к. r(A∨B), то [rA и □A] или [rB и □B]. В первом случае, в силу r(A→C), имеем rC. Во втором случае, в силу r(B→C) (по предположению), также имеем rC. Это и доказывает реализуемость схемы 8) и Утверждения 2.7.2.

Задача Докажите реализуемость схем аксиом 1), 3)-7), 9) и правила MP.

Г Л А В А 3

Чистое исчисление предикатов.

3.1 Как уже объяснялось, существуют такие виды логических рассуждений, которые не могут быть обоснованы в рамках исчисления высказываний. Внутренняя структура таких предложений другая. Также, необходимо понимать такие выражения, как «все», «некоторый» и др. В пункте 1.1 мы уже описывали понятие «предикат» и «квантор» и выясняли смысл этих понятий. Теперь мы опишем на формальном уровне исходные понятия исчисления предикатов, которое есть расширение аксиоматической теории L. К символам, описанным в пункте 2.4, добавим символ ∀, предметные (индивидные) константы (т.к. у нас их не будет, то и никаких обозначений не вводим), предметные (индивидные) переменные (пп), предикатные буквы (прб) $A_к^i$, где к – нижний индекс (номер) прб, а i –

валентность (местность) прб. Функциональных букв у нас не будет и такое исчисление предикатов называется чистым. Прб с переменными и будут элементарными формулами (эф) (заметим, что прб без переменных (валентности 0) есть высказывание). Фл исчисления предикатов определяются так:
(a) всякая эф есть фл; (b) если A и B – фл, то ($\neg$A), (A$\rightarrow$B), ($\forall$yA) также есть фл; (c) выражение является фл только если это следует из (a) и (b). В последней формуле из пункта (b) A называется областью действия квантора $\forall$y (A может и не содержать пп y). Квантор существования $\exists$xA(x) определяется как сокращённая запись $\neg(\forall x\neg A(x))$. Оставляя в силе введённые ранее правила об опускании скобок, будем дополнительно считать, что кванторы $\forall$y и $\exists$y располагаются по силе между связками $\equiv,\rightarrow$ и связками $\neg$, $\wedge$, $\vee$. Пример: вместо $((\forall xA(x))\rightarrow B(x,y))$ пишем $\forall xA(x)\rightarrow B(x,y)$; вместо $(\forall x(A(x)\vee B(x,y)))$ пишем $\forall xA(x)\vee B(x,y)$. Также, вместо нижних индексов просто употребляем разные прб, а верхние индексы опускаем, т.к. все пп, входящие в фл, пишем полностью.

Введём теперь важное понятие связанного и свободного вхождения пп в фл. Данное вхождение данной пп в фл называется связанным, если данное вхождение данной пп есть пп входящего в эту фл квантора или находится в области действия входящего в эту формулу квантора. В противном случае данное вхождение данной пп в формулу

называется свободным.

Задача. Рассмотрите три примера A(x,y); $A(x,y)\to\forall xB(x)$; $\forall x(A(x,y)\to\forall xB(x))$ и укажите для всякого вхождения всякой пп каким это вхождение является.

Переменная называется свободной (связанной) в данной фл, если существуют свободные (связанные) её вхождения в эту фл. Одна и та же пп может быть свободной и связаной в данной фл.

3.2 Интерпретации и модели.

Наши формулы будут иметь смысл, только если мы проинтерпретируем каким-либо образом входящие в них символы. Под интерпретацией будем понимать пару: непустое множество D (область интерпретации) и соответствие, которое каждой прб данной валентности сопоставляет некоторое (той же валентности) отношение на D. При этом пп мыслятся как пробегающие над областью D, а пс и кванторам придаётся обычный смысл. При данной интерпретации всякая фл без свободных переменных (замкнутая фл или зфл) представляет собой высказывание, которое будет либо истинно, либо ложно), а всякая фл со свободными пп выражает некоторое отношение на D, которое для одних значений пп может быть истинно, а для других значений тех же пп – ложно. В качестве упражнения предлагаем читателю рассмотреть на области натуральных чисел (без 0) следующие фл (i) A(x,y);

(ii) $\forall y A(x,y)$; (iii) $\exists y \forall x A(x,y)$, где $A(x,y)$ интерпретируется как $x \leq y$ и выяснить, какие отношения эти фл представляют (затем замените множество всех натуральных чисел на множество всех целых чисел и снова выясните, какие отношения эти же фл представляют).

Теперь мы определим понятия выполнимости и истинности, но не будем крайне формалистичны. Назовём оценкой любое отображение множества пп в область D. Определим значение фл A при оценке f индукцией по построению A. Если $A(x_1, \ldots, x_n)$ – эф и A интерпретируется как отношение $\boldsymbol{A}$ на D^n, то подставим в $\boldsymbol{A}$ вместо переменных их значения при данной оценке f. Если при этом отношение $\boldsymbol{A}(f(x_1),\ldots f(x_n))$ выполнено на D, то значение эф $A(x_1, \ldots, x_n)$ при оценке f равно 1, в противном случае значение эф $A(x_1, \ldots, x_n)$ при оценке f равно 0. Далее, значение фл при оценке определяется по индукции с помощью таблиц истинностности для пс.. Значение фл $\neg A$ при оценке f есть $\neg$(значение фл A при той же оценке). Значение фл $A \rightarrow B$ при оценке f есть (значение фл A при f)$\rightarrow$(значение фл B при f). Значение фл $\forall x A(x, x_1, \ldots, x_n)$ при оценке f есть 1, если отношение $\boldsymbol{A}(d, f(x_1),\ldots,f(x_n))$ выполнено при любом d из D; в противном случае значение фл $\forall x A(x, x_1, \ldots, x_n)$ при оценке f есть 0.

