КОНТЕНТ

Элементы математической логики

В.Х.Хаханян (кафедра «Математика»)

Часть I. Логика высказываний

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 использовали математический аппарат, то предмет такого рода изучения и может быть назван математической логикой.

Конечно, не стоит себе представлять, что логика есть просто часть математики, однако именно использование аппарата математики делает логику строгой наукой. И тем не менее, дело вовсе не сводится к верному использованию математики. Приведу в подтверждение только один пример, взятый из книги Р. Смаллиана «Как же называется эта книга». «Случай …поднимает вопрос о том, может ли человек лгать, не зная, что он лжёт. Ответ на такой вопрос отрицательный. Лгать означает высказывать не ложное утверждение, а утверждение, которое тот, кто его высказывает, *считает* ложным. Действительно, если кто-то высказывает утверждение, считая его ложным, а оно оказывается истинным, то можно сказать, что этот кто-то лжёт. Мне кажется, что истинным содержанием логики является «сплав» собственно логики и хорошо подобранного формального (математического) аппарата, помогающего ясно и точно разобраться в тонких нюансах логических рассуждений».

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, важные, элементы автомобиля). Современная математическая логика, наряду с присущей ей фундаментальностью, является обширным и разветвлённым разделом именно математики. Математическая логика должна быть, как и сама математика, точной наукой: иметь дело с точными понятиями и методами. В последние десятилетия интерес к математической логике 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.

Лекция 1

Исходные понятия математической логики.

1.1 Язык математической логики.

Основными понятиями математической логики являются <u>высказывания</u>, <u>предикаты</u>, <u>логические связки</u> и <u>кванторы</u> (мы не даем формального описания какого-либо языка, но несколько ниже мы приведём примеры таких языков для исчисления высказываний и исчисления предикатов). Сейчас же 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 $\to$ («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: $S = R \to (P \wedge Q)$. Читатель может потренироваться в приведении подобных примеров. Большое количество таких примеров имеется в начальной главе книги Э. Мендельсона «Введение в математическую логику».

Аналогом понятия предикат является понятие группы слов, характеризующих 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, $f\colon M^n \Rightarrow \{0, 1\}$, 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 пар 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 предикатов и такой способ связан с применением кванторов. Пусть P(x) и Q(x,y) – рассмотренные выше предикаты. Тогда $\forall x P(x)$ («для всякого x из области M (M – всегда подразумеваемая область) P(x)=1») и $\exists y Q(x,y)=H(x)$ («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 $\forall$ (для всякого или всеобщности (for all)) и $\exists$ (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 взять x), а тогда утверждение $\forall x \exists y Q(x,y)$ – 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 (не точный, вообще говоря) этих понятий. Но теперь мы перейдём к более формальной стороне вопроса.

1.2 Высказывания и высказывательные формы. Логические операции над высказываниями.

В пункте 1.1 мы уже получили представление о логических связках 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**.

Вопрос. Какие примеры выше являются высказываниями, а какие – высказывательными формами? Является ли высказывание высказывательной формрой?

Обратимся теперь к введённым выше логическим операциям (связкам). К ним мы ещё добавим логическую операцию (бинарную) $\equiv$ («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.

Вопросы и упражнения к Лекции 1

1.Выразить связки $\to$ и $\vee$ через связки $\wedge$ и $\neg$. Убедиться в правильности через логические таблицы.

Ответ: [$A\to B=\neg A\vee B=\neg(\neg\neg A\wedge\neg B)=\neg(A\wedge\neg B)$].

2. Тот же вопрос для пар связок $\to$, $\wedge$ и $\vee$,$\neg$.

3. Аналогичный вопрос для пар связок $\wedge$,$\vee$ и $\to$,$\neg$.

Ответ: [$A\vee B=\neg(\neg A\wedge\neg B$; $A\wedge B=\neg(A\to B)$].

4. А существует ли одна связка, через которую можно выразить все ранее приведённые?

Ответ: да, существует, и не одна! Это т.н. штрих Шеффера. См. Утверждение 2.3.3 ниже.

5. Что такое связанная переменная? Свободная переменная?

6. Может ли одна и таже переменная быть связанной и свободной в одном и том же выражении?

Лекция 2.

Классическое исчисление высказываний

2.1 Истинностные таблицы.

