Белоусов Алексей Иванович
кандидат физико-математических наук, доцент ФБГОУ МГТУ им. Н.Э. Баумана, г. Москва
al_belous@bk.ru

О некоторых методических вопросах преподавания математической логики студентам-программистам

Аннотация.

Актуальность рассматриваемой методической задачи обусловлена тем, что в учебных планах студентов-программистов существенное место занимает математическая логика, и требуется отработка методики строгого и в то же время доступного указанному контингенту изложения основ математической логики.

В статье рассматривается общее понятие формальной теории и приводится конкретный пример теории, связанный с некоторыми концепциями программирования. Рассматриваются некоторые методические вопросы изложения исчисления высказываний, в частности подробно обсуждается понятие схемы формулы, а также некоторые приемы построения формальных доказательств, приводятся примеры решения логических задач.

Ключевые слова: *математическая логика, формальная теория, исчисление высказываний, методические проблемы*

Введение

В настоящее время нет недостатка в различных учебных пособиях по математической логике. Укажем, например, на вышедшее совсем недавно: [1] и [2]. В то же время остаются актуальными некоторые методические проблемы преподавания курса математической логики для определенной аудитории, в частности, для студентов, специализирующихся в программных технологиях. Важность самой дисциплины для студентов-программистов не вызывает сомнений, так как давно известна связь между определенными программными технологиями, такими как оптимизирующие преобразования программ, автоматическое доказательство теорем, с математической логикой и теорией формальных (дедуктивных) систем. Курс должен быть построен таким образом, чтобы по возможности выявлялась связь между теорией программирования и математической логикой и был бы соблюден необходимый уровень строгости изложения.

В данной статье, которую можно рассматривать как продолжение серии методических статей автора, посвященных теории алгоритмов ([3], [4]), рассматриваются некоторые вопросы изложения основ математической логики, а именно, раздела, посвященного исчислению высказываний. Излагаемая методика основана на курсе лекций, читаемых автором в МГТУ им. Н.Э. Баумана.

Основная часть статьи делится на следующие разделы.

В первом разделе рассматривается общее понятие формальной аксиоматической теории и дается пример конкретной теории. Этот пример можно считать методической инновацией, и он как раз важен для программистской аудитории, поскольку устанавливает связь между формальным доказательством и выполнением компьютерной программы.

Второй раздел посвящен исчислению высказываний, причем сначала рассматривается важность самого понятия тавтологии, в частности, что недостаточно отражено в известных руководствах, то обстоятельство, что тавтология определенным образом выражает схему рассуждений в содержательных доказательствах, основанных на классической двузначной логике. Более подробно, чем обычно принято, рассматривается понятие схемы формулы и дается более строгое определение этого понятия.

В изложении исчисления высказываний мы следуем концепции, представленной в книге [5] (русский перевод одного из прежних изданий [6]).

Затем подробно рассматриваются некоторые инструменты поиска формального (объектного) доказательства, причем делается попытка представить ход мысли при придумывании такого доказательства, а не просто излагается доказательство в готовой форме. В этом также состоит элемент новизны рассматриваемой в статье методики.

В заключение рассматриваются два примера с четырьмя и пятью пропозициональными буквами, на которых демонстрируется преимущество установления тождественной истинности дедуктивным способом по сравнению с методом оценки формулы с помощью таблиц истинности, что, как известно, является NP-трудной задачей.

Методология и результаты исследования

Рассматриваемая в статье методика основана на известных из перечисленных источников концепциях изложения математической логики с учетом особенностей аудитории, в которой читается курс.

Далее рассматриваются основные рубрики, по которым раскладывается теоретический материал и в конце дается решение примеров.

Понятие формальной аксиоматической теории

После обсуждения предпосылок возникновения науки математической логики (это отдельная тема, которая в статье не обсуждается) необходимо дать общее понятие формальной теории.

Разумно провести параллель с теорией алгоритмов, подчеркнув, что подобно тому, как алгоритм, долгое время бывший инструментом математического исследования, с возникновением теории алгоритмов стал объектом математического исследования, так и доказательство с возникновением математической логики становится не только инструментом, но и объектом исследования. Инструментом оно остается на уровне метатеории, а объектом в тех объектных теориях, которые анализирует метатеория – математическая логика, называемая также метаматематикой. Задача состоит в том, чтобы дать математически строгое определение математического доказательства.