Скажем, что фл A истинна в данной интерпретации, если она выполнена при любой оценке f. Если формула не выполнена ни при одной

оценке, то она называется ложной (в данной интерпретации). Следующие факты проверяются без труда: a) если фл A ложна в данной интерпретации, то фл ¬A истинна в той же интерпретации и наоборот;
в) никакая фл не может быть одновременно истинной и ложной в данной интерпретации; c) если фл A и A→B истинны в данной интерпретации, то фл B истинна в той же интерпретации; d) фл A→B ложна в данной интерпретации тогда и только тогда, когда фл A истинна, а фл B ложна в этой интерпретации; e) фл A истинна в данной интерпретации (т.е. при любой оценке!), когда фл ∀xA(x) истинна в той же интерпретации; f) всякий частный случай любой тавтологии истинен во всякой интерпретации (частным случаем пф называется фл, получаемая подстановкой в пф вместо пп произвольных фл так, что вместо одной и той же пп подставляется одна и та же фл); g) если свободные переменные фл A оценки f и g оценивают одинаково, то значение фл A при оценке f совпадает со значением A при оценке g.
Задача. Докажите пункты a) – g) самостоятельно.

Фл A называется общезначимой (озф), если она истинна в любой интерпретации. Фл A называется выполнимой (вф), если найдётся интерпретация, при которой она истинна. Следующие факты также доказываются без труда (докажите!): a) A есть озф тогда и только тогда, когда фл ¬A не является вф; в) A есть вф тогда и только тогда, когда фл ¬A не является озф; c) зфл A выполнима тогда и только

тогда, когда она истинна в какой-либо интерпретации.

Фл А – противоречие, если $\neg$А – озф. Фл А влечёт фл В, если в любой интерпретации фл В истинна при всякой оценке, при которой выполнена фл А. Две фл эквивалентны, если каждая из них влечёт другую. Следующие факты докажите самостоятельно: а) фл А влечет фл В, если фл А$\rightarrow$В озф; в) фл А и В эквивалентны, если фл А$\equiv$В озф; с) если фл А влечёт фл В и фл А истинна в данной интерпретации, то фл В истинна в той же интерпретации.

Задача. Докажите, что: а) всякий частный случай тавтологии есть озф (определение частного случая было дано выше); в) если фл А не содержит х свободно, то фл $\forall x(A\rightarrow B)\rightarrow(A\rightarrow\forall xB(x))$ – озф; с) фл $\forall xA(x)\rightarrow A(y)$ – озф; d) фл $\forall x\exists yA(x,y)\rightarrow\exists y\forall xA(x,y)$ не является озф (рассмотрите подходящую интерпретацию для данной фл!).

Задача. Докажите, что фл $[\forall xA(x)\rightarrow\forall xB(x)]\rightarrow[\forall x(A(x)\rightarrow B(x))]$ не является озф; докажите также общезначимость таких фл: а) $\forall xA(x)\rightarrow\exists xA(x)$; в) $\forall xA(x)\equiv\neg\exists x\neg A(x)$; с) $\forall x(A(x)\rightarrow B(x))\rightarrow(\forall xA(x)\rightarrow\forall xB(x))$; d) $(\forall xA(x)\wedge\forall xB(x))\equiv\forall x(A(x)\wedge B(x))$ и тот же факт, но с заменой $\wedge$ на $\vee$; е) $\exists x\forall yA(x,y)\rightarrow\forall x\exists yA(x,y)$.

3.3 Аксиомы чистого исчисления предикатов

К схемам аксиом из пункта 2.4 (3)) добавим ещё две: А4) $\forall xA(x)\rightarrow A(y)$ и А5) $\forall x(A\rightarrow B(x))\rightarrow$

(A→∀xB(x)), где фл A не содержит пп x свободно. К правилам вывода из пункта 2.4. (4)) добавим такое правило вывода: фл ∀xA есть непосредственное следствие фл A (правило Gen).

Любая теория в языке первого порядка (т.е.в языке без кванторов по прб) содержит (если язык без функциональных символов, а последнее требование не ограничивает общности рассмотрения) отмеченные нами схемы аксиом и правила вывода (логика теории), а также какие-либо собственные аксиомы. У чистого исчисления предикатов таких собственных аксиом нет.

Моделью чистого исчисления предикатов называется любая интерпретация, в которой истинны все аксиомы чистого исчисления предикатов (обозначим его через К), а правила вывода при применении к истинным в данной интерпретации фл дают истинные в той же интерпретации фл. Тогда всякая теорема теории К истинна в той же интерпретации. Ограничения на пункты схем A4) и A5) необходимы. Пусть A(x) есть ¬∀yB(x,y) и пп y не входит свободно в A(x). Рассмотрим частный случай схемы аксиом A4): ∀x(¬∀yB(x,y)) → ¬∀yB(y,y) и теперь в качестве интерпретации возьмём область с не менее чем двумя элементами, а в качестве B – отношение тождества (совпадения). Тогда антецедент (посылка) нашего частного случая A4) истинен, а консеквент (сукцедент, заключение) – ложен. В схеме аксиом A5) отказ от ограничения также невозможен: пусть A и B есть C(x) (теперь x входит в A

свободно!); рассмотрим такой пример схемы аксиом A5):
$\forall x(C(x)\to C(x))\to(C(x)\to\forall xC(x))$. Посылка примера общезначима, но если в нашей интерпретации C выполнено не для всех элементов области, то заключение не будет истинным.

Наряду с теорией K будем рассматривать теорию K_4, которая получается следующим образом: берем исчисление предложений в форме L_4 (см. пункт 2.5 для определения (изменяется и язык!)) и добавляем в язык квантор существования $\exists$, а в качестве аксиом добавляем две схемы аксиом и два правила вывода (они известны как правила Бернайса): $\forall xA(x)\to A(y)$; $A(x)\to\exists xA(x)$; если в K_4 выводима фл $\forall x(B\to A(x))$, где пп x не входит свободно в B, то в K_4 выводима фл $B\to\forall xA(x)$ (правило B1); если в K_4 выводима фл $\forall x(B(x)\to A)$, то в K_4 выводима фл $\exists xB(x)\to A$, где пп x не входит свободно в A (правило B2). В дальнейшем некоторые факты для K будут доказываться при нотации с квантором существования, однако в этих случаях этот квантор будет всегда выражен через квантор всеобщности так: $\exists xA(x) = \neg\forall x\neg A(x)$.
Задача. Докажите, что исчисления K и K_4 обладают одним и тем же множеством теорем.