Придадим всему сказанному выше ещё более формальное описание. Пропозициональной переменной (пп) называется переменная, пробегающая над множеством высказывательных форм (в том числе и высказываний). 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. Пропозициональная форма (пф) получается с помощью следующего индуктивного определения.

(i) любая пп есть пф; (ii) если A и B – пф, то $(\neg A)$, $(A \wedge B)$, $(A \vee B)$, $(A \to B)$, $(A \equiv B)$ 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 $A \vee B \to C$ может быть представлена такой таблицей:

A	B	C	$A \vee B$	$A \vee B \to C$
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

Упражнение. Составьте таблицу истинностности для $(A\to B)\vee(\neg A)$;
Решение.

A	B	$A\to B$	$\neg A$	$(A\to B)\vee(\neg A)$
0	0	1	1	1
0	1	1	1	1
1	0	0	0	0
1	1	1	0	1

Введём ряд соглашений о более экономном употреблении скобок в записях пф. 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 $\to$, а затем $\equiv$).Пример: $A\to B\to C$ есть $((A\to B)\to C)$; $A\vee\neg B\to C\equiv A$ есть $(((A\vee(\neg B))\to C)\equiv A)$.

Упражнение. Проверить, что различная расстановка скобок в формуле $A\to B\to C$ даёт различные таблицы истинностности.

Отметим теперь, что если в пф имеется n различных пп, то возможны 2^n различных распределений истинностн 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 $A\to B$ 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, $(A\to B)\to(\neg B\to\neg A)$ – закон контрапозиции и т.д. Отметим еще, что $A\wedge(A\to B)$ 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. $(A\equiv B)\equiv((A\to B)\wedge(B\to A))$.
Ответ: 1. Нет. 2. Нет. 3. Да. Указание: вычислите таблицы истинностности.

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

Задача. Приведите пять примеров пф, которые являются противоречиями. Указание: напишите пять примеров тавтологий и «навесьте» на них отрицание.

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 высказывание), 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 A и $A\to B$ – тавтологии, то B – тавтология.

Замечание. Вы уже 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 A и $A\to B$ – тавтологии, то при любом распределении (фиксированном) истинностных значений входящих в них пп они принимают значение 1. Если бы B принимала при этом значение 0, то пф $A\to B$ принимала бы значение 0 также и мы получили бы противоречие. Следовательно, B принимает значение 1.

Замечание. Не лучшее доказательство. Попробуйте рассудить «более логично».

Утверждение 2.2.2. Если A – тавтология с пп $A_1,\ldots,A_n$ и пф B получается из пф A подстановкой пф $B_1,\ldots,B_n$ вместо пп выше, то пф B – также тавтология (подстановка в тавтологию **любых пф** приводит снова к тавтологии).

Докажите Утверждение 2.2.2 самостоятельно. Вспомните, что такое тавтология.

Утверждение 2.2.3 Если пф B_1 получается из пф A_1 подстановкой пф B вместо одного или большего числа вхождений пф A, то $(A\equiv B)\to(A_1\equiv B_1)$ есть тавтология, т.е. из логической эквивалентности пф A и B следует логическая эквивалентность пф A_1 и B_1.
Доказательство 2.2.3. Т.к. $A\equiv B$, то подстановка B вместо A в любом вхождении A в A_1 не изменит таблицу истиностности последней, т.е. B_1 будет принимать те же значения истинности, что и A_1, что и даёт тавтологию формулы $A_1\equiv B_1$.

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 $\neg$, $\wedge$, $\vee$.

Утверждение 2.3.1 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 $(\neg,\to)$ 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 $\wedge$, $\vee$, $\to$ 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.

A	B	$\downarrow$	$\vert$
1	1	0	0
0	1	0	1
1	0	0	1
0	0	1	1

Если связки p(A,B) достаточно для выразимости любой пф, то если p(1,1)=1 и $\neg$ нельзя было бы выразить, т.е. p(1,1)=0. Совершенно аналогично, p(0,0)=1. Если второе и третье места есть 0,0 или 1,1 соответственно, то получим наши связки. Если же на этих местах стоят 0,1 или 1,0 соответственно, то формы $p(A,B)\equiv\neg B$ и $p(A,B)\equiv\neg A$ оказываются тавтологиями и тогда p(A,B) выражена через $\neg$, а это не так (через $\neg$ можно выразить либо тождественную истину, либо тождественную ложь).