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

$$T = \langle V, F, A, P \rangle,$$

где V - ***алфавит теории*** (по определению не более чем *счетное* множество), F - 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:

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

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

Пусть Γ - множество формул, причем предполагается, что это множество не пересекается с множеством аксиом. Будем называть формулы этого множества ***гипотезами***.

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

$$\Phi_0, \Phi_1, ..., \Phi_n, ...$$

(конечная или бесконечная) такая, что для каждого $i \geq 0$ формула Φ_i есть либо аксиома, либо гипотеза, то есть 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 в указанном выше обозначении опускают, если это не вредит точности.

Если множество гипотез Γ пусто, 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***.

Вывод будем характеризовать двумя параметрами: 1) ***числом шагов***, под которым будем понимать число формул в выводе, и 2) ***длиной***, под которой понимается число формул в выводе, полученных в результате применения некоторого правила вывода. Таким образом, каждое применение правила вывода увеличивает длину вывода на единицу. В выводе же нулевой длины каждая формула есть либо аксиома, либо гипотеза.

Отметим простой, но важный факт:

Теорема 1. 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.

Доказательство очевидно.

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 $Atom = \{0,1,\ldots,9\}$, 2) переменных $Var = \{a,b,\ldots,x,y,z\}$, 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 Φ - формула, то слово (–Φ) - формула, 3) если Φ и Ψ - формулы, то слова $(\Phi + \Psi)$ и $(\Phi * \Psi)$ – формулы, 4) ничто другое не является формулой; тремя ***схемами правил***:

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

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

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.

Допустимо, и именно в аудитории студентов-программистов, дать такую интерпретацию определенной таким образом формальной теории, подчеркнув при этом, что это одна из возможных интерпретаций и в саму формальную теорию она не входит, а определяется чисто содержательно вне формализации.

Атомы-аксиомы будем считать обозначениями натуральных чисел от 0 до 9, переменные – числовыми переменными, каждой из которой можно присвоить значение от 0 до 9. Символы +, * и «–« будем считать обозначениями стандартных арифметических операций. Тогда теорема теории – это арифметическое выражение, значение которого может быть вычислено. Так в рассмотренном выше первом примере это будет -27. Если же формула, полученная в результате вывода, не содержит атомов, то ее значение вычислено быть не может до тех пор, пока переменные не будут инициализированы. Формула (арифметическое выражение) может быть вычислена частично. Скажем, пусть в последнем примере заданы значения переменных $y := 5, z := 7$. Тогда соответствующие гипотезы устраняются, и мы выводим частично вычисленное выражение $-(4*(x+35))$.

В свете этой интерпретации построение вывода в формальной теории можно рассматривать как выполнение программы, но выполнение недетерминированное и, в общем случае, частичное. Это согласуется с некоторыми концепциями в теоретическом программировании, такими как логическое и реляционное программирование [7], концепция смешанных (частичных) вычислений [8].

Эта программистская семантика формальной теории станет более содержательной и близкой к реальному программированию, если вместо атомов рассматривать константы с фиксированной или плавающей точкой, а вместо переменных – идентификаторы. Разумеется, тогда и уже в само чисто синтаксическое определение теории нужно ввести грамматики для этих объектов.

Можно модифицировать определение теории Ex, приняв, что аксиомами будут как атомы, так и переменные. Тогда теория превращается просто в грамматику некоторых алгебраических выражений и имеет только синтаксический аспект. Имеет смысл подчеркнуть это обстоятельство, а именно, что формальная теория может «функционировать» как грамматика, то есть множество правил построения некоторых синтаксически правильных конструкций из исходных элементарных.

Исчисление высказываний

Основная формальная теория, изучаемая в курсе математической логики – известное исчисление высказываний.

Приступая к изучению этой формальной теории, студент владеет основными результатами теории булевых функций в объеме базового учебника [9].