3.4 Свойства чистого исчисления предикатов.

На самом деле все наши дальнейшие результаты будут верны для любой теории первого порядка, а не

только для исчисления К.

Утверждение 3.4.1 Если фл А теории К есть частный случай тавтологии, то фл А есть теорема теории К и может быть выведена только с употреблением схем А1) – А3) и правила МР.

Доказательство. Возьмём вывод тавтологии А в L и сделаем в нём всюду такие изменения: (i) если пп входит в вывод, то на места всех её вхождений во все фл вывода подставляем ту фл теории К, которая подставлялась вместо этой пп при получении фл А; (ii) если данная пп не входит в вывод, то на места всех её вхождений во все фл вывода подставляем одну и ту же фл теории К (произвольную). Полученная новая последовательность фл и будет выводом нашей фл А в К, при этом использовались только отмеченные в Утверждении 3.4.1 схемы и правила вывода.

Упражнение. Возьмите какой-либо вывод какой-либо фл в L и преобразуйте сначала полученную тавтологию, а затем её вывод так, как указано выше!

Утверждение 3.4.2 Чистое исчисление предикатов непротиворечиво.

Доказательство. Для фл А через П(А) обозначим фл, которая получится из А опусканием всех кванторов и стоящих за ними пп. Полученное выражение является пф (вместо пп в них будут стоять прб). Наша операция П проносится через пс (проверьте это!). Если фл А есть пример аксиом А1) – А5), то П(А) – тавтология (проверьте это для схем А4) и А5)). Проверьте также, что правила МР и Gen преобразуют тавтологии в тавтологии. Если бы теперь в К

выводились фл В и ¬В, то оба выражения П(В) и П(¬В) были бы тавтологиями, однако последнее невозможно (почему?). Итак, теория К – непротиворечива.

Замечание. Немного ниже мы приведём другое доказательство непротиворечивости К, использующее теорему о полноте для чистого исчисления предикатов К.

Теорема о дедукции прямо на исчисление предикатов не переносится. Например, пусть А $\vdash$ $\forall$xA(x), однако не всегда $\vdash$ А $\rightarrow\forall$xA(x). Рассмотрим область из двух элементов а и в. Пусть фл А интерпретируется свойством, которым обладает только элемент а. Тогда фл А выполнена при любой оценке, отображающей пп х в а, а фл $\forall$xA(x) не выполнена ни при какой оценке, т.е. фл А $\rightarrow\forall$xA(x) не есть озф. Но в теореме о полноте мы докажем, что всякая теорема теории К является озф.

Но все же некоторая ослабленная форма теоремы о дедукции остаётся верной и для исчисления К. Рассмотрим конечное множество фл Г, фл А$\in$Г и вывод $B_1,\ldots,B_n$ из Г, снабженный обоснованием каждого шага. Скажем, что B_i в этом выводе зависит от А, если B_i есть А и обоснованием B_i служит принадлежность B_i к Г или B_i обосновано как следствие по MP или Gen некоторых предшествующих фл, хотя бы одна из которых зависит от А. Приведём пример: А, $\forall$xA(x)$\rightarrow$C $\vdash$ $\forall$xC

1. А гипотеза

2. $\forall x A(x)$ из 1. По Gen
3. $\forall x A(x) \to C$ гипотеза
4. C из 2. и 3. По MP
5. $\forall x C$ из 4 по Gen.

В приведенном выводе шаг 1 зависит от A, шаг 2 зависит от A, шаг 3 зависит от $\forall x A(x) \to C$, шаг 4 зависит от A и от $\forall x A(x) \to C$ и шаг 5 зависит от A и от $\forall x A(x) \to C$.

Утверждение 3.4.3 Если фл B не зависит от фл A в выводе Г, A □ B, то Г □ B.

Доказательство. Пусть $B_1,\ldots,B_n=B$ – вывод B из {Г, A} и пусть B не зависит от A. Проведём индукцию по длине вывода. Итак, пусть наше доказывемое предложение верно для всякого вывода, длина которого меньше n. Если B принадлежит Г или есть аксиома, то наше утверждение верно. Если B есть непосредственное следствие каких-либо фл (одной или двух в зависимости от правила вывода), то, т.к. B не зависит от A, то от A не зависит ни одна из этих фл и по предположению индукции из Г выводятся эти фл а, следовательно, и фл B.

Утверждение 3.4.4 (Теорема о дедукции для К).

Пусть Г, A □ B и пусть при этом существует такой вывод, в котором ни при каком применении правила Gen к фл, зависящим в этом выводе от A, не связывается квантором никакая свободная переменная фл A. Тогда Г □ $A \to B$.

Прежде чем доказывать Утверждение 3.4.4, дадим его более слабые, но полезные в применении

следствия.

Следствие 3.4.5 Если Г, A □ B и вывод свободен от применения правила Gen к свободным переменным из фл A, то Г □ A→ B.

Следствие 3.4.6 Если фл A замкнута и Г, A □ B, то Г □ A→ B.

