Оглавление

Лекция 1

Предпосылки возникновения математической логики

Где-то на рубеже 19 и 20 веков математическое сообщество было потрясено открытием в теории множеств, построенной Г. Кантором, которая замышлялась, как строгий фундамент математики, противоречий, антиномий, когда оказалось возможным доказать одновременно некоторое утверждение и его отрицание.

Одним из этих парадоксов является парадокс Рассела, который может быть проанализирован следующим образом (см. также Дополнение Д1.1 Учебника[1], но там парадокс не проанализирован полностью).

Начнем с примера, предложенного Гильбертом.

Рассмотрим множество Y, элементами которого являются множества, содержащие не менее трех элементов.

Запишем это так:

$Y = \{X :| X | \geq 3\}$.

Тогда, скажем, $\{1,2,3\},\{1,2,3,4\},\{1,2,3,4,5\} \in Y$, то есть мы набрали три элемента для Y и, тем самым, оно обладает свойством своих элементов и, стало быть, является элементом самого себя: $Y \in Y$. Это необычно, так как в математической практике мы имеем дело с множествами, не являющимися элементами самих себя. Гильберт предложил назвать такие множества нормальными, а множество всех нормальных множеств может быть через коллективизирующее свойство описано так:

$Z = \{X : X \notin X\}$.

Проанализируем тогда ситуацию с самим множеством Z: какое оно – нормальное или нет?

Если допустить, что оно само нормальное, то есть $Z \notin Z$, оно должно принадлежать множеству всех нормальных множеств, то есть самому себе. Но тогда, не будучи нормальным, оно не должно принадлежать себе как множеству всех нормальных. Получается такое странное утверждение:

---

[1] Белоусов А.И., Ткачев С.Б. Дискретная математика. – М.: Изд-во МГТУ им. Н.Э. Баумана. 2015 (5-е изд.). Далее – Учебник.

$Z \in Z \Leftrightarrow Z \notin Z$

Но это, хоть и неприятно, но пока не парадокс. Докажем, что имеет место конъюнкция этих взаимоисключающих утверждений.

Рассуждаем от противного. Пусть $Z \notin Z$. Это значит, что, будучи нормальным множеством, Z не принадлежит множеству *всех* таких множеств, то есть существует нормальное множество, не принадлежащее множеству всех нормальных множеств. Полученное противоречие доказывает, что имеет место утверждение $Z \in Z$, откуда, в силу доказанного ранее, $Z \notin Z$. Это значит, что имеет место конъюнкция $(Z \in Z)\&(Z \notin Z)$. Вот это и есть антиномия, когда удается строго доказать два противоречащих друг другу утверждения.

В этом суть парадокса Рассела. Сам Рассел любил его шутливо-сказочный вариант.

Предположим, что в некоторой деревне старой доброй Англии живет *парикмахер, который должен брить всех тех, кто не бреет себя сам*. В какое же положение он попадает? Если он будет себя брить, он должен немедленно прекратить это занятие, так он должен брить только тех, кто не бреет себя сам. Но как только он перестает себя брить, он сразу же попадает в категорию не бреющих себя и, следовательно, должен себя брить, что он, как мы видели выше, не имеет права делать. Наш парикмахер попадает в безвыходное положение.

В своей строгой форме, как парадокс теории множеств, парадокс Рассела является теоретико-множественным проявлением так называемых *парадоксов самоприменимости*.

Есть логический вариант – известный парадокс лжеца, человека, который только лжет (и никогда не говорит правду). Если он скажет: «Я лгу», то получается, что он лжет, что он лжет, то есть говорит правду, но если фраза «Я лгу» правдива, то в ней утверждается, что произнесший ее лжет.

Известен лингвистический парадокс самоприменимости.

Назовем прилагательное русского языка самоприменимым, если оно само, как слово, обладает тем свойством, о котором говорит. Таким будет, например, прилагательное ТРЕХ-СЛОЖ-НЫЙ, так как говорит о свойстве трехсложности и само состоит из трех слогов. Возьмем тогда прилагательное НЕСАМОПРИМЕНИМЫЙ. Если предположить, что несамоприменимо, то получится, что оно обладает тем свойством, о котором говорит и, следовательно, является самоприменимым. Но раз так, то оно не обладает тем свойством, о котором говорит. Противоречие.

Парадоксы самоприменимости не имеют никакого отношения к алгоритмической проблеме самоприменимости, неразрешимость которой мы доказали в теории алгоритмов. Там получалось, что нормальный алгорифм, предположенный полуразрешающим для этой проблемы, не может быть построен, так как должен быть одновременно применим и неприменим к своей записи, что невозможно. Это не парадокс, а обычное противоречие, возникающее в классическом доказательстве от противного.

Неприятная ситуация с парадоксами в канторовской теории множеств заставила математиков искать выход из положения.

Гильберт предложил программу, в которой предлагалось построить математическую теорию, рассматривающую другие математические теории с точки зрения наличия/отсутствия в них противоречий. Предлагалась, по существу, программа самообоснования математики. Философ уровня Гегеля сразу почувствовал бы здесь явно несостоятельную претензию, и сказал бы, что проект обречен на неудачу. Математика не может себя обосновать, как человек не может поднять себя за волосы от земли. Так оно потом и оказалось, но, как иногда бывает, попытка решить неразрешимую задачу дает в виде побочного продукта, так сказать, много интересных и плодотворных идей. В частности, с развитием во второй половине 20 века вычислительной техники и программирования, оказалось, что многие результаты, полученные в рамках гильбертовского проекта, важны в теории программирования, например, при разработке оптимизирующих преобразований программ.

Итак, отправимся по пути, предложенному Гильбертом.

Математическая теория, анализирующая другие математические теории, становится как бы над ними, оказывается *метаматематикой*. «Мета» по-гречески значит «после», «за». Знаменитый трактат Аристотеля «Метафизика» есть, на самом деле, запись его бесед со своими учениками и называлась «Та мета та физика», то есть то, что идет за «Физикой», основным философским трудом Аристотеля, в котором давалась общая картина мироздания, как она представлялась ученым умам в 4 веке до нашей эры. К науке физике в современном понимании этого слова труд Аристотеля не имеет почти никакого отношения, хотя там и фигурируют термины, которые до сих пор являются терминами физической науки (движение, сила, материя).

С появлением метаматематики, а это и есть математическая логика, математика раздвоилась. Доказательство стало не только инструментом математического исследования, но еще и его объектом. И необходимо было понятие доказательства формализовать, превратить его в математическое понятие. Точно также было формализовано понятие алгоритма, который долгое время был просто инструментом в вычислительной практике. Мы должны различать теоремы и их доказательства, как говорят, на *метауровне*; и теоремы и их доказательства на *объектном уровне*. К первым относятся теоремы и доказательства математической логики (метаматематики), ко вторым – теоремы и доказательства той теории (или тех теорий), которые изучает математическая логика. Без понимания этого раздвоения математики при изучении математической логики нельзя продвинуться ни на шаг. Мы будем говорить о метатеоремах и метадоказательствах и объектных теоремах и объектных доказательствах.

Интересно, что подобное раздвоение (или расслоение) на объектный и метауровень имеет место и в программировании. Мы реализуем рабочие (объектные) программы под управлением программ системных, тех же трансляторов (но не только их, конечно).

По поводу противоречий в теории множеств заметим следующее. Математики построили несколько теорий множеств, называемых аксиоматическими. Понятие множества в них не остается на интуитивном уровне, а дается через набор аксиом. Принимаются ограничения на применение коллективизирующих свойств. Вводятся так называемые праэлементы, которые не являются множествами, и из которых путем применения определенных правил строятся множества, называемые допустимыми. Тогда удается устранить многие противоречия, в том числе и парадокс Рассела, но проблема непротиворечивости таких теорий до сих пор не решена.

Превращение теорем и доказательств в объект производится путем определения понятия формальной аксиоматической теории.