В частности, в той аксиоматизации, которая рассматривается в данном курсе, используются две логические связки (операции): импликации (обозначение $\to$) и отрицания (обозначение $\neg$). Множество $\{\neg, \to\}$ является, как известно, функционально полным, и две стандартные операции дизъюнкции и конъюнкции выражаются через импликацию и отрицание следующим образом:

$$A \vee B = \neg A \to B; A \& B = \neg(A \to \neg B).$$

Но перед изложением самой теории целесообразно обсудить 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:

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

Нетрудно проверить, что это тавтология (считая буквы в формуле логическими переменными).

Здесь представлена схема умозаключений в доказательстве от противного: пусть надо доказать некое B . Мы предполагаем его отрицание и выводим из этого отрицание некоего A. Затем, когда это уже установлено, от отрицания B мы заключаем к самому A . Это значит, что предположение отрицания B ведет к противоречию, и имеет место B.

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:

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.

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.

Применительно к написанной выше формуле это выглядит следующим образом.

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.

Дальше, уже в контексте формальной теории исчисления высказываний мы рассмотрим соответствующее решение этой задачи.

Рассмотрим теперь основные принципы изложения исчисления высказываний

Мы хотим построить формальную теорию, теоремами которой были бы все тавтологии и только они. Первое свойство выражает полноту теории (доказательство полноты в этой статье не рассматривается), из второго вытекает непротиворечивость теории, то есть невозможность доказать формулу вместе с ее отрицанием.

В этой статье, как и в соответствующем курсе математической логики, исчисление высказываний строится в согласии с тем подходом, который представлен в книге [11]. Этот вариант исчисления высказываний будем называть теорией L. Такая аксиоматика представляется нам более лаконичной и удобной, чем, например, представленная в классическом учебнике [12].

Дадим определение компонент этой теории:

$L = (V_L, F_L, A_L, P_L)$.

Алфавит V_L включает в себя множество логических переменных (в сущности, то же самое, что булевы переменные в теории булевых функций), обозначения двух основных логических связок – отрицания и импликации, а также множество вспомогательных символов (в том числе скобки, обозначения дополнительных связок дизъюнкции и конъюнкции и прочие служебные символы).

Множество формул F_L строится по индукции: 1) любая переменная есть формула; 2) если Φ формула, то слово $\neg\Phi$ также является формулой; 3) если Φ и Ψ суть формулы, то слово $(\Phi \to \Psi)$ есть формула; 4) других формул нет.

При этом дополнительные логические связки дизъюнкции и конъюнкции вводятся как сокращения записи некоторых формул, а именно, дизъюнкция $(\Phi \vee \Psi)$ есть сокращенная запись формулы $(\neg\Phi \to \Psi)$, а конъюнкция $(\Phi \& \Psi)$ считается сокращенной записью формулы $\neg(\Phi \to \neg\Psi)$. Это можно рассматривать и как определения дополнительных логических связок, введя в кортеж, определяющий формальную теорию компоненту определений (дефиниций). Определения ведь составляют неотъемлемую часть любой содержательной теории.

Множество аксиом A_L 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 произвольной формулы, причем все вхождения одной и той же буквы заменяются одной и той же формулой. Выше, в связи с обсуждением теории Ex, такая замена была названа согласованной. Важно подчеркнуть, что буквы в схемах являются просто буквами, своего рода указателями мест.

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. MP***). Ради краткости мы дальше говорим просто о правиле MP.

Понятие схемы заслуживает и более детального обсуждения, и речь об этом пойдет ниже.

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

Теорема 2. 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.

Заметим, что в записи формул мы зачастую опускаем внешние скобки.

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 значений переменных $\tilde{\alpha} = (\alpha_1, ..., \alpha_n)$, на котором формула Ψ (а точнее, представляемая ею булева функция) принимает значение $Л$ («ложь»). Тогда имеем: $\Phi(\tilde{\alpha}) = И, (\Phi \to \Psi)(\tilde{\alpha}) = \Phi(\tilde{\alpha}) \to \Psi(\tilde{\alpha}) = И$, но $\Psi(\tilde{\alpha}) = Л$, т.е.

$И \to Л = Л$, что неверно. Стало быть, такой набор $\tilde{\alpha}$ невозможен, и формула Ψ является тавтологией.