Докажем теперь Утверждение 3.4.4. Используем индукцию по построению вывода. Пусть $B_1,\ldots,B_n=B$ – вывод B из {Г,A}, удовлетворяющий условиям теоремы. Докажем теперь для всякого $i \le n$ наше Утверждение 3.4.4. Если B_i есть аксиома или B_i принадлежит Г, то Г □A→B_i, т.к. $B_i\to(A\to B_i)$ есть аксиома. Если B_i=A, то Утверждение 3.4.4 верно в силу выводимости A→A. Если есть j и k меньшие i такие, что $B_к$ есть $B_j\to B_i$, то в силу индукционного предположения имеем Г□A→B_j и Г□A→$(B_j\to B_i)$. Используя схему аксиом A2) и правило MP, получим Г□A→B_i. Наконец, пусть найдётся $j < i$ такое, что $B_i=\forall x_к B_j$. По предположению, Г □A→B_j и B_j либо не зависит от A, либо переменная x_k не свободна в фл A. Если первое, то в силу Утверждения 3.4.3 имеем Г □B_j и, по правилу Gen, Г□$\forall x_к B_j$, т.е. Г□B_i. Используя схему аксиом A1) и MP, имеем Г□A→B_i. Если же $x_к$ не свободная переменная фл A, то по схеме A5) □$\forall x_k(A\to B_j)\to(A\to\forall x_k B_j)$. Т.к. Г□A→$B_j$, то по правилу Gen получаем Г□$\forall x_k(A\to B_j)$ и, по MP, Г□A→$\forall x_k B_j$, т.е. Г □A→B_i. Это и завершает наше доказательство. Т.к. $i\le n$, то имеем требуемое.

Приведём полезный пример. Докажем, что $\vdash \forall x \forall y A \to \forall y \forall x A$

1. $\forall x \forall y A$ гипотеза.
2. $\forall x \forall y A \to \forall y A$ схема A4)
3. $\forall y A$ из 1 и 2 по MP
4. $\forall y A \to A$ схема A4)
5. A из 3 и 4 по MP
6. $\forall x A$ из 5 по Gen
7. $\forall y \forall x A$ из 6 по Gen

В силу 1 – 7 получаем, что $\forall x \forall y A \vdash \forall y \forall x A$ и что в нашем выводе ни при одном применении правила Gen не связывается никакая свободная переменная фл $\forall y \forall x A$. Поэтому, на основании Следствия 3.4.5, получаем требуемый результат.

Задача. Докажите выводимость в К таких фл:

а) $\vdash \forall x(A \to B) \to (\forall x A \to \forall x B)$; в) $\vdash \forall x(A \to B) \to (\exists x A \to \exists x B)$; с) $\vdash \forall x(A \wedge B) \equiv (\forall x A \wedge \forall x B)$.

Утверждение 3.4.7 (Теорема о полноте для исчисления К). В чистом исчислении предикатов К фл А выводима тогда и только тогда, когда А есть озф.

Мы докажем только половину (более лёгкую) этой теоремы. Относительно второй половины скажем только, что она есть следствие следующих двух утверждений: а) (лемма Линденбаума) если теория первого порядка непротиворечива (в частности, чистое исчисление предикатов), то существует ее полное непротиворечивое расширение (т.е. расширение, в котором для любой замкнутой фл

выводимы либо сама фл, либо её отрицание); в) всякая непротиворечивая теория первого порядка (в частности, чистое исчисление предикатов) имеет счётную модель (модель, у которой область D счётная).

Доказательство первой половины Утверждения 3.4.7

Легко проверить, что любой пример любой схемы аксиом является озф (проверьте этот факт!).

Также, нетрудно видеть (частично это уже делалось в пункте 3.2 в самом конце), что понятие озф сохраняется при применении правил вывода MP и Gen. Следовательно, всякая теорема исчисления К является озф. Также, как следствие первой половины нашего Утверждения 3.4.7, получаем ещё одно доказательство непротиворечивости исчисления К (проделайте это самостоятельно).

Пусть A – фл с одной точно свободной пп (наше ограничение сделано для простоты рассмотрения). Рассмотрим фл A(x) и A(y), где x и y – разные переменные. Фл выше называются подобными, если пп x свободна для пп y в фл A(y) и A(y) не имеет свободных вхождений пп x. Нетрудно видеть (и в этом нужно убедиться самим), что наше отношение подобия симметрично.

Утверждение 3.4.8 Если фл A(x) и A(y) подобны, то $\vdash \forall x A(x) \equiv \forall y A(y)$.

Доказательство. По схеме аксиом A4) $\vdash \forall x A(x) \to A(y)$. Теперь применим правило Gen: $\vdash \forall y(\forall x A(x) \to A(y))$ и, по схеме аксиом A5), имеем $\vdash \forall x A(x) \to \forall y A(y)$. Вторая половина Утверждения

доказывается аналогично в силу симметрии. Применяя тавтологию (которая выводима в К, Утверждение 3.4.1), $A\to(B\to(A\wedge B))$, завершаем доказательство.

Задача. Докажите, что если фл A(x) и A(y) подобны, то $\vdash \exists xA(x) \equiv \exists yA(y)$.

Замечание. Теорема о полноте была впервые доказана К. Гёделем (т.н. первая теорема Гёделя) в 1930 г. и её оригинальное доказательство было совсем другим. Мы приведём сейчас несколько следствий из теоремы о полноте, которые очень парадоксальны.

а) фл А истинна в каждой счётной модели $\Leftrightarrow$ $\vdash_K A$;

в) если фл В является следствием множества фл Г, то $\Gamma \vdash_K A$;

с) (теорема Сколема – Лёвенгейма) если теория К (любая теория первого порядка!) имеет какую-нибудь модель, то она имеет счётную модель (и это несмотря на то, что в формальной теории К «речь может идти о несчётных множествах»!; пример: теория множеств Цермело-Френкеля является теорией первого порядка). Следствие (конечно, не прямо теоремы о полноте, а доказательства второй её половины) достаточно парадоксальное.

В завершение изучения исчисления предикатов К приведем еще несколько дополнительных метатеорем (метатеоремой называется утверждение о свойствах какой-либо формальной теории) и рассмотрим вопрос о приведении фл языка теории К к некоторому важному стандартному (т.н. предваренному нормальному!) виду.