Понятие формальной аксиоматической теории

Формальная аксиоматическая теория (дальше часто просто ***формальная теория*** или даже ***теория***) задается упорядоченной четверкой

$$T = < V, \Phi, P, A >,$$

где V - ***алфавит теории*** (по определению не более чем *счетное* множество), Φ - множество слов в алфавите V, элементы которого называются ***формулами теории***, P - множество ***правил вывода теории***, A - подмножество множества Φ, элементы которого называются ***аксиомами теории***.

Заметим, что множества правил вывода и аксиом могут не быть конечными, но должны быть, в определенном смысле, *конечно заданы*. Что именно подразумевается под термином «конечно заданный», будет ясно из рассмотрения конкретных формальных теорий.

Каждое правило вывода, по определению, имеет вид:

$$\frac{\Phi_1,\ldots,\Phi_m}{\Phi_0},$$

где $\Phi_0,\Phi_1,\ldots,\Phi_m$ суть формулы, причем $m\geq 1$, формулы $\Phi_1,\ldots,\Phi_m$ называются ***посылками правила***, а формула Φ_0 - ***заключением правила***. В этом случае говорят, что ***формула*** Φ_0 ***получена применением*** данного ***правила к формулам*** $\Phi_1,\ldots,\Phi_m$. Всякое правило вывода указанной структуры называется m***-посылочным правилом***. В частности, говорят об ***однопосылочных***, ***двухпосылочных*** и т.д. правилах.

Вывод из заданного множества формул Γ ***в теории*** T есть последовательность формул

$$\Phi_0,\Phi_1,\ldots,\Phi_n,\ldots$$

(конечная или бесконечная) такая, что для каждого $i\geq 0$ формула Φ_i есть либо элемент множества Γ, либо существует правило вывода в P, посылками которого являются формулы $\Phi_{j_1},\ldots\Phi_{j_p}$ данной последовательности при $j_1,\ldots,j_p<i$, а заключением – формула Φ_i.

Говорят, что ***формула*** Ψ ***выводится в теории*** T ***из множества формул*** Γ и пишут при этом $\Gamma\vdash_T\Psi$, если существует *конечный* вывод из Γ, последней формулой которого является формула Ψ. Заметим, что указание на теорию T в указанном выше обозначении опускают, если это не вредит точности.

Если множество формул Γ есть подмножество множества аксиом теории, то вывод из Γ называют ***доказательством теории***. В частности, тогда вывод формулы Ψ из Γ называют ***доказательством формулы*** Ψ (в теории T) и пишут: $\vdash_T\Psi$. Всякая формула теории, для которой может быть построено доказательство, называется ***теоремой теории***.

Дадим определение ***длины вывода*** $l_\Gamma(\Psi)$ формулы Ψ из множества Γ.

Если $\Psi\in\Gamma$, то $l_\Gamma(\Psi)=0$; если формула Ψ получена применением правила

$$\frac{\Phi_{j_1},\ldots,\Phi_{j_p}}{\Psi},$$

то $l_\Gamma(\Psi)=\max\limits_{1\leq k\leq p} l_\Gamma(\Phi_{j_k})+1.$

Нетрудно сообразить, что длина вывода формулы Ψ из множества Γ равна числу применений правил в данном выводе. Если $l_\Gamma(\Psi)=n$, то будем писать $\Gamma\vdash^n\Psi$ и говорить, что ***формула*** Ψ ***выводится из множества формул*** Γ ***посредством*** n ***применений правил вывода***. Этот параметр (длину) конечного вывода

будем отличать от числа ***шагов вывода***, которое равно, по определению, числу формул в выводе. Тогда запись $\Gamma \vdash^{m} \Psi$ будет означать, что вывод формулы Ψ из множества формул Γ состоит из *m* формул, последней из которых является формула Ψ. Тогда будем говорить, что ***формула*** Ψ ***выводится из множества формул*** Γ ***за*** *m* ***шагов***.

Пусть множество формул Γ есть объединение некоторого подмножества множества аксиом теории и некоторого множества формул H, не являющихся аксиомами. Тогда формулы множества H называются гипотезами, а вывод из Γ при этом называют также ***выводом из множества гипотез*** (или ***относительно множества гипотез***) H и пишут $\mathrm{H} \vdash_T \Psi$ при условии, что $\Gamma \vdash_T \Psi$. Таким образом, доказательство теории можно рассматривать как вывод из пустого множества гипотез, а в записи $\Gamma \vdash_T \Psi$ без ограничения общности можно считать, что среди формул множества Γ нет ни одной аксиомы, т.е. все формулы Γ считать гипотезами. Так в дальнейшем мы и будем поступать, не оговаривая этого особо.

Заметим, что если $\Psi \in \mathrm{H} \cup A$, то $l_{\mathrm{H}}(\Psi) = 0$ и обратно, если $l_{\mathrm{H}}(\Psi) = 0$, то формула Ψ есть либо аксиома, либо элемент множества H [2].

Отметим простой, но важный факт:

Теорема. Если $\Gamma \vdash_T \Psi$, то для любого надмножества $\Gamma' \supset \Gamma$ имеет место $\Gamma' \vdash_T \Psi$.

В частности, если формула доказуема в теории, ее можно считать выводимой из любого множества гипотез.

Рассмотрим простейший пример формальной теории.

Теория

$$Ex = (V_{Ex}, \Phi_{Ex}, P_{Ex}, A_{Ex})$$

задается: алфавитом V_{Ex}, который является объединением четырех попарно непересекающихся множеств: 1) атомов $Atom = \{0,1,...,9\}$, 2) переменных $Var = \{a,b,...,x,y,z\}$, 3) символов «операций» +, *, – и 4) специальных, или вспомогательных, символов: (,), … и т.п.; множеством формул Φ_{Ex}, которое определяется следующим образом: 1) каждый атом и каждая переменная есть формула, 2) если Ф - формула, то слово (–Ф) - формула, 3) если Ф и Ψ - формулы, то слова (Ф + Ψ) и (Ф * Ψ) – формулы, 4) ничто другое не является формулой; тремя ***схемами правил***:

(1) $\dfrac{X, Y}{(X + Y)}$, (2) $\dfrac{X, Y}{(X * Y)}$ и (3) $\dfrac{X}{(-X)}$;

множеством аксиом, которое совпадает с множеством атомов: $A_{Ex} = Atom$.

---

[2] Таким образом, если $\mathrm{H} \vdash_T \Psi$, то каждая формула соответствующего вывода есть либо аксиома, либо элемент множества H, либо получена применением некоторого правила вывода к ранее полученным формулам. Иначе говоря, при $\Gamma \vdash_T \Psi$ можно считать множество Γ определенным с точностью до любого (добавляемого) подмножества аксиом.

Конкретное правило получается из схемы правила подстановкой на место каждой буквы произвольной формулы, причем на место одной и той же буквы подставляется одна и та же формула. Такую замену будем называть согласованной. Буквы в схемах берутся из вспомогательной части алфавита и рассматриваются просто как буквы, «указатели мест».

Вот пример доказательства в построенной теории:

1. $1,2,3$ - атомы (аксиомы);
2. $(1+2)$ - применение схемы правила (1) к атомам $1,2$;
3. $((1+2)*3)$ - применение схемы правила (2) к формуле п. (2) и атому 3;
4. $-((1+2)*3)$ - применение схемы правила (3) к формуле п. (3).
5. $(-((1+2)*3))*(1+2))$ - применение схемы правила (3) к формулам пп. (4) и (2).

Длина вывода полученной формулы равна 4, а число шагов составляет 5.

Следующий же вывод нельзя считать доказательством, но его можно рассматривать как вывод его последней формулы из множества формул (переменных, гипотез) x, y, z.

1. x, y, z - исходные формулы;
2. $(x+z)$ - применение схемы правила (1) к переменным x, z;
3. $(-y)$ - применение схемы правила (3) к переменной y;
4. $((x+z)*(-y))$ - применение схемы правила (2) к формулам пп. (2) и (3).

Кроме того, нетрудно видеть, что имеет место, например, такая выводимость в теории Ex:

$$x, y, z \vdash_{Ex} -(4*(x+(y*z))),$$

где 4 - атом.