Задачи.

1. Выразите через связки $\downarrow$, $|$ сначала $\wedge$, а затем $\neg$.
2. Докажите, что ни одна из пар связок $(\wedge,\vee)$ и $(\neg,\equiv)$ не является достаточной для выражения всех истинностных функций (рассмотрите таблицы истинности для соответствующих связок).

Указание.

A	B	A→B.	
1	1	1	Заметьте, что в последней строке напротив двух нулей стоит 1 и получить ее с помощью только
0	1	1	связок $\vee$ и $\wedge$ никак нельзя, т.е. $\rightarrow$ нельзя выразить
1	0	0	через эти связки. Для другой пары связок дать
0	0	1	аналогичное рассуждение.

Приведём теперь ряд логических задач из книги Р. Смаллиана, которые можно решить с помощью составления логических таблиц, но рекомендуется решить с помощью логических рассуждений.

Предположим, что рыцарь – человек, который всегда говорит правду, что лжец – человек, который всегда лжёт и что нормальный человек иногда говорит правду, а иногда лжёт.

А) задачи про рыцарей и лжецов.

1. Трое людей А, В, и С разговаривали между собой. У А спросили: «Вы рыцарь или лжец?», на что А ответил очень неразборчиво. Тогда спросили у В «Что сказал А?». «А сказал, что он лжец»- ответил В. Но тогда С сказал, что В лжёт. Кто из островитян В и С рыцарь и кто – лжец? А кто такой А?

   Ответ: В – лжец, С – рыцарь; установить, кто такой А - нельзя.

   Решение. Сделаем сначала общее замечание по решению этой и всех последующих задач: если в задаче несколько участников, то нужно вычислить таблицу истинностных значений как булеву функцию и проверить, какой вариант подойдёт. Но гораздо интереснее рассудить логически.

   Ни рыцарь, ни лжец не могут сказать «Я лжец». Поэтому В лжёт и он лжец. Следовательно, С сказал правду и он рыцарь.

2. Из двух персонажей A и B нужно узнать, кто рыцарь, а кто лжец, если A сказал: «Среди нас есть лжец».
   Ответ: A – рыцарь, B – лжец.
   Решение. Если A – лжец, то высказанное утверждение ложно и оба рыцари, но это противоречит посылке и A – рыцарь и сказал истину, а тогда B – лжец.
3. A говорит: «Или я лжец, или B рыцарь». Кто из A и B есть кто?
   Ответ: A и B оба рыцари.
   Решение. По аналогии с предыдущей задачей. Но можно и вычислить таблицу истинностности
4. Единственный персонаж A говорит: «Или я лжец, или снег всегда чёрный». Какие выводы можно сделать?
   Ответ: Составитель задачи – не рыцарь!!
   Противоречивое условие задачи!!
5. A говорит: «Я лжец, а B – не лжец». Кто из них рыцарь, а кто – лжец?
   Ответ: A и B оба лжецы.
   Решение. Если A рыцарь, то сказал бы правду, т.е. что он – лжец. Следовательно, A – лжец. A тогда он солгал, но т.к. левая часть Конъюнкции истинна, то должна быть ложна вторая часть, т.е. B – тоже лжец.
6. Вы встречаете рыцаря или лжеца, помните, что его зовут то ли Вася, то ли Витя, но не помните, как. Вы спрашиваете «Как Вас зовут» и слышите в ответ «Витя». Как его зовут?
   Ответ: Это нельзя определить, т.к. ни одна из четырёх комбинаций из рыцарей и лжецов не подойдёт под условия задачи.

Б) задачи про рыцарей, лжецов и нормальных людей.

1. Из трёх людей один – рыцарь, другой – лжец и третий – нормальный человек. Они высказывают такие утверждения. A: «Я нормальный человек»; B: «A сказал правду»; C: «Я не нормальный человек ». Кто такие A, B и C?
   Ответ: Это лжец, нормальный человек и рыцарь в порядке следования.
   Решение. A не может быть рыцарем и значит B сказал правду. Но если B – не нормальный человек (таким является A!!?) и он – рыцарь. Тогда C – лжец. Но лжец не может о себе сказать, что он – нормальный человек. Получили противоречие. Но тогда A – лжец! Островитянин B тогда солгал и он – нормальный человек и, следовательно, C – рыцарь.