Утверждение 3.4.9 (правило индивидуализации)
$\forall x A(x) \vdash A(y)$ Использовать схему аксиом А4) и правило MP.
Утверждение 3.4.10 Если пп x не свободна в фл A, то следующие фл являются теоремами теории K:
a) $A \to \forall x A(x)$; в) $\exists x A(x) \to A$;
c) $\forall x(A \to B) \equiv (A \to \forall x B)$; d) $\forall x(B \to A) \equiv (\exists x B \to A)$.
Задача. Докажите последнее Утверждение 3.4.10 самостоятельно.
Утверждение 3.4.11 (правило существования)
$\vdash A(y) \to \exists x A(x)$ (пп y не входит свободно в фл A).
Доказательство. По аксиоме А4) $\vdash \forall x \neg A(x) \to \neg A(y)$. Из тавтологии $(A \to \neg B) \to (B \to \neg A)$ по MP получаем $\vdash A(y) \to \neg \forall x \neg A(x)$ и $\vdash A(y) \to \exists x A(x)$, ч.т.д.

Приведём теперь ещё без доказательства правило переименования связанных пп.
Утверждение 3.4.12 (переименование связанных пп). Если $\forall x B(x)$ есть подформула фл A, фл B(y) подобна фл B(x) и A` есть результат замены по крайней мере одного вхождения $\forall x B(x)$ в A на $\forall y B(y)$, то $\vdash A \equiv A`$.

Наконец, приведем т.н. правило C, сделав предварительно небольшой комментарий. В математике распространены выводы следующего типа: пусть доказано утверждение вида $\exists x A(x)$. Тогда рассуждают так: если a есть объект такой, что верно A(a), то… проводим некоторое рассуждение …, в конце которого получаем фл B, которая уже не содержит произвольно выбранного объекта a. Отсюда заключают, что верно утверждение $\exists x A(x) \to B$. На

самом деле выбор элемента a со свойством A не нужен и в выводе в K можно обойтись без этого выбора. Мы не будем приводить как точную формулировку, так и обоснование этого правила, а заметим только, что можно определить понятие вывода в K с правилом C и доказать, что если есть вывод в теории K с правилом C, то есть вывод просто в теории K (за более точными формулировками и доказательствами относительно правила C отсылаем читателя к книге Мендельсона, стр. 83-85).

Завершая изучение чистого исчисления предикатов K докажем, что всякую фл A языка теории K можно привести к следующему, назовём его предваренным нормальным, виду: $Q_1x_1Q_2x_2\ldots Q_nx_nB$, где каждое Q_i есть либо квантор $\forall$, либо $\neg\forall$, а фл B кванторов не содержит.

Утверждение 3.4.13. Всякая фл равносильна (в смысле общезначимости, а значит и в смысле выводимости в K) некоторой фл в предваренной нормальной форме.

Доказательство. Следующие фл являются озф при условии, что y не входит свободно ни в A, ни в B:

I) $(\forall xA(x)\to B) \equiv \exists y(A(y)\to B)$;

II) $\exists xA(x)\to B \equiv \forall y(A(y)\to B)$;

III) $B\to\forall xA(x) \equiv \forall y(B\to A(y)$;

IV) $B\to\exists xA(x) \equiv \exists y(B\to A(y))$; на фл в пунктах Y и YI предыдущее ограничение на y не распространяется;

Y) $\neg\forall xA \equiv \exists x\neg A$; YI) $\neg\exists xA \equiv \forall x\neg A$.

Замечание. Полезно в качестве упражнения вывести указанные фл в теории K.

Общезначимость фл в Y) и YI) доказывается

очень просто (докажите самостоятельно). Докажем, что фл из I) есть озф. Пусть фиксированы интерпретация и оценка. Предположим, что истинна (при данных интерпретации и оценке) фл $\exists y(A(y)\to B)$ (напомним, что переменая y не входит свободно в B; вообще, без ограничения общности, считаем, что B – замкнутая фл и что в фл A свободно входит только переменная x). Это означает, что найдется элемент $d\in D$ (D – область интерпретации) такой, что истинна фл $A(d)\to B$. Если для всякого $d\in D$ A(d) – истинная фл, то и B – то же истинная фл и тогда истинна фл $\forall xA(x)\to B$. Если же A(d) истинна не для всякого d, то истинна фл $\forall xA(x)\to B$ в силу ложности посылки. Обратно, предположим, что $\forall xA(x)$ – ложная фл. Но тогда для некоторого d фл A(d) – ложна и, следовательно, фл $\exists y(A(y)\to B)$ – истинна. Если же $\forall xA(x)$ – истинная фл, то B – истинная фл и фл $\exists y(A(y)\to B)$ также истинна. Общезначимость фл II доказывается аналогично.

Задача Докажите, что фл III и IV также есть озф. Утверждение 3.4.13 доказано. Это и доказывает возможность приведения каждой фл исчисления K к предваренной нормальной форме.

Г Л А В А 4.

Элементы теории алгоритмов

При написании этой Главы автор в большой

степени следовал пособию В.А.Успенского для МГУ, которое упоминалось в предисловии.

4.1 Вычислимые функции.

Введём некоторые понятия, причем эти понятия не определяем, т.к. считаем их интуитивно ясными: это понятия «алгоритм», «исходное данное» и ряд др. С каждым алгоритмом будем связывать множество возможных исходных данных. Если x - возможное исходное данное, то при применении алгоритма A к x возможны три исхода: применение A к x завершится за конечное число шагов и будет получен некоторый результат; применение A к x закончится, но безрезультатно; алгоритм A будет работать на x бесконечно, т.е. применение не закончится. В первом случае говорят, что A применим к x, в двух других случаях говорят, что A не применим к x. Попробуйте самостоятельно привести нужные примеры!

Множество тех исходных данных, к которым алгоритм применим, будем называть областью применения алгоритма.