Лекция 2

Исчисление высказываний

Формальная теория, определяемая в этом разделе, известна под названием ***исчисления высказываний*** (сокращение - ***ИВ***). Формулами этого исчисления являются формулы, представляющие булевы функции[3], теоремами – так называемые ***тавтологии***; формулы, представляющие булевы функции, значение которых равно «истине» (1) при любых значениях переменных (тождественно истинные функции)[4]. Сам термин «высказывание» означает ничто иное, как «формула».

Рассматриваемый здесь вариант ИВ предполагает использование только формул над базисом $\{\neg, \rightarrow\}$, содержащим связки «отрицание» и «импликация», который, как легко проверить, является полным, т.е. формулой над ним представляется любая булева функция.

Итак, теория ИВ (исчисление высказываний) задается алфавитом, который состоит из булевых переменных, булевых констант (0 и 1), символов логических связок, скобок и т. п.; множеством формул над базисом $\{\neg, \rightarrow\}$, причем разрешается использование

[3] При изложении исчисления высказываний предполагается знакомство читателя с теорией булевых функций в объеме гл. 6 учебника «Дискретная математика» (вып. XIX в серии «Математика в техническом университете»).

[4] Важность понятия тавтологии с точки зрения логики обсуждается в Дополнении 3.

других связок как прием сокращения записи (так, мы можем написать $(X \& Y)$ как сокращение записи формулы $\neg(X \to \neg Y)$); множеством аксиом, которое задается посредством трех ***схем аксиом***:

(1) $(A \to (B \to A))$,

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

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

Конкретная аксиома получается из схемы аксиомы путем подстановки на место вхождения каждой буквы (переменной) произвольной формулы, причем все вхождения одной и той же буквы заменяются одной и той же формулой.

Правила вывода ИВ задаются единственной схемой правила, имеющей вид:

$$\frac{A, A \to B}{B}.$$

Эта схема правила, из которой конкретное правило получается так же, как конкретная аксиома получается из схемы аксиомы, носит название «***правила отсечения***» (на латыни – ***modus ponens***).

Предложенная теория – один из вариантов аксиоматизации исчисления высказываний. В литературе можно найти и другие аксиоматики. Назовем этот вариант исчисления высказываний ***теорией L***.

Обоснованием указанного выбора аксиом и правил вывода служит следующая легко доказываемая теорема:

Теорема 1. 1) Каждая аксиома теории L есть тавтология.

2) Если формулы Φ и $\Phi \to \Psi$ теории ИВ суть тавтологии, то формула Ψ также является тавтологией.

Доказательство первого пункта теоремы сводится к элементарной проверке.

Чтобы доказать второй пункт, допустим, что формула Ψ не является тавтологией при условии, что формулы Φ и $\Phi \to \Psi$ суть тавтологии. Тогда найдется набор переменных $\tilde{\alpha} = (\alpha_1, \ldots, \alpha_n)$, на котором формула Ψ (а точнее, представляемая ею булева функция) принимает значение 0. Тогда имеем: $\Phi(\tilde{\alpha}) = 1, (\Phi \to \Psi)(\tilde{\alpha}) = \Phi(\tilde{\alpha}) \to \Psi(\tilde{\alpha}) = 1$, но $\Psi(\tilde{\alpha}) = 0$, т.е. $1 \to 0 = 1$, что неверно. Стало быть, такой набор $\tilde{\alpha}$ невозможен, и формула Ψ является тавтологией.

Таким образом, в силу доказанной выше теоремы каждая аксиома теории L есть тавтология и применение правила вывода сохраняет свойство «быть тавтологией». На основании этого можно доказать, что любая теорема ИВ есть тавтология, и, тем самым ИВ есть ***непротиворечивая*** теория, т.е. в ней не доказуемы одновременно некая формула и ее отрицание. Однако, из этого еще не следует, что всякая тавтология является теоремой ИВ. Этот вопрос о ***полноте*** ИВ мы обсудим позже.

Рассмотрим пример доказательства в ИВ. Докажем очевидную тавтологию $(A \to A)$ (для произвольной формулы A).

Имеем (ниже для большей наглядности в некоторых формулах опущены внешние скобки):

1. $(A \to ((A \to A) \to A)) \to ((A \to (A \to A)) \to (A \to A))$ - схема аксиомы (2) при подстановке $(A \to A)$ вместо B и A вместо C;

2. $A \to ((A \to A) \to A)$ - схема аксиомы (1) при подстановке $(A \to A)$ вместо B;

3. $(A \to (A \to A)) \to (A \to A)$ - применение правила МР к формулам пп. (1) и (2);

4. $A \to (A \to A)$ - схема аксиомы (1) при подстановке A вместо B;

5. $(A \to A)$ - применение правила МР к формулам пп. (3) и (4).

Заметим, что длина вывода здесь равна 2, так как правило МР применяется два раза. Число шагов в выводе равно 5.

Однако часто при построении таких выводов затруднительно бывает обойтись только сведением к аксиомам. Полезно использовать некоторые технические приемы, облегчающие поиск и проведение таких выводов. Одним из важнейших инструментов здесь служит так называемая ***теорема дедукции***.

Лекция 2

Теорема дедукции

Эта теорема, принадлежащая Эрбрану, связывает выводы формул из множества гипотез с доказательствами некоторых других формул.

Будем использовать запись $\Gamma, A_1, ..., A_n \vdash \Phi$ как сокращение записи $\Gamma \cup \{A_1, ..., A_n\} \vdash \Phi$, означающей выводимость формулы Φ из множества гипотез $\Gamma \cup \{A_1, ..., A_n\}$. Такую запись принято называть ***секвенцией***.

Теорема 2 (*дедукции, Эрбрана*). Если $\Gamma, A \vdash B$, то $\Gamma \vdash (A \to B)$.

Доказательство. Индукция по длине $l_{\Gamma, A}(B)$ вывода формулы B из Γ, A.

При $l_{\Gamma, A}(B) = 0$ формула B либо совпадает с формулой A, либо принадлежит множеству Γ, либо является аксиомой. В первом случае формула $(A \to B)$ совпадает с формулой $(A \to A)$, которая есть, как доказано выше, теорема ИВ. Так как, следовательно, $\vdash (A \to A)$, то $\Gamma \vdash (A \to A)$. Во втором и в третьем случаях используем первую схему аксиом в виде $B \to (A \to B)$, и применение МР к этой схеме и формуле B дает $(A \to B)$, т.е. $\Gamma \vdash (A \to B)$.

Пусть утверждение теоремы доказано для вывода B из Γ, A любой длины, не большей $n-1$. Пусть $\Gamma, A \vdash^n B$, причем формула B получена применением правила МР к формулам Φ и $\Phi \to B$. Так как $\Gamma, A \vdash^k \Phi$ и $\Gamma, A \vdash^m \Phi \to B$, где $k, m < n$, то по предположению индукции $\Gamma \vdash (A \to \Phi)$ и $\Gamma \vdash (A \to (\Phi \to B))$. Тогда используя вторую схему аксиомы в виде $(A \to (\Phi \to B)) \to ((A \to \Phi) \to (A \to B))$ и дважды применяя МР, получим $(A \to B)$, т.е. $\Gamma \vdash (A \to B)$.

Следствие 1. Если $\Gamma \vdash (A \to B)$, то $\Gamma, A \vdash B$.

Доказательство. Действительно, пусть $\Phi_0,\ldots, \Phi_n$ – вывод формулы $(A \to B)$ из Г. Продолжим этот вывод, введя формулу A как гипотезу. Тогда, применяя MP, получим формулу B, т.е. $\Gamma, A \vdash B$.

Далее *секвенцией* будем называть любое утверждение о выводимости в исчислении высказываний. Заметим, что этот термин в математической логике имеет и другие значения.

В силу следствия 1 секвенции $\Gamma \vdash (A \to B)$ и $\Gamma, A \vdash B$ равносильны, т.е. каждая из них имеет место тогда и только тогда, когда имеет место другая.