Обратим внимание на то, что в метаязыке мы используем обозначения логических констант: $Л$ («ложь») и $И$ («истина»), чему в теории булевых функций отвечают булевы константы 0 и 1.

Таким образом, в силу доказанной выше теоремы каждая аксиома теории L есть тавтология и применение правила вывода сохраняет свойство формул «быть тавтологией», то есть по двум посылкам-тавтологиям дает заключение, также являющееся тавтологией. На основании этого можно доказать, что любая теорема теории L есть тавтология, и, тем самым эта ***непротиворечива***, т.е. в ней не доказуемы одновременно некая формула и ее отрицание. Однако, из этого еще не следует, что всякая тавтология является теоремой данной теории. Доказательство ***полноты*** ИВ в этой статье не обсуждается.

Разумно сразу после этого рассмотреть пример доказательства очевидной тавтологии, а именно формулы $(A \to A)$ (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.

Методически целесообразно прокомментировать это известное из различных источников доказательство, попытавшись представить ход мысли того, кто его придумал.

Доказательство можно рассматривать как своего рода игру, ради достижения цели в которой нужно придумать выигрышную стратегию. Тогда сразу формула первого шага в записанном выше доказательстве представляет эту стратегию. Нам надо «добраться» до импликации $A \to A$, которая является заключением предпоследней импликации в формуле первого шага. Тогда надо как-то убрать посылку этой импликации, а также посылку внешней импликации во всей формуле, каковой оказывается формула $A \to ((A \to A) \to A)$ (внешние скобки опущены). Но можно заметить, что эта формула есть подстановка в первую схему, равно как и формула $A \to (A \to A)$.

Тогда план «игры» становится ясен, и мы пишем вывод.

Здесь же, на первом примере вывода в теории L, нужно зафиксировать внимание учащихся на том, когда может быть применено правило MP. А именно, если в выводе на каких-то двух шагах (их относительное расположение в выводе несущественно) записаны формулы Φ и $\Phi \to \Psi$, где выделена внешняя импликация в дереве импликаций, то на следующем шаге можно записать формулу Ψ - заключение внешней импликации, посылку которой, формулу Φ, записанную в выводе отдельно, мы отсекаем согласно правилу MP.

Схемы формул и формулы

Весьма важным является вопрос о схемах аксиом, вообще о схемах формул. Это не всегда и не везде достаточно подробно разъясняется.

Выше было сказано, что в схемах аксиом, как и в схемах правил, фигурируют просто буквы как указатели мест. Можно считать, что они взяты из вспомогательной части алфавита. Эти буквы могут быть заменены произвольными формулами, но согласованно, т. е. так, что разные вхождения одной и той же буквы заменяются одной и той же формулой. Но поскольку любая формула может быть или истинна, или ложна, а третьего не дано, то буквы в схемах в смысле вырабатываемого значения ведут себя так же, как и переменные: на месте каждой из них при оценке формулы, получаемой из схемы, т. е. при вычислении ее истинностного значения, будет стоять либо «истина», либо «ложь».

Более формально, эти буквы можно считать переменными в метаязыке, которые пробегают множество формул теории. Тогда указанную выше согласованную замену в схеме формулы можно уподобить выполнению оператора присваивания в компьютерной программе. Никого же не удивляет запись в программе вида $x := x + 1;$ точно также, когда в какой-нибудь схеме мы делаем (в процессе вывода) замену $A := \neg A$, это совершенно аналогично записанному выше присваиванию и состоит в присваивании нового значения переменной типа «формула». На самом деле во всех выводах, которые мы пишем, мы имеем дело не с конкретными формулами, а со схемами формул, в которых любая буква может быть согласованно заменена любой формулой. Это относится ко всем объектным теоремам. Такое объяснение связи между схемами формул и самими формулами, насколько нам известно, не принято в строгих логических текстах, но вполне уместно в программистской аудитории и естественно воспринимается, как показывает наш преподавательский опыт.

Можно было бы пойти по другому пути: считать, что мы имеем дело не со схемами аксиом, а с конкретными формулами, называемыми аксиомами. Тогда буквы в них действительно будут логическими переменными, но тогда придется наряду с правилом MP ввести правило замены, или правило подстановки, позволяющее каждую переменную согласованно заменить произвольной формулой. Это сильно удлиняло бы запись выводов и пользоваться схемами удобнее.