Частичной функцией из множества X в множество Y назовем любое подмножество $A \subseteq X \times Y$ такое, что если первые компоненты упорядоченных пар равны, то и их вторые компоненты равны (в частности, A м.б. пусто). Частичные функции назовём просто функциями, при этом такая функция м.б. и всюду определенной. Каждому алгоритму на множестве исходных данных X м.б. сопоставлена естественным

образом функция на X так, что $f(x) \cong \mathfrak{I}(x)$, где $\mathfrak{I}$ - алгоритм на множестве X. При этом знак $\cong$ называется условным равенством, т.е. $\mathfrak{I}$ и f одновременно определены или неопределены и первом случае имеет место $f(x)=\mathfrak{I}(x)$.

Функция называется вычислимой, если существует вычисляющий ее алгоритм. Например, нигде не определенная функция вычислима.

Конечно, понятие алгоритма имеет смысл только в случае, если исходные данные и результат вычисления (обработки) исходных данных – «конструктивные» объекты. Мы будем считать, что натуральные числа или конечные слова в алфавите (также конечном) суть «конструктивные» объекты и никаких дальнейших пояснений о «конструктивных» объектах не делаем.

Замечание. Не следует думать, что для доказательства вычислимости функции нужно предъявлять соответствующий алгоритм: функция f равная 1, если верна гипотеза Ферма и равная 0 в противном случае вычислима, т.к. равна тождественно 1 или 0.

Функция вычислима, если существует алгоритм, ее вычисляющий.

Задача а) приведите примеры вычислимых функций; б) определим функцию так: $f(n)=0$, если в десятичное разложение числа π входит кортеж 012345678910…n и $f(n)=1$ в противном случае; является ли f вычислимой функцией?

Замечание Если множество X бесконечно и множество Y не пусто, то найдётся невычислимая

функция из X в Y (т.к. множество всех алгоритмов счётно). Сколько элементов должно содержать множество Y, чтобы нашлась всюду определенная невычислимая функция из X в Y?

4.2 Разрешимые множества.

Пусть X и Y – множества «конструктивных» объектов. Подмножество $A \subseteq X$ – разрешимое, если найдется алгоритм, который по всякому $x \in X$ решает, $x \in A$ или нет (другими словами, если характеристическая функция A (т.е. такая функция f(x), что f(x)=1, если $x \in A$ и f(x)=0 иначе) является вычислимой).

Утверждение 4.2.1. Пересечение, объединение и дополнение разрешимых множеств разрешимо.

Задача Докажите Утверждение 4.2.1.

Следствие Утверждения 4.2.1: множества нечетных чисел, простых чисел, кубов натуральных чисел разрешимы.

Замечание. Если X – бесконечное множество, то существует неразрешимое подмножество X (вспомнить, что множество вычислимых функций – счётно).

4.3 Полуразрешимые множества

Назовём множество $A \subseteq X$ полуразрешимым, если найдется алгоритм, который применим к элементам множества A и не работает на элементах из дополнения A, т.е. если A является областью определения какой-либо вычислимой функции.

Замечание Для бесконечного X не всякое его подмножество полуразрешимо, т.к. множество вычислимых функций счётно.

Утверждение 4.3.1. Всякое разрешимое множество полуразрешимо.

Задача. Докажите Утверждение 4.3.1.

Замечание. Несколько ниже мы докажем, что обращение Утверждения 4.3.1 невозможно.

Утверждение 4.3.2 Любое конечное $A \subseteq X$ – разрешимо.

Задача. Докажите Утверждение 4.3.2.

Замечание. Мы считаем, что любое множество «конструктивных» объектов не более чем счётно, а также, что любое множество «конструктивных» объектов можно «перебрать», т.е. существует такая вычислимая функция, которая пересчитывает все объекты из X без повторений. Также мы принимаем без доказательства тот факт, что если X и Y – множества «конструктивных» объектов, то $X \times Y$ – также множество «конструктивных» объектов.

Пусть $A \subseteq X \times Y$. Проекцией A назовём множество $\text{пр}A = \{x: \exists y \in Y(\langle x,y\rangle \in A)\}$.

Утверждение 4.3.3. Проекция разрешимого множества полуразрешима.

Доказательство. Укажем требуемый алгоритм: «перебираем элементы множества Y до тех пор, пока не найдется такой $y \in Y$, что $\langle x,y\rangle \in A$; если такой y найден, то выдать результатом 0».

Замечание Если нужного y нет, то на таком x алгоритм работает бесконечно.

Всюду определенная функция $f : N \to X$ называется вычислимой последовательностью, если f – вычислимая функция.

Утверждение 4.3.4. Множество значений вычислимой последовательности полуразрешимо.

Доказательство. Укажем нужный алгоритм: «для исходного данного x перебирать все натуральные числа, пока не найдётся такое $n \in N$, что $f(n)=x$; при нахождении такого n выдать результатом 0».

4.4 Основные теоремы теории алгоритмов

Пусть $\mathfrak{I}$ - некоторый алгоритм с исходными данными из множества «конструктивных» объектов X в множество «конструктивных» объектов Y. Следующий алгоритм $\mathfrak{R}$ информирует о работе $\mathfrak{I}$ по шагам: исходные данные $\mathfrak{R}$ есть пары $\langle x,n \rangle$, $x \in X$, $n \in N$ и алгоритм $\mathfrak{R}$ примененный к паре $\langle x,n \rangle$ сообщает, закончится ли применение алгоритма $\mathfrak{I}$ к x за n шагов и если «да», то каков ответ применения (можно для $\mathfrak{R}$ среди значений ввести дополнительный символ, появление которого сигнализирует о том, что работа $\mathfrak{I}$ на x не закончена). Докажем теперь такие усиления Утверждений 4.3.3 и 4.3.4.