Замечание Если решать перебором, то рассматриваются $3\times3=9$ случаев. Совет: ещё раз медленно «пройдите» по решению.

2. Два человека высказывают такие утверждения. А: «В – рыцарь»; В: «А – не рыцарь». Докажите, что хотя бы один из них говорит правду и что это не рыцарь. Разберите возможные случаи.

   Решение. Раберём случаи.

   а) Пусть А говорит правду. Тогда В – рыцарь и говорит правду. Тогда А – не рыцарь, т.е. А – лицо, говорящее правду, не являясь рыцарем.

   в) Пусть А лжёт. Тогда В – не рыцарь, но В должен говорить правду, т.к. А не является рыцарем. Следовательно, В говорит правду, не будучи рыцарем.
3. Пусть А и В говорят. А: «В – рыцарь»; В: «А – лжец». Тогда либо один из них говорит правду и это не рыцарь, либо один из них лжёт и это не лжец.

   Решение. Разберём случаи.

   а) Если В говорит правду, то А – лжец и лжёт. Но тогда В – не рыцарь и говорит правду, не будучи рыцарем.

   в) В лжёт, тогда А – не лжёт. Но говоря о В А заведомо лжёт, т.к. В не м.б. рыцарем, если не говорит правду. Следовательно, А лжёт, не будучи лжецом.
4. Пусть лжецы имеют минимальный ранг, нормальные люди – средний и рыцари – высший ранг. Два человека говорят. А: «По рангу я ниже В». В: «Не правда». Можно ли определить ранг А или В? Можно ли установить истинностное значение каждого из двух утверждений?

   Ответ: А и В – нормальные люди; высказывание А ложно, высказывание В истинно.

Вопросы и упражнения к Лекции 2.

1. Что такое таблица истинности?
2. Что такое пропозициональная форма, пропозициональная переменная?
3. Что такое тавтология и противоречие?
4. Что такое полная система связок?

Лекция 3

Классическое исчисление высказываний (продолжение)

3.1 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 или теории доказательств), 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):

а) задано счётное число исходных символов – **алфавит теории T**; конечные последовательности (слова) этих символов называются выражениями теории T;

в) имеется подмножество выражений теории T, называемых **формулами теории T**; почти всегда 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;

c) выделено некоторое множество формул, называемых **аксиомами теории T**; здесь также часто (но далеко не всегда) 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, состоят ли данное множество 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 А; такой вывод называется выводом формулы А в теории Т.

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

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

Простейшие свойства выводимости:

а) если $\Gamma \subseteq \Delta$ и Г □ А, то Δ □ А; в) Г □ А тогда и только тогда, когда в Г существует <u>конечное</u> подмножество Δ такое, что Δ □ А; с) если Δ □ А и Г □ В для любого В из Δ, то Г □ А. Все приведённые свойства имеют простое толкование, связанное с понятием вывода Попробуйте самостоятельно «перевести» эти свойства на обычный язык. Например, а) если есть вывод из Г и Г есть подмножество Δ, то, конечно, есть вывод и из Δ.

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 $(A\to B)$ также фл; с) других фл, кроме полученных по пунктам а) и в), нет.
3) следующие фл суть аксиомы теории L:
A1. $(A\to(B\to A))$; A2. $(A\to(B\to C))\to((A\to B)\to(A\to C))$; A3. $((\neg B\to \neg A)\to((\neg B\to A)\to B))$, где A,B и C – любые фл.
4) правило вывода (modus ponens (MP)): B есть непосредственное следствие A и $A\to B$.
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.** 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 $\neg(A\to\neg B)$; $(A\vee B)$ 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 3.1.1. Для любой фл A $\square_L$ $A\to A$ (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 A1;
(9) $A\to A$ из 3 и 4 по MP. Вывод завершен.
Задача. Постройте выводы в **L** для следующих фл:
а) $(\neg A\to A)\to A$;
в) $A\to C$ из гипотез $A\to B$ и $B\to C$;
с) $B\to(A\to C)$ из гипотезы $A\to(B\to C)$;
Решения. а) По схеме A3 $(\neg A\to\neg A)\to((\neg A\to A)\to A)$ подставляем A вместо B. $(\neg A\to\neg A)$ выведена выше. По MP имеем требуемое.
в) По схеме A1 $(B\to C)\to(A\to(B\to C))$ (вместо A ставим $B\to C$, вместо B - A. Применяем MP и получаем $A\to(B\to C)$. Из схемы A2 и