Вот как будет тогда выглядеть вывод самой первой тавтологии, которую мы доказали:

$\vdash A \to A$

1. $(x \to (y \to z)) \to ((x \to y) \to (x \to z))$ - аксиома (2), т. е. теперь уже не схема, а формула с переменными x, y, z;

2. $(x \to ((x \to x) \to z)) \to ((x \to (x \to x)) \to (x \to z))$ - подстановка (замена) $y := x \to x$ в формуле шага (1);

3. $(x \to ((x \to x) \to x)) \to ((x \to (x \to x)) \to (x \to x))$ - подстановка (замена) $z := x$ в формуле шага (2);

4. $x \to (y \to x)$ - аксиома (1);

5. $x \to ((x \to x) \to x)$- подстановка $y := x \to x$ в формуле шага (4);

6. $x \to (x \to x)$- подстановка $y := x$ в формуле шага (4);

7. $(x \to (x \to x)) \to (x \to x)$ - MP, (3) и (5);

8. $x \to x$ - MP, (6) и (7);

9. $A \to A$- подстановка $x := A$в формуле шага (8), где A- произвольная формула.

Это напоминает процесс выполнения некоторой программы, где производится последовательность присваиваний, но уже не переменным метаязыка, а логическим переменным. Но процесс недетерминированный. На одном шаге можно заменять несколько переменных (шаги 2 и 3 выше можно объединить).

В итоге же, значением «метапеременной» будет либо истина, либо ложь, так что, отождествляя буквы в схемах с логическими переменными, мы, конечно, допускаем вольность речи, но она простительна.

Замечание. Точнее, значением буквы как переменной типа «формула» будет некоторая формула, а значением этой последней будет либо «истина», либо «ложь». Имеет место двухступенчатый процесс оценки формулы: сначала из схемы получаем формулу, а потом вычисляем значение этой формулы.

Дополнительные правила вывода

Часто при построении 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***.

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

Будем использовать запись $\Gamma, A_1, \ldots, A_n \vdash \Phi$ как сокращение записи $\Gamma \cup \{A_1, \ldots, A_n\} \vdash \Phi$, означающей выводимость формулы Φ из множества гипотез $\Gamma \cup \{A_1, \ldots, A_n\}$. Такую запись принято называть ***секвенцией***. То есть в контексте этого изложения под секвенцией будем понимать любое утверждение о выводимости в теории L.

Теорема 3 (*теорема дедукции*). Если $\Gamma, A \vdash B$, то $\Gamma \vdash (A \to B)$.

Доказательство опускается. См., например, в [Мендельсон].

Легко доказать также обратную теорему.

Теорема 4. Если $\Gamma \vdash (A \to B)$, то $\Gamma, A \vdash B$.

В силу этих двух теорем можно считать, что записанные в условии секвенции равносильны. Основываясь на них, можно как устранять гипотезы, так и вводить их.

Важно в этом месте объяснить учащимся, как следует вводить новые гипотезы.

Вводя дополнительные гипотезы, следует твердо помнить, что *гипотезу можно вводить только как* ***посылку внешней импликации*** *в той формуле, которая выводится*.

Именно, пусть надо доказать секвенцию $\Gamma \vdash \Phi$ для некоторого (возможно пустого) множества гипотез Γ и некоторой формулы Φ. Если формула Φ представима в виде $\Theta \to \Psi$, то формулу Θ можно ввести как дополнительную гипотезу и свести исходную задачу к доказательству секвенции $\Gamma, \Theta \vdash \Psi$. Далее, если формула Ψ допускает представление в виде $\Psi_1 \to \Psi_2$, то посылку этой импликации можно взять за новую гипотезу и доказать уже такую секвенцию: $\Gamma, \Theta, \Psi_1 \vdash \Psi_2$ и т.д. Вводить новые гипотезы не обязательно, но этот прием часто помогает облегчить решение задачи.

Эта идея иллюстрируется на примере доказательства следующей объектной теоремы:

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

Это так называемый закон контрапозиции, выражающий известную схему рассуждения при доказательстве от противного.