Теорема дедукции является примером ***метатеоремы*** об ИВ, т.е. это теорема излагаемой нами математической теории, предметом которой является, на данном этапе изложения, формальная теория, именуемая исчислением высказываний. В отличие от метатеорем *теорема* ИВ есть некая формула (тавтология), для которой может быть построено доказательство (вывод) из аксиом применением правила отсечения (MP). Доказательство теоремы ИВ называется ***объектным доказательством*** (сама теорема ИВ – тавтология – может быть также названа ***объектной теоремой***), тогда как доказательство метатеоремы называют ***доказательством на метауровне*** (коротко – ***метадоказательством***).

С использованием теоремы дедукции могут быть доказаны дальнейшие полезные свойства ИВ, применение которых облегчает построение объектных доказательств.

Перечень этих свойств сведем в следующей *мета*теореме[5].

Теорема 3. 1) $A \to B, B \to C \vdash A \to C$;

2) $A \to (B \to C), B \vdash A \to C$;

3) $\vdash \neg\neg A \to A$;

4) $\vdash A \to \neg\neg A$;

5) $\vdash \neg A \to (A \to B)$;

6) $\vdash (\neg B \to \neg A) \to (A \to B)$;

7) $\vdash (A \to B) \to (\neg B \to \neg A)$;

8) $\vdash A \to (\neg B \to \neg (A \to B))$;

9) $\vdash (A \to B) \to ((\neg A \to B) \to B)$.

Доказательство. Объектные доказательства пп. (1) – (9) оформим в виде таблиц. Также используется в комментариях к шагам вывода сокращение вида: X := Ф, означающее «при замене буквы (переменной) X формулой Ф (в схеме аксиомы или теореме)».

1)

Шаг	Формула	Комментарий	Длина вывода
1	A	Гипотеза	0
2	$A \to B$	Гипотеза	0
3	$B \to C$	Гипотеза	0
4	B	MP: (1), (2)	1
5	C	MP: (3), (4)	2

[5] Ниже в записи формул опущены внешние скобки.

Итак, $A, A\to B, B\to C \vdash C$, откуда по теореме дедукции $A\to B, B\to C \vdash A\to C$.

2)

Шаг	Формула	Комментарий	Длина вывода
1	A	Гипотеза	0
2	B	Гипотеза	0
3	$A \to (B\to C)$	Гипотеза	0
4	$B\to C$	MP: (1), (3)	1
5	C	MP: (2), (4)	2

Итак, $A\to(B\to C), B, A \vdash C$, откуда по теореме дедукции $A\to (B\to C), B \vdash A\to C$.
В частности, если $\vdash B$, то $A\to (B\to C) \vdash A\to C$.

Теперь заметим, что в объектных доказательствах, рассматриваемых ниже, мы будем пользоваться уже доказанными свойствами как *новыми* правилами вывода. Номер шага и длина вывода определяются уже в соответствии с этим модифицированным понятием правила вывода. В принципе, применение нового правила может быть расписано по правилу MP. Кроме этого, формулы ИВ, являющиеся теоремами, используются в этих выводах наравне с аксиомами. В принципе вывод каждой такой формулы может быть развернут и вставлен в то объектное доказательство, которое мы строим.

3)

Шаг	Формула	Комментарий	Длина вывода
1	$(\neg A\to\neg\neg A) \to((\neg A\to\neg A) \to A)$	Схема аксиомы (3) при $B:= A$, $A:= \neg A$	0
2	$\neg A\to\neg A$	Теорема ИВ	0
3	$(\neg A\to\neg\neg A) \to A$	П. (2) настоящей теоремы при $A:= (\neg A\to\neg\neg A)$, $B:= (\neg A\to\neg A)$, $C:= A$	1
4	$\neg\neg A \to (\neg A\to\neg\neg A)$	Схема аксиомы (1) при $A:= \neg\neg A$, $B:= \neg A$	0
5	$\neg\neg A \to A$	П. (1) настоящей теоремы при $A:= \neg\neg A$, $B:= (\neg A\to\neg\neg A)$, $C:= A$	2

4)

Шаг	Формула	Комментарий	Длина вывода
1	$(\neg\neg\neg A\to\neg A) \to((\neg\neg\neg A\to A) \to\neg\neg A)$	Схема аксиомы (3) при $B:= \neg\neg A$	0
2	$\neg\neg\neg A\to\neg A$	Теорема ИВ (п. (3) настоящей теоремы)	0
3	$(\neg\neg\neg A\to A) \to\neg\neg A$	MP: (1), (2)	1
4	$A \to (\neg\neg\neg A\to A)$	Схема аксиомы (1) при $B:= \neg\neg\neg A$	0
5	$A \to\neg\neg A$	П. (1) теоремы 1 при $B:= (\neg\neg\neg A\to A)$, $C:= \neg\neg A$	2

5)

Шаг	Формула	Комментарий	Длина вывода
1	$\neg A$	Гипотеза	0
2	A	Гипотеза	0
3	$A \to (\neg B \to A)$	Схема аксиомы (1) при $B := \neg B$	0
4	$\neg A \to (\neg B \to \neg A)$	Схема аксиомы (1) при $A := \neg A$, $B := \neg B$	0
5	$\neg B \to A$	MP: (2), (3)	1
6	$\neg B \to \neg A$	MP: (1), (4)	1
7	$(\neg B \to \neg A) \to ((\neg B \to A) \to B)$	Схема аксиомы (3)	0
8	$(\neg B \to A) \to B$	MP: (6), (7)	2
9	B	MP: (5), (8)	3

Итак, $\neg A, A \vdash B$. Дважды применяя теорему дедукции, получим $\vdash \neg A \to (A \to B)$. Поскольку порядок, в котором устраняются гипотезы, неважен, то данную секвенцию можно также представить в форме $\vdash A \to (\neg A \to B)$.

6)

Шаг	Формула	Комментарий	Длина вывода
1	$\neg B \to \neg A$	Гипотеза	0
2	A	Гипотеза	0
3	$(\neg B \to \neg A) \to ((\neg B \to A) \to B)$	Схема аксиомы (3)	0
4	$A \to (\neg B \to A)$	Схема аксиомы (1) при $B := \neg B$	0
5	$(\neg B \to A) \to B$	MP: (1), (3)	1
6	$\neg B \to A$	MP: (2), (4)	1
7	B	MP: (5), (6)	2

Итак, $\neg B \to \neg A, A \vdash B$, откуда, дважды применив теорему дедукции, получим $\vdash (\neg B \to \neg A) \to (A \to B)$. Эта объектная теорема носит название ***закона контрапозиции***; ее содержательная форма такова: «если из отрицания высказывания B следует отрицание высказывания A, то из самого A следует B.

7)

Шаг	Формула	Комментарий	Длина вывода
1	$A \to B$	Гипотеза	0
2	$\neg\neg A$	Гипотеза	0
3	$\neg\neg A \to A$	Теорема ИВ (п. (3) настоящей теоремы)	0
4	$\neg\neg A \to B$	П. (1) настоящей теоремы при $A := \neg A$, $B := A$, $C := B$ (шаги (2), (4))	1
5	$B \to \neg\neg B$	Теорема ИВ (п. (3) настоящей теоремы)	0
6	$\neg\neg A \to \neg\neg B$	П. (1) настоящей теоремы для	2

		шагов (5), (6)	
7	$\neg\neg B$	MP: (3), (7)	3

Таким образом, $A\to B, \neg\neg A \vdash \neg\neg B$, откуда по теореме дедукции $\vdash (A\to B) \to(\neg\neg A \to \neg\neg B)$, а в силу п. (6) настоящей теоремы $\vdash (\neg\neg A \to \neg\neg B)\to (\neg B\to \neg A)$, откуда в силу п. (1) настоящей теоремы $\vdash (A\to B) \to(\neg B\to \neg A)$.