полученной формулы по МР получаем $(A\to B)\to(A\to C)$. Из посылки $(A\to B)$ и полученной последней формулы получаем $A\to C$.
с) По схеме А1 $A\to(B\to C)\to[B\to(A\to(B\to C))]$ (что вместо чего в А1 подставляется?) По МР и посылке имеем $[B\to(A\to(B\to C))]$. По А2 $B\to(A\to(B\to C))\to[B\to(A\to B)\to(B\to(A\to C))]$ (тот же вопрос, что и ранее (указание: просто на все формулы «навешиваем» впереди B)). По МР и выведенной раньше формуле $B\to(A\to(B\to C))$ получим $[B\to(A\to B)\to(B\to(B\to(A\to C))]$. Т.к. посылка $(B\to(A\to B)$ – пример А1, то применяем снова МР и получаем требуемое.

3.2. Теорема о дедукции для исчисления **L**.

Теперь докажем одну из важнейших теорем для исчисления высказываний – теорему о дедукции, которая является важным вспомогательным правилом вывода и часто применяется в неформальных математических доказательствах.
3.2.1. **<u>Теорема о дедукции.</u> Если Г – множество фл, А и В – фл и $\Gamma, A \vdash B$, то $\Gamma \vdash A\to B$ (Эрбран, 1930 г.).**
Доказательство. Пусть $B_1,\dots,B_n$ – вывод из $\Gamma\cup\{A\}$ и $B=B_n$. Индукцией по длине вывода докажем, что $\Gamma \vdash A\to B$.
<u>Основание индукции.</u> Тогда $B=B_1$ есть либо элемент Г, либо $B=A$, либо В – аксиома. В первом и третьем случаях, используя аксиому $B\to(A\to B)$, получаем $\Gamma \vdash A\to B$ по МР. Во втором случае в силу Утверждения 3.1.1 имеем также $\Gamma \vdash A\to B$ и основание индукции завершено (более детально проверьте этот пункт).
<u>Индукционный шаг</u>. 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 МР 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 (обязательно дайте точное доказательство!). В последнем случае применяем индукционное предположение, согласно которому $\Gamma \vdash A\to B_j$, $\Gamma \vdash A\to B_m$, т.е. $\Gamma \vdash A\to(B_j\to B_n)$. По схеме аксиом А2) имеем $\vdash(A\to(B_j\to B_n))\to((A\to B_j)\to(A\to B_n))$. Теперь по правилу МР $\Gamma \vdash (A\to B_j)\to(A\to B_n)$ и снова по МР $\Gamma \vdash(A\to B_n)$. Доказательство индукционного шага и всей теоремы о дедукции завершено.

Отметим, что доказательство носит **конструктивный** характер: оно позволяет по данному выводу В из Г и А построить вывод $A\to B$

из Г. Также отметим, что при доказательстве были использованы только схемы A1 и A2. Теорема о дедукции позволяет сократить долгий и не простой иногда вывод нужной формулы.

Следствие 3.2.2. $A \to B,\ B \to C \vdash A \to C$; $A \to (B \to C),\ B \vdash A \to C$.

Задача. Докажите Следствие 3.2.2 самостоятельно, используя **теорему о дедукции.**

Утверждение 3.2.3. 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 3.2.3., построив в **L** выводы.

В качестве примера докажем (a):

1) $(\neg B \to \neg\neg B) \to ((\neg B \to \neg B) \to B)$ схема аксиом A3

(укажите, что в этой схеме аксиом есть фл A и фл B);

2) $\neg B \to \neg B$ по Утверждению 3.1.1;

3) $(\neg B \to \neg\neg B) \to B$ из 1) и 2), в пункте 3.1.1. в **Задаче** вывод c);

4) $\neg\neg B \to (\neg B \to \neg\neg B)$ схема аксиом 1;

5) $\neg\neg B \to B$ из 3) и 4), в пункте 3.1.1 в **Задаче** вывод в).

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

Утверждение 3.2.4**.** Всякая теорема теории **L** является тавтологией.