Введем посылку внешней импликации записанной выше формулы (точнее, схемы формулы, но мы дальше будем отождествлять эти два понятия) как гипотезу:

1. $\neg B \to \neg A$ - гипотеза (договоримся всюду, как правило, опускать внешние скобки);

2. A - гипотеза (эту дополнительную гипотезу мы имеем право ввести, так как она является посылкой единственной импликации в формуле $(A \to B)$, которую нужно вывести из первой гипотезы.

Далее рассуждаем так: из записанных выше двух гипотез надо вывести B. Вспоминаем, что единственная из трех схем аксиом, в конце которой, как заключение последней импликации, стоит буква, - схема (3). Поэтому продолжаем вывод, записывая эту схему в исходной форме:

3. $(\neg B \to \neg A) \to ((\neg B \to A) \to B)$ - схема аксиомы (3);

Теперь видим, что к шагам (1) и (3) можно применить правило MP:

4. $(\neg B \to A) \to B$ - MP к шагам (1) и (3);

Отсечь посылку внешней импликации в формуле 4-го шага можно через вторую гипотезу и схему (1), а именно:

5. $A \to (\neg B \to A)$- схема аксиомы (1) при замене $B := \neg B$;

6. $\neg B \to A$ - MP к шагам (2) и (5);

7. B - MP к шагам (4) и (6).

Итак, доказана секвенция $\neg B \to \neg A,\ A \vdash B$.

Устраняя по теореме дедукции вторую (дополнительную) гипотезу, получим $\neg B \to \neg A \vdash A \to B$. Применяя теорему дедукции второй раз и устраняя первую (основную) гипотезу, придем к доказываемой объектной теореме.

Следует подчеркнуть, что теорема дедукции и основанный на ней (как и на обратной теореме) метод построения доказательств, является эффективным инструментом, позволяющим относительно просто находить объектные доказательства, частично «алгоритмизировать» игровой процесс.

Можно было и не вводить вторую гипотезу, но тогда пришлось бы сначала доказать секвенцию

$$A \to B, B \to C \vdash A \to C,$$

выражающую естественное свойство транзитивности импликации. Считая это доказанным (подробно см. ниже), можно переписать доказательство закона контрапозиции следующим образом:

1. $\neg B \to \neg A$ - гипотеза;
2. $(\neg B \to \neg A) \to ((\neg B \to A) \to B)$ - схема аксиомы (3);
3. $(\neg B \to A) \to B$ - МР к шагам (1) и (2);
4. $A \to (\neg B \to A)$ - схема аксиомы (1) при замене $B := \neg B$;
5. $A \to B$ - по свойству транзитивности импликации.

Вывод получился короче, но в нем де факто использовано дополнительное к МР правило вывода, обоснование которого, как будет доказано позже, также основано на применении теоремы дедукции.

Ключевым результатом всего курса является следующая теорема:

Теорема 5. В теории L имеют место следующие секвенции:

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

Доказательства некоторых из этих секвенций будут даны ниже, но важно то, что каждая из них дает в дополнение к МР новое правило вывода. Эти новые 9 правил дают в руки дополнительные эффективные средства поиска и записи объектных доказательств. Выпишем эти правила:

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

В курсе лекций подробно доказываются все секвенции. Здесь рассмотрим только некоторые.

1) 1. $A \to B$ - гипотеза;

2. $B \to C$ - гипотеза;

3. A - гипотеза;

4. B - МР к шагам (1) и (3);

5. C - МР к шагам (2) и (4).

Итак, $A \to B$, $B \to C$, $A \vdash C$, откуда, применяя теорему дедукции, получаем секвенцию (1).

Секвенция (2) доказывается аналогично.

На примере доказательства секвенций (3) и (4) полезно обсудить сам принцип поиска доказательства. Рассмотрим тут в таком плане доказательство третьей секвенции.

Надо доказать $\vdash \neg\neg A \to A$

Посылку можно принять за гипотезу. Тогда из нее надо вывести *A*. Вспоминаем, в какой схеме аксиомы в конце стоит одна буква (или буква с отрицаниями). Это схема (3):

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

(внешние скобки по умолчанию опущены).