8)

Шаг	Формула	Комментарий	Длина вывода
1	A	Гипотеза	0
2	$A\to B$	Гипотеза	0
3	B	MP: (1), (2)	1
4	$A \to((A\to B) \to B)$	Теорема дедукции (дважды)	3
5	$((A\to B) \to B) \to (\neg B\to \neg (A\to B))$	Предыдущий пункт настоящей теоремы	0
6	$A \to(\neg B\to \neg (A\to B))$	П. (1) настоящей теоремы для шагов (4), (5)	4

9)

Шаг	Формула	Комментарий	Длина вывода
1	$A\to B$	Гипотеза	0
2	$\neg A\to B$	Гипотеза	0
3	$(A\to B) \to(\neg B\to\neg A)$	П. (7) настоящей теоремы	0
4	$\neg B\to\neg A$	MP: (1), (3)	1
5	$(\neg A\to B) \to(\neg B\to\neg\neg A)$	П. (7) настоящей теоремы	0
6	$\neg B\to\neg\neg A$	MP: (2), (5)	1
7	$(\neg B\to\neg\neg A)\to((\neg B\to\neg A) \to B))$	Схема аксиомы (3) при $A:= \neg A$	0
8	$(\neg B\to\neg A) \to B)$	MP: (6), (7)	2
9	B	MP: (4), (8)	3

Итак, $A\to B, \neg A\to B \vdash B$, откуда (после двукратного применения теоремы дедукции) $(A\to B) \to ((\neg A\to B) \to B)$.

Теорема доказана полностью.

Каждая секвенция доказанной теоремы может служить дополнительным правилом вывода. Эти правила вывода подробно описаны в Дополнении 2.

Следствие 2. Если $\Gamma, A \vdash \Phi$ и $\Gamma,\neg A \vdash \Phi$, то $\Gamma \vdash \Phi$.

Доказательство. По теореме дедукции имеем $\Gamma \vdash (A\to \Phi)$ и $\Gamma \vdash (\neg A\to \Phi)$. Применяя п. (9) теоремы 3, будем иметь $(A\to \Phi)\to ((\neg A\to \Phi)\to\Phi)$, откуда, дважды использовав MP, получим Φ, т.е. докажем секвенцию $\Gamma \vdash \Phi$.

Следствие 3. Если $\Gamma \vdash \Phi$ и $\Gamma \vdash \Psi$, то: 1) $\Gamma \vdash (\Phi \,\&\, \Psi)$ и 2) $\Gamma \vdash (\Phi \vee \Psi)$.

Доказательство. 1) Так как $(\Phi \,\&\, \Psi)$ означает $\neg (\Phi\to\neg\Psi)$, то согласно п. (8) теоремы 3 получим формулу $\Phi \to (\neg\neg\Psi\to\neg(\Phi \to\neg\Psi))$. Так как при $\Gamma \vdash \Psi$ имеет место и секвенция $\Gamma \vdash \neg\neg\Psi$ (в силу теоремы $\Psi \to \neg\neg\Psi$), то, дважды применив MP, получим $\neg(\Phi \to\neg\Psi)$, т.е. конъюнкцию $(\Phi \,\&\, \Psi)$.

2) Формула (Ф ∨ Ψ) означает ¬Ф →Ψ. Применим п. (5) теоремы 3: ¬¬Ф→(¬Ф →Ψ). Так как Г ├ Ф, то Г ├ ¬¬Ф, и, следовательно, Г ├ ¬Ф →Ψ.

Лекция 3

Свойства дизъюнкции и конъюнкции

Дополнительные логические связки дизъюнкции и конъюнкции могут быть формально введены, как способы сокращенной записи некоторых формул.
Именно, дизъюнкция вводится следующим образом:
$A \vee B = \neg A \to B$;
конъюнкция:
$A \& B = \neg(A \to \neg B)$.
Обычный знак равенства всюду здесь означает «есть то же самое, что». Легко видеть, что здесь действительно определены равные булевы функции.
Утверждение 1 (*свойства дизъюнкции*).
1) $A \vdash A \vee B$, $B \vdash A \vee B$ (из любого члена дизъюнкции выводится вся дизъюнкция);
2) $A \vee B \vdash B \vee A$(коммутативность дизъюнкции);
3) для любой формулы Ф при условии, что $A \vdash B$, выполняется $\Phi \vee A \vdash \Phi \vee B$ и $A \vee \Phi \vdash B \vee \Phi$.
Доказательство. 1) 1. A - гипотеза
2. $A \to (\neg A \to B)$ - секвенция 5
3. $\neg A \to B = A \vee B$ - MP, 1 и 2.

Итак, первая выводимость (секвенция) п. (1) есть просто форма секвенции 5 из теоремы 3 о 9 секвенциях. Вторую легко доказать аналогично с использованием схемы 1.
2) 1. $\neg A \to B = A \vee B$ - гипотеза
2. $\neg B \to \neg\neg A$- правило R7 к шагу 1 (о дополнительных правилах, соответствующих 9 секвенциям теоремы 3, см. Дополнение 2).
3. $\neg\neg A \to A$ - секвенция 3
4. $\neg B \to A = B \vee A$- R1 (секвенция 1), 2 и 3
Что и требовалось доказать.
Заметим, что логическое обоснование алгебраических свойств логических операций (связок) есть одна из задач математической логики. Простой пример такого обоснования есть только что доказанная секвенция, выражающая свойство коммутативности дизъюнкции.
3) Предлагается доказать самостоятельно.
На основании утверждения 1 можно написать следующие дополнительные правила вывода:

$$\frac{A}{A \vee B}, \frac{B}{A \vee B}, \frac{A \vee B}{B \vee A},$$

$$\frac{A \to B, \Phi \vee A}{\Phi \vee B}, \frac{A \to B, A \vee \Phi}{B \vee \Phi}$$

При построении выводов на них можно ссылаться единообразно: свойства дизъюнкции.
Утверждение 2 (*свойства конъюнкции*).
1) $A \& B \vdash A, B$ (каждый аргумент конъюнкции выводим из всей конъюнкции)
2) $A, B \vdash A \& B$(из обоих аргументов конъюнкции выводится вся конъюнкция)
3) $A \& B \vdash B \& A$(коммутативность конъюнкции)
Доказательство. 1) Докажем секвенцию $A \& B \vdash A$. В силу секвенций 6 и 7 теоремы 3 это равносильно доказательству секвенции $\neg A \vdash \neg(A \& B)$.
Имеем:

1. $\neg A$ - гипотеза
2. $\neg A \to (A \to \neg B)$ - секвенция 5 при замене $B := \neg B$
3. $A \to \neg B$ - MP, 1 и 2
4. $\neg\neg(A \to \neg B) = \neg(A \& B)$ - правило R4, шаг 3.

Доказано.

Секвенция $A \& B \vdash B$, или, что равносильно, $\neg B \vdash \neg(A \& B)$, доказывается аналогично, но вместе секвенции 5 теоремы 3 используется схема аксиомы (1).

2) 1. A, B - гипотезы

2. $\neg\neg B$ - правило R3, шаг 1
3. $\neg(A \to \neg B) = A \& B$ - правило R8 к шагам 1 (формула A) и 2 при замене $B := \neg B$.

Доказано.

3) Доказать самостоятельно.

Утверждение 2 позволяет ввести дополнительные правила вывода в согласии со свойствами конъюнкции:

$$\frac{A \& B}{A}, \frac{A \& B}{B}, \frac{A, B}{A \& B}, \frac{A \& B}{B \& A},$$

где первые два правила можно назвать условно правилами «распаковки» конъюнкции, а третье соответственно правилом «сборки» конъюнкции. При записи выводов на них можно ссылаться единообразно как на свойства конъюнкции.

Лекция 4

Полнота исчисления высказываний

Установим теперь полноту ИВ, доказав, что всякая тавтология есть теорема ИВ.

Пусть Ф есть формула, построенная из переменных $x_1,\ldots,x_n$; пусть $\tilde{\alpha} = (\alpha_1,\ldots,\alpha_n)$ - набор значений переменных. Тогда, по определению, формула $\Phi^{\tilde{\alpha}}$ есть формула Ф, если $\Phi(\tilde{\alpha}) = 1$, и формула ¬Ф, если $\Phi(\tilde{\alpha}) = 0$.

В указанных обозначениях справедлива следующая лемма.