Мы оставляем доказательство Утверждения 3.2.4 читателю (нужно убедиться, что любая аксиома есть тавтология и что правило MP по тавтологиям даёт тавтологию, см. Утверждение 2.2.1).

Указание. Для доказательства 3.2.4. воспользуйтесь таблицами истинностности.

Утверждение 3.2.5. 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 A принимает значение 1 и утверждается , что $B_1, \neg B_2 \vdash \neg B_1 \to B_2$.

Доказазательство 3.2.5. Индукция по числу n вхождений пс в А. Основание индукции: n=0 и А есть просто пб B_1. Утверждение сводится к доказательству $\neg B_1$ □ $\neg B_1$ или B_1 □ B_1 (см. Утверждение 3.1.1 и примени теорему о дедукции).

Индукционный шаг: пусть Утверждение 3.1.5 верно при любом к< n. 1 случай: $A = \neg B$ и число вхождений пс в B меньше n. Если при заданном распределении истинностных значений пб B принимает значение 1, тогда А принимает значение 0 и B\`=B, а A\`= $\neg$A. По предположению индукции имеем B_1\`,…,$B_к$\` □ B. Но тогда по Утверждению 3.2.3 (b) и MP B_1\`,…,$B_к$\` □ $\neg\neg$B, которое и есть А. Пусть теперь B принимает значение 0, тогда А принимает значение 1 и B\`= $\neg$B и A\`=A. По предположению индукции B_1\`,…,$B_к$\` □ $\neg$B, а это и есть А. 2 случай: $A=B\rightarrow C$. Число вхождений пс в B и C меньше n и по индукционному предположению B_1\`,…,$B_к$\` □ B\` и $B_1$\`,…,$B_к$\` □ C\`. Если B принимает значение 0, то А принимает значение 1 и B\`= $\neg$B и A\`=A. Но тогда B_1\`,…,$B_к$\` □ $\neg$B и по Утверждению 3.2.3 (c) B_1\`,…,$B_к$\` □ $B\rightarrow C$, т.е. А. Если С принимает значение 1, то А принимает значение 1 и C\`= C, A\`=A. Т.к. B_1\`,…,$B_к$\` □ C(=C\`), то по схеме аксиом A1) $B_1$\`,…,$B_к$\` □ $B\rightarrow C$(=A\`). Пусть, наконец, B принимает значение 1 и С принимает значение 0. Тогда А принимает значение 0 и A\`= $\neg$A, B\`=B и C\`= $\neg$C. По предположению индукции имеем $B_1$\`,…,$B_к$\` □ B и $B_1$\`,…,$B_к$\` □ $\neg$C. Тогда по Утверждению 3.2.3 (f) получаем, что $B_1$\`,…,$B_к$\` □ $\neg(B\rightarrow C)$, что и есть А. Индукционный шаг, а с ним и Утверждение 3.2.5 доказаны.

Вопросы и упражнения к Лекции 3.

1. Дайте определения: алфавита, выражения, теоремы, вывода в формальном исчислении.
2. Сформулируйте теорему о дедукции и поясните, почему она является **вспомогательным правилом вывода**.
3. Сформулируйте аксиомы и правила вывода для исчисления **L**.
4. Сколько аксиом в исчислении **L**? А сколько схем аксиом?
5. Сколько правил вывода в исчислении **L**?
6. Что означает, что формула А является следствием множества формул Г в исчислении **L**? Может ли Г быть бесконечным множеством?

Лекция 4.

Классическое исчисление высказываний (окончание)

4.1. Полнота и разрешимость исчисления **L**.

Утверждение 4.1.1. **Теорема о полноте. Если фл А теории L является тавтологией, то она есть теорема теории L**.

Доказательство (Кальмар). Пусть А есть тавтология и $B_1,\ldots,B_к$ - пб, входящие в А. В силу Утверждеия 3.2.5 при всяком распределении истинностных значений пб имеем $B_1`,\ldots,B_к`$ □ А (т.к. А – тавтология). Отсюда получаем, что если $B_к$ принимает значение 1, то $B_1`,\ldots,B`_{к-1},B_к$ □ А, а если $B_к$ принимает значение 0, то $B_1`,\ldots,B`_{к-1},\neg B_к$ □ А. А тогда по теореме о дедукции и по Утверждению 3.2.3 (g) $B_1`,\ldots,B`_{к-1}$ □ А. Продолжая этот процесс исключения пб, мы получим □ А. Теорема о полноте доказана.