Значит, если мы хотим эту схему использовать, то букву *B* следует заменить на *A*.

Тогда должно быть так:

$(\neg A \to \neg X) \to ((\neg A \to X) \to A)$.

Но что поставить вместо *X*?

Мы можем ввести гипотезу $\neg\neg A$. Если мы вместо *X* подставим $\neg A$, то получится:

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

Сразу становится понятным план дальнейших действий: чтобы добраться до последнего *A*, нужно убрать предшествующие посылки. Первая посылка отсекается с помощью схемы (1), где на первом месте стоит двойное отрицание *A*, наша гипотеза. Вторая посылка есть уже доказанная теорема (каждая формула влечет саму себя), и задача решена.

В итоге пишем такой вывод:

1. $\neg\neg A$ - гипотеза,

2. $(\neg A \to \neg\neg A) \to ((\neg A \to \neg A) \to A)$ - схема (3) при заменах $A := \neg A, B := A$,

3. $\neg\neg A \to (\neg A \to \neg\neg A)$ - схема (1) при $A := \neg\neg A, B := \neg A$,

4. $\neg A \to \neg\neg A$ - МР, (1) и (3)

5. $(\neg A \to \neg A) \to A$ - МР, (2) и (4),

6. $\neg A \to \neg A$ - теорема,

7. *A* – МР, (5) и (6)

Что и требовалось. Остается применить теорему дедукции.

В таком же духе можно разобрать доказательство секвенции (4).

Секвенция (6) была доказана выше. Приведем доказательства 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. $(A \to B) \to B$ - МР, 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.

Инструментарий поиска объектных доказательств может быть пополнен правилами, основанными на свойствах дополнительных связок дизъюнкции и конъюнкции. Эти свойства сведем в теорему:

Теорема 6. 1) Свойства дизъюнкции:

1.1) $A \vdash A \vee B$, $B \vdash A \vee B$ (из любого члена дизъюнкции выводится вся дизъюнкция);

1.2) $A \vee B \vdash B \vee A$(коммутативность дизъюнкции).

2) Свойства конъюнкции:

2.1) $A \& B \vdash A, B$ (каждый аргумент конъюнкции выводим из всей конъюнкции)

2.2) $A, B \vdash A \& B$(из обоих аргументов конъюнкции выводится вся конъюнкция)

2.3) $A \& B \vdash B \& A$(коммутативность конъюнкции).

Доказательство рассмотрим только для пунктов (2.1) и (2.2).

2.1) Доказательство выводимости $A \& B \vdash A$, согласно секвенциям (6) и (7) равносильно доказательству выводимости $\neg A \vdash \neg(A \& B)$.

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 вместо секвенции 5 используется схема аксиомы (1).

2.2) 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 $B := \neg B$.

Тогда можно добавить правила вывода, основанные на этих свойствах:

$\frac{A}{A \vee B}, \frac{B}{A \vee B}, \frac{A \vee B}{B \vee A}$ (свойства дизъюнкции);

$\frac{A \& B}{A}, \frac{A \& B}{B}, \frac{A, B}{A \& B}, \frac{A \& B}{B \& A}$, (свойства конъюнкции).

Примеры решения задач

В завершение рассмотрим решение двух конкретных задач.

1) Докажем в теории L тавтологию в рассмотренной выше на содержательном уровне задаче о забастовке:

$\vdash ((p \to (\neg q \vee (r \& s))) \& (p \& \neg s) \to \neg q$.

Имеем (по соглашению, внешние скобки опускаются):

1. $((p \to (\neg q \vee (r \& s))) \& (p \& \neg s)$ - гипотеза;

2. $p \to (\neg q \vee (r \& s))$ - по свойствам конъюнкции, шаг (1);

3. $p \& \neg s$ - по свойствам конъюнкции, шаг (1);

4. p - по свойствам конъюнкции, шаг (2);

5. $\neg s$ - по свойствам конъюнкции, шаг (2);

6. $\neg q \vee (r \,\&\, s) = \neg\neg q \to (r \,\&\, s)$ - МР к шагам (2) и (4) и определение дизъюнкции;

7. $\neg(r \,\&\, s) \to \neg\neg\neg q$ - правило (R7) к шагу (6);

8. $\neg s \to \neg(r \,\&\, s)$ - теорема, вытекающая из свойств конъюнкции;

9. $\neg(r \,\&\, s)$ - МР к шагам (5) и (8);

10. $\neg\neg\neg q$ - МР к шагам (7) и (9);

11. $\neg q$ - правило (R3) к шагу (10).