Лемма 1. Имеет место секвенция $x_1^{\alpha_1},\ldots,x_n^{\alpha_n} \vdash \Phi^{\tilde{\alpha}}$.

Доказательство. Индукция по числу *n* связок (¬ и →) в формуле Ф.

При *n* = 0 в качестве формулы имеем какую-либо переменную *x* , и тогда, очевидно, $x \vdash x$ (так как формула ($x \to x$) есть теорема ИВ[6]).

Пусть утверждение леммы доказано для любой формулы, число связок в которой не превышает *n* – 1. Возьмем формулу Ф, содержащую *n* связок.

Возможны следующие случаи.

1° Формула Ф есть формула ¬Ψ для некоторой формулы Ψ. В силу предположения индукции $x_1^{\alpha_1},\ldots,x_n^{\alpha_n} \vdash \Psi^{\tilde{\alpha}}$. Если $\Psi^{\tilde{\alpha}}$ совпадает с Ψ, т.е. $\Psi(\tilde{\alpha}) = 1$, то Ψ $\vdash$ ¬¬Ψ (Теорема 3, п. 4), и тогда $x_1^{\alpha_1},\ldots,x_n^{\alpha_n} \vdash$ ¬¬Ψ, но формула ¬¬Ψ совпадает с формулой ¬Ф, которая и есть $\Phi^{\tilde{\alpha}}$ (так как в этом случае $\Phi(\tilde{\alpha}) = 0$). Если же $\Psi^{\tilde{\alpha}}$

[6] См. следствие 1 и пример доказательства формулы $A \to A$.

совпадает с ¬Ψ, т.е. $\Psi(\tilde{\alpha}) = 0$, то тогда $\Phi(\tilde{\alpha}) = 1$, $\Phi^{\tilde{\alpha}}$ есть Φ, и $x_1^{\alpha_1}, \ldots, x_n^{\alpha_n} \vdash \neg\Psi$, т.е. $x_1^{\alpha_1}, \ldots, x_n^{\alpha_n} \vdash \Phi$.

2° Формула Φ есть формула (Ψ→Θ) для некоторых формул Ψ и Θ. Возможны тогда следующие случаи[7]:

2.1° $\Psi^{\tilde{\alpha}} = \Psi, \Theta^{\tilde{\alpha}} = \Theta$, т.е. Ψ(α) = Θ(α) = 1, и, следовательно, Φ (α) = 1 → 1 = 1, т.е. $\Phi^{\tilde{\alpha}}$ есть Φ. По предположению индукции $x_1^{\alpha_1}, \ldots, x_n^{\alpha_n} \vdash \Psi$ и $x_1^{\alpha_1}, \ldots, x_n^{\alpha_n} \vdash \Theta$. Тогда Θ→ (Ψ→Θ), в силу схемы аксиомы (1), и, применив МР, получим (Ψ→Θ), т.е. $x_1^{\alpha_1}, \ldots, x_n^{\alpha_n} \vdash (\Psi\to\Theta) = \Phi^{\tilde{\alpha}}$.

2.2° $\Psi^{\tilde{\alpha}} = \neg\Psi, \Theta^{\tilde{\alpha}} = \Theta$, откуда по предположению индукции $x_1^{\alpha_1}, \ldots, x_n^{\alpha_n} \vdash \neg\Psi$ и $x_1^{\alpha_1}, \ldots, x_n^{\alpha_n} \vdash \Theta$. Но в этом случае Φ (α) = 0 → 1 = 1, т.е. $\Phi^{\tilde{\alpha}}$ есть Φ. Используя объектную теорему п. (5) (мета)теоремы 3, т.е. формулу ¬Ψ →(Ψ→Θ), после применения МР получим $x_1^{\alpha_1}, \ldots, x_n^{\alpha_n} \vdash (\Psi\to\Theta) = \Phi^{\tilde{\alpha}}$.

2.3° $\Psi^{\tilde{\alpha}} = \Psi, \Theta^{\tilde{\alpha}} = \neg\Theta$, и тогда Φ (α) = 1 → 0 = 0, т.е. $\Phi^{\tilde{\alpha}}$ есть ¬Φ = ¬ (Ψ→Θ). По предположению индукции $x_1^{\alpha_1}, \ldots, x_n^{\alpha_n} \vdash \Psi$ и $x_1^{\alpha_1}, \ldots, x_n^{\alpha_n} \vdash \neg\Theta$; используя п. (8) теоремы 3, формулу (Ψ→(¬ Θ → ¬ (Ψ→Θ))), и дважды применив МР, получим $x_1^{\alpha_1}, \ldots, x_n^{\alpha_n} \vdash \neg(\Psi\to\Theta) = \Phi^{\tilde{\alpha}} = \neg\Phi$.

2.4° $\Psi^{\tilde{\alpha}} = \neg\Psi, \Theta^{\tilde{\alpha}} = \neg\Theta$, и Φ (α) = 0 → 0 = 1, т.е. $\Phi^{\tilde{\alpha}} = \Phi = (\Psi\to\Theta)$.По предположению индукции $x_1^{\alpha_1}, \ldots, x_n^{\alpha_n} \vdash \neg\Psi$ и $x_1^{\alpha_1}, \ldots, x_n^{\alpha_n} \vdash \neg\Theta$; используя схему аксиомы (1) в виде ¬Ψ → (¬Θ→¬Ψ), после применения МР получим (¬Θ→¬Ψ). Затем, используя закон контрапозиции и еще раз применив МР, получим (Ψ→Θ), т.е. окончательно $x_1^{\alpha_1}, \ldots, x_n^{\alpha_n} \vdash (\Psi\to\Theta) = \Phi^{\tilde{\alpha}} = \Phi$[8].

Тем самым лемма 1 доказана полностью.

---

[7] Далее для краткости мы пишем знак равенства между формулами, читая запись Ψ=Θ как «формула Ψ есть формула Θ» (совпадает с ней).

[8] Как и в случае 2.2, можно поступить так: ¬Ψ →(Ψ→Θ), после чего получаем Ψ→Θ.

Теорема 4 (*Кальмара, о полноте ИВ*). Всякая тавтология есть теорема ИВ.

Доказательство. Если формула Ф, представляющая булеву функцию от переменных $x_1, \ldots, x_n$, является тавтологией, то для любого набора $\tilde{\alpha}$ $\Phi^{\tilde{\alpha}} = \Phi$, и $x_1^{\alpha_1}, \ldots, x_n^{\alpha_n} \vdash \Phi$. В частности, для произвольных двух наборов ($\alpha_1,\ldots, \alpha_{n-1}$, 1) и ($\alpha_1,\ldots, \alpha_{n-1}$, 0) будем иметь $x_1^{\alpha_1}, \ldots, x_{n-1}^{\alpha_{n-1}}, x_n \vdash \Phi$ и $x_1^{\alpha_1}, \ldots, x_{n-1}^{\alpha_{n-1}}, \neg x_n \vdash \Phi$. По следствию 2 отсюда получим $x_1^{\alpha_1}, \ldots, x_{n-1}^{\alpha_{n-1}} \vdash \Phi$. Так как полученная секвенция верна для любого набора ($\alpha_1,\ldots, \alpha_{n-1}$) размерности $n - 1$, то рассуждая точно так же, как и выше, элиминируем литерал $x_{n-1}^{\alpha_{n-1}}$ и т. д. до тех пор, пока не докажем, что $\vdash \Phi$, т.е., элиминировав все литералы $x_i^{\alpha_i}, i = \overline{1,n}$, получим, что формула Ф доказуема в ИВ.

Лекция 5.

Эквивалентные формулы

Будем называть формулы Ф и Ψ ***эквивалентными*** и записывать это как Ф ~ Ψ, если $\vdash (\Phi \to \Psi)$ и $\vdash (\Psi \to \Phi)$.

Лемма 2. Если Ф ~ Ψ, то $\vdash \Phi \equiv \Psi$.

Доказательство. Так как $(\Phi \equiv \Psi) = (\Phi \to \Psi)\&(\Psi \to \Phi)$, то согласно следствию 3 $\vdash \Phi \equiv \Psi$.