Утверждение 4.4.1. Следующие свойства подмножества A множества «конструктивных» объектов эквивалентны:

1) A есть область определения вычислимой функции (A – полуразрешимо);

2) A есть проекция разрешимого множества;
3) A=∅ или A есть множество значений вычислимой последовательности;
4) A есть множество значений вычислимой функции.

Доказательство. 1)⇒2) Если A=Domf и f: X→Y – вычислимая функция, то A есть проекция разрешимого множества B={⟨x,n⟩ : x∈X, n∈N и алгоритм, вычисляющий f, применяется к x не более чем за n шагов}.

2)⇒3). Пусть множество B⊆X×Y – разрешимо и A=прB. По очереди перебираем все элементы множества «конструктивных» объектов X×Y и если n-ый элемент $\langle x_n,y_n\rangle$ попал в множество B, то пусть $f(n)=x_n$; в противном случае, т.к. A не пусто, то пусть f(n) равно какому-нибудь фиксированному элементу из A. Тогда последовательность значений функции f будет перечислять элементы множества A (дайте более формальное доказательство).

3)⇒4). В случае пустоты A оно есть множество значений нигде не определенной функции. Если же A есть множество значений вычислимой последовательности, то соответствующая функция и есть требуемая вычислимая функция.

4)⇒1). Пусть f : Y→X – вычислимая функция со множеством значений A. Требуемая функция с областью определения, равной A, вычисляется алгоритмом: «перебирать все пары ⟨n,y⟩, n∈N, y∈Y и для каждой такой пары делать n шагов вычислений f(y); как только для хотя бы одной пары будет получен ответ f(y)=x, то в качестве результата выдать

0». Ясно, что если нужного y нет, то алгоритм не остановится, а если есть (f(y)=x), то алгоритм остановится на некотором шаге m (более формально рассудите самостоятельно). Наше Утверждение 4.4.1 доказано.

Напомним, что множество A называется счётным, если A=∅ или A есть множество значений некоторой последовательности.

Подмножество A множества «конструктивных» объектов назовем перечислимым, если A=∅ или A есть множество значений некоторой вычислимой последовательности. Ясно, что понятие перечислимого множества есть вычислимый аналог счётного множества. Утверждение 4.4.1 утверждает, что множество перечислимо тогда и только тогда, когда оно полуразрешимо.

Утверждение 4.4.2. Пусть $A \subseteq X$, $B \subseteq X$ – перечислимые множества. Тогда $A \cup B$ и $A \cap B$ – перечислимые множества. Если $C \subseteq X \times Y$ перечислимое множество, то прC также перечислимое множество.

Доказательство Утверждения 4.4.2. Если A пусто или B пусто, то доказывать нечего. В противном случае, по Утверждению 4.4.1, A и B есть множества значений вычислимых функций f и g. Но тогда $A \cup B$ есть множество значений последовательности h, которая определяется так: h(2k)=f(k), h(2k+1)=g(k) (сами опишите работу требуемого алгоритма!).

Докажем перечислимость прC (перечислимость же множества $A \cap B$ также докажите сами в качестве

упражнения). Пусть $f : Z \to X \times Y$ и пусть $g : X \times Y \to X$. Полагаем $h=g(f(z))$. Функция h вычислима как композиция вычислимых функций (опишите соответствующий алгоритм). Очевидно, что функция h перечисляет множество прС. Утверждение 4.4.2 доказано.

Утверждение 4.4.3 (Теорема Поста). Подмножество А множества «конструктивных» объектов X разрешимо тогда и только тогда, когда А и его дополнение $X \setminus A$ перечислимы.

Доказательство. Если А разрешимо, то $X \setminus A$ – разрешимо и оба множества перечислимы. Далее, если одно из множеств А или $X \setminus A$ пусто, то все очевидно. Иначе требуемый алгоритм таков: «для исходного x перебираем натуральные числа до тех пор, пока не будет $f(n)=x$ или $g(n)=x$ (здесь f и g вычислимые функции, перечисляющие А и $X \setminus A$ соответственно); для первого такого n, если $f(n)=x$, то $x \in A$, если $g(n)=x$, то $x \in (X \setminus A)$». Т.к. одновременное выполнение обеих равенств невозможно (почему?), то требуемый алгоритм описан и разрешимость А доказана.

Из теоремы Поста следует, что неразрешимое множество обязательно имеет неразрешимое дополнение.

Утверждение 4.4.4 (теорема о графике). Функция $f : X \to Y$ вычислима тогда и только тогда, когда ее график $\{\langle x,y\rangle : y=f(x)\}$ есть перечислимое множество.

Доказательство. Если f – вычислимая функция с непустым графиком (иначе теорема

тривиальна), то ее область определения (по Утверждению 4.4.1, пункт 1)) есть {g(0), g(1), …}, где g – вычислимая функция, а тогда ее график перечислим как множество значений вычислимой функции $h(n)=\langle g(n),f(n)\rangle$. Обратно, если график функции f перечислим и не яв-
ляется пустым множеством, то график есть область значений для некоторой, всюду определенной на N, функции $g : N\to X\times Y$. Тогда исходная функция f вычислима таким алгоритмом: «для исходного данного x перебирать все натуральные числа, пока не найдётся n такое, $g(n)=\langle x,y\rangle$; если нашлось, то взять первое такое n и в качестве результата выдать то y, что $g(n)=\langle x,y\rangle$». Заметим, что если f(x) не определено, то алгоритм работу не заканчивает. Утверждение 4.4.4 доказано.

Задача а) доказать, что образ и прообраз перечислимого множества при вычислимой функции перечислимы; б) доказать, что непустое множество A натуральных чисел разрешимо тогда и только тогда, когда оно есть множество значений вычислимой возрастающей последовательности; в) доказать, что любое бесконечное перечислимое множество содержит бесконечное разрешимое подмножество; г) доказать, что если A и B – перечислимые множества, то найдутся перечислимые множества C и E такие, что $C\subseteq A$, $E\subseteq B$, $C\cap E=\varnothing$ и $C\cup E=A\cup B$.