Следствие 4.1.2. Если выражение В содержит все пропозициональные связки и является сокращением для некоторой фл А теории **L**, то В является тавтологией тогда и только тогда, когда А есть теорема теории **L**.

Доказательство. Сокращения для связок являются эквивалентными им пропозициональными формами и в силу 2.2.3. их подстановка не изменит логической эквивалентности формул А и В, т.е. формулы А и В являются тавтологиями одновременно. По теореме о полноте В тавтология тогда и только тогда, когда А является теоремой.

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

Утверждение 4.1.3. **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 3.2.3 (с) □ $\neg A\to(A\to B)$, то из противоречивости **L** и правила МР в **L** была бы выводима любая фл В (этот факт был бы верен в любой теории с правилом МР, в которой выполнено Утверждение 3.2.3 (с)). Теорию, в которой не все фл

выводимы, иногда называют **абсолютно непротиворечивой** и такое определение применимо к теориям, не содержащим пс отрицания.
Утверждение 4.1.4. **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**.

4.2. Другие аксиоматизации для исчисления высказываний.

Приведём здесь только один, самый распространённый, пример аксиоматизации исчисления высказываний. Обозначим эту систему через $\mathbf{L_4}$.

Пс служат $\to$, $\wedge$, $\vee$, $\neg$ и упоминавшиеся в формализации для **L** скобки и пб. Единственное правило вывода – МР. 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 связки $\equiv$ применяется обычное сокращение.
Задача. Докажите, что системы **L** и $\mathbf{L_4}$ имеют одно и то же множество теорем (с точностью до принятых сокращений). Используйте **теорему о дедукции**. Не забудьте, что при погружении $\mathbf{L_4}$ в **L** нужно связки-сокращения заменить на их оригиналы в языке **L**.

4.3. 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 многозначной логики – двузначная логика).

Пусть числа 0,1, … , n являются **истинностными значениями** и выберем какое-либо число m такое, чтобы $1 \le m \le n$. Числа 0, … , m назовём **выделенными истинностными значениями**. Выберем некоторое число **истинностных таблиц**, которые представляют собой 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 этой ситуации говорят, что задана **многозначная логика М.** Аксиоматическая теория, содержащая пб и связки логики **М**, называется подходящей для логики **М** в том и только в том случае, если множество теорем этой теории совпадает с множеством выделенных пф логики **М** (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 3.2.4 и 4.4.1 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 4.3.1. Схема аксиом A1 является независимой. Доказательство. Рассмотрим таблицы:

A	¬A
0	1
1	1
2	0

A	B	A→B
0	0	0
1	0	2
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, что правило MP сохраняет свойство выделенности. Нетрудно также проверить, что всякая аксиома, получающаяся по схемам A2 или A3, также является выделенной. Также, 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 относительно многозначной логики, а только так называемую корректность, т.е. аналог Утверждения 3.2.4.

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, т.к. они просто не меняютсвой вид (в них связка $\neg$ не входит). Правило MP также сохраняет свойство A иметь в качестве P(A) тавтологию. Теперь достаточно взять следующий частный пример схемы A3: $B = (\neg A \to \neg A) \to ((\neg A \to A) \to A)$, вычислить P(B) (вычислите!) и убедиться, что P(B) не является тавтологией. Если подставить в P(B) 0 вместо A, то получим 0. Таким образом, схема аксиом A3 является независимой от схем аксиом A1 и A2.

Вопросы и упражнения к Лекции 4.

1. Какая формальная теория называется непротиворечивой?
2. Дайте другое (эквивалентное) определение понятия непротиворечивой теории.
3. Сформулируйте теорему о полноте исчисления высказываний.
4. Почему исчисление высказываний является разрешимой теорией?
5. Если в пф входит 10 пп, то сколько строк будет в таблице истинностности такой пф?
6. Почему система **L** непротиворечива?

7. Что такое полная формальная теория?
8. Опишите понятие независимой аксиомы (схемы аксиом) в данной формальной теории.
9. Что такое многозначная логика?
10. Какая формальная теория называется подходящей для данной многозначной логики?