Пример. Рассмотрим доказательство эквивалентности некоторых формул:

1) $A \& B \equiv \neg(\neg A \vee \neg B)$.

Докажем секвенцию $A \& B \vdash \neg(\neg A \vee \neg B)$. Для этого докажем, что $(\neg A \vee \neg B) \vdash \neg(A \& B) = \neg\neg(A \to \neg B)$. В силу теоремы $\neg\neg\Phi \to \Phi$ это равносильно доказательству секвенции $(\neg A \vee \neg B) \vdash (A \to \neg B)$. Имеем: (1) $(\neg A \vee \neg B) = \neg\neg A \to \neg B$ - гипотеза, (2) $A \to \neg\neg A$ - теорема, (3) $A \to \neg B$ - п. (1) теоремы 3. Итак, $(\neg A \vee \neg B) \vdash \neg(A \& B) = \neg\neg(A \to \neg B)$, откуда, согласно закону контрапозиции, $A \& B \vdash \neg(\neg A \vee \neg B)$.

Теперь докажем секвенцию $\neg(\neg A \vee \neg B) \vdash A \& B$. Для этого, опять-таки с использованием закона контрапозиции, достаточно доказать, что $(A \to \neg B) \vdash (\neg A \vee \neg B) = \neg\neg A \to \neg B$. Имеем: (1) $(A \to \neg B)$ - гипотеза, (2) $\neg\neg A \to A$ - теорема, (3) $\neg\neg A \to \neg B$ - п. (1) теоремы 3.

2) $A \vee A \equiv A$

Имеем: (1) $A \vee A = \neg A \to A$ - гипотеза, (2) $(\neg A \to \neg\neg A) \to ((\neg A \to \neg A) \to A)$ - схема (3) при $B := A, A := \neg A$, (3) $A \to \neg\neg A$ - теорема, (4) $\neg A \to \neg\neg A$ - п. (1) теоремы 3, (5) $(\neg A \to \neg A) \to A$ - МР, (2)и (4), (6) $\neg A \to \neg A$ - теорема, (7) A - МР. Итак, $A \vee A \vdash A$. То, что $A \vdash A \vee A$, следует сразу из первой схемы аксиомы: $A \to (\neg A \to A)$.

Теорема 5 (*о замене эквивалентными формулами*). Пусть формула Ф доказуема в ИВ, т.е. ├ Ф, и пусть Ф′ - формула, полученная из Ф заменой каких-либо ее подформул эквивалентными формулами. Тогда ├ Ф′.

Доказательство. Так как для эквивалентных формул Ψ и Θ формула Ψ ≡ Θ является тавтологией (лемма 2), то для любого набора $\tilde{\alpha}$ выполняется $\Psi(\tilde{\alpha}) = \Theta(\tilde{\alpha})$. Следовательно, замена произвольной подформулы в формуле Ф эквивалентной формулой не меняет истинностного значения формулы Ф[9]. Тогда формула Ф′ является тавтологией и, по теореме 4, доказуема в ИВ.

Используя теорему 5, можно упрощать доказательства в ИВ. Например, «инверсный закон контрапозиции», т.е. формула $(A \to B) \to (\neg B \to \neg A)$, может быть получена из самого закона контрапозиции $(\neg B \to \neg A) \to (A \to B)$ подстановкой формул $\neg A$ вместо B и $\neg B$ вместо A и последующей замены подформулы $\neg\neg A$ эквивалентной формулой A, а подформулы $\neg\neg B$ эквивалентной формулой B.

Следствие 4. Если в условиях теоремы 5 для некоторого конечного множества формул Γ имеет место Γ ├ Ф, то выполняется и Γ ├ Ф′.

Доказательство. Пусть Γ = {$A_1, A_2, \ldots, A_n$}. Тогда по теореме дедукции получим ├ $A_1 \to (A_2 \to \ldots(A_n \to \Phi))\ldots)$. Тогда по теореме 5 ├ $A_1 \to (A_2 \to \ldots(A_n \to \Phi'))\ldots)$, а по следствию 1 Γ ├ Ф′.

Дополнение 1. Глубина вложенности подформулы в формулу

Определение. Пусть Φ- формулы, а Θ - какая-то ее подформула. ***Глубина вложенности*** подформулы Θ в формулу Φ, обозначаемая $d(\Theta \mid \Phi)$, определяется следующим образом:

1) если $\Theta = \Phi$, то $d(\Theta \mid \Phi) = 0$; по определению также принимается, что если формула Θ вообще не входит в Φ, то и в этом случае $d(\Theta \mid \Phi) = 0$;
2) если $\Phi = \neg\Psi$, и $d(\Theta \mid \Psi) = m$, то $d(\Theta \mid \Phi) = m + 1$,
3) если $\Phi = \Psi \to \mathrm{H}$, то $d(\Theta \mid \Phi) = \max(d(\Theta \mid \Psi), d(\Theta \mid \mathrm{H}) + 1$.

Из этого определения понятно, что число $d(\Theta \mid \Phi)$ равно максимальной длине пути в дереве, представляющем формулу Φ от корня до узла, являющегося корнем поддерева, представляющего формулу Θ (таких поддеревьев может быть несколько).

Пусть в условиях предыдущего определения запись $\Phi[\Theta'/\Theta]$ обозначает формулу, полученную из Φ заменой некоторых (всех, в частности) вхождений подформулы Θ эквивалентной ей формулой Θ'. При этом, если Θ не входит в Φ, то формула $\Phi[\Theta'/\Theta]$ считается совпадающей с формулой Φ.

Утверждение. Для произвольного набора $\tilde{\alpha}$ значений переменных $\Phi(\tilde{\alpha}) = \Phi[\Theta'/\Theta](\tilde{\alpha})$.

---

[9] Строго говоря, это надо доказывать индукцией по «глубине вложенности» подформулы в формулу (см. Дополнение 1 ниже).

Доказательство. Индукция по глубине $d(\Theta \mid \Phi)$.

Базис. $d(\Theta \mid \Phi) = 0$, т.е. либо $\Theta = \Phi$, т.е., $\Phi[\Theta'/\Theta] = \Theta'$, и значения этих формул – как эквивалентных - совпадают на любом наборе $\tilde{\alpha}$; либо $\Phi[\Theta'/\Theta] = \Phi$, и тогда доказывать нечего.

Предположение. Пусть утверждение верно при любой глубине $d(\Theta \mid \Phi) \le m-1, m \ge 1.$

Переход. Полагаем $d(\Theta \mid \Phi) = m$.

Тогда, если $\Phi = \neg\Psi$, то $d(\Theta \mid \Psi) = m-1$, и по предположению индукции для любого $\tilde{\alpha}$ имеем $\Psi(\tilde{\alpha}) = \Psi[\Theta'/\Theta](\tilde{\alpha})$. Переходя к отрицанию, получим тот же результат и для формулы Φ.

Если же $\Phi = \Psi \to \mathrm{H}$, то, поскольку $d(\Theta \mid \Psi), d(\Theta \mid \mathrm{H}) < m$, то по предположению индукции

$$\Phi[\Theta'/\Theta](\tilde{\alpha}) = \Psi[\Theta'/\Theta](\tilde{\alpha}) \to \mathrm{H}[\Theta'/\Theta](\tilde{\alpha}) =$$
$$= \Psi(\tilde{\alpha}) \to \mathrm{H}(\tilde{\alpha}) = \Phi(\tilde{\alpha}),$$

что и требовалось.

Дополнение 2. Правила вывода, соответствующие доказанным выше 9 секвенциям.

Каждая из доказанных выше 9 секвенций (теорема 3) может рассматриваться, как дополнительное правило вывода, которое можно использовать в других доказательствах и при решении задач

Правило R1: $\dfrac{A \to B, B \to C}{A \to C}$

Правило R2: $\dfrac{A \to (B \to C), B}{A \to C}$

Правило R3: $\dfrac{\neg\neg A}{A}$

Важно: правилом R3 можно пользоваться только для снятия *внешнего* двойного отрицания. Применять его для снятия двойного отрицания с некоторой подформулы нельзя.