4.5 Универсальная вычислимая функция

Пусть X и Y – множества «конструктивных» объектов. Рассмотрим все алгоритмы, исходными данными которых являются элементы X, а значения принадлежат Y. Через Выч(X,Y) обозначим множество всех вычислимых функций из X в Y. Также, пусть P – третье множество «конструктивных» объектов. Скажем, что функция $F : P\times X\to Y$ называется универсальной для класса функций Выч(X,Y), если для всякой функции f из этого класса найдётся такое p из P, что $(\forall x\in X)(F(p,x) \cong f(x))$. Совершенно очевидно, что для класса Выч (X,Y) существует универсальная функция, т.к. данный класс счётен и если $f_0, f_1, \ldots f_n,..$ – пересчет этого класса, то пусть P=N и полагаем $F(n,x) \cong f_n(x)$ для всех $n\in N$, $x\in X$.

Для приведённой универсальной функции полагаем: $F_p(x) \cong F(p,x)$ для всех x из X.

Утверждение 4.5.1. Для любых множеств «конструктивных» объектов X и Y существует множество «конструктивных» объектов P и вычислимая функция $F : P\times X\to Y$, которая является универсальной для класса Выч (X,Y).

Доказательство. Мы докажем Утверждение 4.5.1. С этой целью мы постулируем существование алгоритмического языка, на котором можно записать программу любого алгоритма с множеством исходных данных X и результатов применения из Y. Эти программы есть элементы какого-то множества «конструктивных» объектов P. Теперь определяем

функцию F: $F(p,x)=y \Leftrightarrow$ (p является синтаксически правильной программой, дающей на входе x результат y). Функция F – вычислима (алгоритм, вычисляющий F, называется интерпретатором введённого языка программирования) и универсальна, т.к. если $f \in$ Выч(X,Y) и вычисляется алгоритмом $\mathfrak{I}$ и если p – программа для $\mathfrak{I}$, тогда для некоторого p $(\forall x \in X)\ (f(x) \cong F(p,x))$. Утверждение 4.5.1 доказано.

Замечание. Если $F_p = f$, то соответствующих f программ p может быть много.

Если в Утверждении 4.5.1 в качестве P взять множество натуральных чисел N, то получим такое

Следствие 4.5.2. Для любых множеств «конструктивных» объектов X и Y существует вычислимая функция $H : N \times X \to Y$, универсальная для класса Выч(X,Y). Действительно, по Утверждению 4.5.1 есть множество P и универсальная функция F. Если h – вычислимая биекция из N в P, то пусть $h(n)=p_n$. Положим $H(n,x) \cong F(p_n,x)$. Ясно, что $H : N \times X \to Y$ – вычислима и является универсальной функцией для класса Выч (X,Y).

Замечание Если $H : N \times X \to Y$ универсальная функция и $f \in$ Выч(X,Y), то программу вычисления f относительно H называют номером f относительно H, а отображение $n \to H_n$ (последняя функция получается из H фиксацией первого аргумента) – нумерацией вычислимых функций, соответствующей универсальной функции H.

Пусть теперь $H : N \times N \to N$ есть универсальная

вычислимая функция для класса Выч(N,N). Пусть функция f определена так: $f(n)\cong H(n,n)+1$. Но таким образом мы все же не пришли к противоречию (какому?), т.к. значение H(s,s) м.б. не определено (здесь s есть номер функции f выше относительно нумерации $n\to H_n$).

Предположим теперь, что f^ - всюду определенное продолжение функции f (т.е. f^ всюду определена и там, где определена f имеем f(x)=f^(x); сама f определена так: $f(n)\cong H(n,n)+1$, где H – универсальная функция для класса Выч((N,N)). Теперь уже не верно, что $f(n)\cong H_n(n)$, т.к. левая часть равенства определена, а правая – нет. Если же правая часть определена, то и f(n) определено и равно $H_n(n)+1$ и f^(n) совпадает с f(n) и не равно $H_n(n)$. Тогда f^ отлична от всех функций H_n и поэтому не является вычислимой функцией. Следовательно, доказано

Утверждение 4.5.3. Существует вычислимая функция $f : N\to N$, которая не имеет всюду определенного вычислимого продолжения.

Утверждение 4.5.4. Существует перечислимое и неразрешимое множество.

Доказательство. Если множество A есть область определения функции f из Утверждения 4.5.3, то A – перечислимо. Если бы A было разрешимо, то легко бы было построить всюду определенное вычислимое продолжение уже упомянутой функции f (постройте это продолжение самостоятельно).

Задача а) множество $B\subseteq N\times N$ называется универсальным, если для всякого перечислимого

множества $A \subseteq N$ найдется такой номер n, что $A=\{x \in N : \langle n,x \rangle \in B\}$;
доказать, что существует универсальное перечислимое множество; б) доказать, что всякое универсальное множество является неразрешимым; в) доказать, что не существует всюду определенной вычислимой функции, универсальной для семейства всех всюду определенных вычислимых функций.

4.6 Тезис Черча

Предположим, что неформальное определение вычислимой функции через понятие алгоритма удалось некоторым образом формализовать (таких формализаций было несколько и оказалось, что все они эквивалентны). Тогда можно высказать следующий философский принцип (который нельзя как доказать, так и опровергнуть). Этот принцип носит название Тезис Черча (по имени автора, впервые его выдвинувшего).

Тезис Черча. Всякая вычислимая (неформально) функция является формально вычислимой (в данной предложенной формализации).

Оглавление

Св. план 2004г., поз. 87

Хаханян Валерий Христофорович

Элементы математической логики
и теории алгоритмов

Учебное пособие

Подписано в печать	Формат	Тираж
Усл.-изд. л.	Заказ №	Цена

127994 Москва, ул.Образцова, 15
Типография МИИТа.
68