Правило R4: $\dfrac{A}{\neg\neg A}$

Опять-таки навесить двойное отрицание согласно этому правило можно только как внешнее.

Правило R5: $\dfrac{A, \neg A}{B}$

Правило R6: $\dfrac{\neg B \to \neg A}{A \to B}$

(правило контрапозиции)

Правило R7: $\dfrac{A \to B}{\neg B \to \neg A}$

(правило обратной контрапозиции)

Правило R8: $\dfrac{A, \neg B}{\neg(A \to B)}$

Правило R9: $\dfrac{A \to B, \neg A \to B}{B}$

Проиллюстрируем применение этих правил на примере доказательств секвенций (7)-(9).
Секвенция 7
1. $A \to B$ - гипотеза
2. $\neg\neg A \to A$ - секвенция 3
3. $\neg\neg A \to B$ - правило R1 к шагам 2 и 1
4. $B \to \neg\neg B$ - секвенция 4
5. $\neg\neg A \to \neg\neg B$ - правило R1 к шагам 3 и 4
6. $\neg B \to \neg A$ - правило R6 при заменах $A := \neg B, B := \neg A$

Итак, $A \to B \vdash \neg B \to \neg A$, откуда по теореме дедукции получаем секвенцию 7.

Заметим, что нельзя было сразу в формуле $A \to B$ навесить двойные отрицания, и мы использовали сами секвенции 3 и 4 на шагах 2 и 4.

Секвенция 8
Считая доказанной формулу $A \to ((A \to B) \to B)$, имеем:
1. A - гипотеза
2. $A \to ((A \to B) \to B)$ - теорема
3. $(A \to B) \to B$ - MP, 1 и 2
4. $\neg B \to \neg(A \to B)$ - R7, 3

Тем самым из гипотезы A выведена формула $\neg B \to \neg(A \to B)$ и, согласно теореме дедукции, доказана секвенция 8.

Секвенция 9
1. $A \to B$ - гипотеза
2. $\neg A \to B$ - гипотеза
3. $\neg B \to \neg A$ - R7, 1
4. $\neg B \to \neg\neg A$ - R7, 2
5. $(\neg B \to \neg\neg A) \to ((\neg B \to \neg A) \to B)$ - схема (3) при замене $A := \neg A$
6. $(\neg B \to \neg A) \to B$ - MP, 4 и 5
7. B - MP, 3 и 6.

Итак, $A \to B$, $\neg A \to B \vdash B$, откуда, дважды применив теорему дедукции, получим секвенцию 9.
Как видно, с использованием дополнительных правил построение вывода существенно упрощается.

Дополнение 3. Важность понятия тавтологии

Формально тавтология – тождественно истинная булева функция. Но с точки зрения логики тавтология важна, по крайней мере, в двух аспектах.

1) Тавтология может определенным образом выражать последовательность рассуждений в обычной бинарной логике.

Рассмотрим с этой точки зрения формулу, получаемую из схемы аксиом (3):

$$(\neg B \to \neg A) \to ((\neg B \to A) \to B)$$

Здесь представлена схема умозаключений в доказательстве от противного: пусть надо доказать некое В. Мы предполагаем его отрицание и выводим из этого отрицание некого А. Затем, когда это уже установлено, от отрицания В мы заключаем к самому А. Это значит, что предположение отрицания В ведет к противоречию, и имеет место В.
Еще одна схема доказательства от противного представлена в секвенции (6). Это схема рассуждения по правилу контрапозиции: если надо доказать, что А влечет В, то предполагаем не-В и выводим отсюда не-А, то есть отрицание В несовместимо с А, что и означает логическое следование В из А.

Схема аксиомы (1)

$$A \to (B \to A)$$

может быть с точки зрения содержательной логики интерпретирована так: если имеет место некое А, то его можно считать логическим следствием любого В. Это то же, что множество гипотез в логическом выводе можно как угодно расширять.

2) Тавтология выражает факт логического следствия утверждения из некоторых исходных предпосылок.

Именно, по определению, утверждение (высказывание) G считается логическим следствием высказываний $F_1, F_2, ...F_n$, если импликация $F_1 \& F_2 \& ... \& F_n \to G$ является тавтологией. Действительно, импликация ложна только в одном случае: когда посылка истинна, а заключение ложно. Следовательно, если истинность всех исходных высказываний посылки влечет истинность заключения, то естественно считать заключение логическим следствием исходных высказываний, и вся импликация тогда оказывается тавтологией. Заметим, что речь идет именно о *логическом* следствии, и никакого отношения к причинно-следственным связям это не имеет.

Рассмотрим с этих позиций такую содержательную логическую задачу[10]:

Задача. Если конгресс отказывается действовать, то забастовка не будет окончена, если только она не длится более года и президент фирмы не уходит в отставку.
Закончится ли забастовка, если конгресс отказывается действовать, а забастовка только началась?

Решение

Введем логические переменные:
p – конгресс отказывается действовать,
q – забастовка заканчивается,
r – президент (фирмы) уходит в отставку,
s – забастовка длится более года.

Составим высказывания:

$F_1 = p \to (\neg q \vee (r \& s))$ (тут надо заметить, что по условию задачи затянувшаяся забастовка и уход президента фирмы в отставку имеют место одновременно; сказываются особенности перевода на русский язык в некоторой двусмысленности этой фразы);

$F_2 = p, F_3 = \neg s$

По условию задачи эти высказывания истинны. Тогда нужно проверить, будет ли формула $F_1 \& F_2 \& F_3 \to \neg q$ тавтологией.

[10] Чень Ч, Ли Р. Математическая логика и автоматическое доказательство теорем. – М.: Мир, 1983. – С. 29.

Тут возникает проблема: как доказать, что формула является тавтологией? Всегда можно составить таблицу истинности, но заметим, что задача вычисления таблицы булевой функции имеет экспоненциальную сложность: она растет как функция 2^n, где n – число переменных. Такие задачи являются, как говорят, NP-*трудными*, то есть не решаемыми за полиномиальное время (non polynomial time). С этим, кстати, связана и задача перечисления тавтологий в рамках некоторой формальной теории (исчисления высказываний) без построения таблиц истинности. Но можно предложить еще такой способ: попытаться опровергнуть формулу, найдя набор значений переменных, на котором она становится ложной. Если это приведет к противоречию, то формула является тавтологией. В развитом формализованном виде это приводит к методу резолюций, о котором речь впереди, а сейчас решим предложенную задачу сначала через попытку опровержения, а потом построим вывод теории L.

1) Попытка опровержения

Пусть $F_1 \& F_2 \& F_3 \to \neg q$ ложна. Тогда $F_1 \& F_2 \& F_3$ истинна, а $\neg q$ ложна, т.е. q = И. Так как p = И, s = Л, то для истинности F_1 необходима истинность дизъюнкции $\neg q \vee (r \& s)$, но поскольку $\neg q$ =Л, то должно быть r&s = И, что невозможно ввиду ложности s. Итак, написанная выше импликация является тавтологией.

2) **Доказательство в теории L**.

1. $(p \to (\neg q \vee (r \& s))) \& p \& \neg s$ – гипотеза,
2. a) $p \to (\neg q \vee (r \& s))$,
   b) p,
   c) $\neg s$ – свойства конъюнкции, шаг 1
3. $\neg q \vee (r \& s) = \neg\neg q \to (r \& s)$ - MP, (2a), (2c),
4. $\neg(r \& s) \to \neg\neg\neg q$ - R7 к шагу 3,
5. $\neg s \to \neg(r \& s)$ – свойства конъюнкции и правило R7
6. $\neg(r \& s)$ - MP, (2c) и (5)
7. $\neg\neg\neg q$ - MP, (4) и (6)
8. $\neg q$ - R3, (7)

Итак, $(p \to (\neg q \vee (r \& s))) \& p \& \neg s \vdash \neg q$, откуда по теореме дедукции следует, что рассматриваемая импликация является тавтологией. Забастовка не закончится. Но это *логический* вывод. Жизнь может внести свои коррективы.