Итак, $((p \to (\neg q \vee (r \,\&\, s))) \,\&\, (p \,\&\, \neg s) \vdash \neg q$, откуда по теореме дедукции получаем требуемое.

Ключевой момент в этом решении – переход от 6-го к 7-му шагу. На 6-м шаге мы получили импликацию, посылкой которой служит $\neg\neg q$. Поскольку нам надо вывести $\neg q$, разумно прибегнуть к обратной контрапозиции и поставить цель достижения $\neg\neg\neg q$, к чему и направлены шаги (8)-(10).

Рассмотрим теперь доказательство тавтологии с пятью пропозициональными буквами:

$\vdash [((A \to B) \to (\neg C \to \neg D)) \to E] \to [(E \to A) \to (\neg D \to A)]$

Эта задача поучительна, так как доказательство выйдет значительно короче и легче в смысле трудозатрат, чем построение таблицы истинности из 32 строк (5 переменных).

Предварительно докажем, что:

$\neg(A \to B) \vdash A \& \neg B$ (правило отрицания импликации).

Так как в левой части стоит внешнее отрицание и ее неудобно использовать в качестве гипотезы, то прибегаем к контрапозиции, то есть выводим отрицание левой части из отрицания правой.

1. $\neg(A \& \neg B) = \neg\neg(A \to \neg\neg B)$ - гипотеза;

2. $A \to \neg\neg B$ - R3, шаг (1);

3. $\neg\neg B \to B$ - секвенция (3) (здесь нужно применить именно секвенцию (3), а не правило R3, так как снимать двойное отрицание внутри формулы запрещено;

4. $A \to B$ - R1, (2) и (3);

5. $\neg\neg(A \to B)$ - R4, шаг (4), что и требовалось.

Переходим к решению основной задачи.

1. $((A \to B) \to (\neg C \to \neg D)) \to E$ - гипотеза;

2. $E \to A$ - гипотеза;

3. $\neg D$ - гипотеза;

4. $((A \to B) \to (\neg C \to \neg D)) \to A$ - R1, (1) и (2);

5. $\neg A \to \neg((A \to B) \to (\neg C \to \neg D))$ - R7, шаг (4);

6. $\neg((A \to B) \to (\neg C \to \neg D)) \to \neg(A \to B) \& \neg(\neg C \to \neg D)$ - теорема (правило отрицания импликации);

7. $\neg A \to \neg(A \to B) \& \neg(\neg C \to \neg D)$ - R1, (5) и (6);

8. $\neg(A \to B) \& \neg(\neg C \to \neg D) \to \neg(\neg C \to \neg D)$ - свойства конъюнкции, шаг (7);

9. $\neg A \to \neg(\neg C \to \neg D)$ - R1, (7) и (8);

10. $(\neg C \to \neg D) \to A$ - R6, шаг (9);

11. $\neg D \to (\neg C \to \neg D)$ - схема (1) при заменах $A := \neg D, B := \neg C$;

12. $\neg D \to A$ - R1, (11) и (10);

13. A - MP, (3) и (12).

Итак, $((A \to B) \to (\neg C \to \neg D)) \to E$, $E \to A$, $\neg D \vdash A$.

Применив три раза теорему дедукции, получим доказываемую объектную теорему.

Заключение

Представлена целостная методика изложения одного из разделов математической логики студентам-программистам.

Элементы новизны методики состоят в следующем.

При изложении общего понятия формальной аксиоматической теории предлагается простой, но важный конкретный пример теории, который может интерпретирован в программистском ключе и в то же время показывает связь между понятиями теории и грамматики.

Подробно объясняется понятие схемы формулы в свете чего процесс формального доказательства можно рассматривать как недетерминированное выполнение программы, в процессе которого меняются значения переменных метаязыка.

На некоторых примерах показывается ход мысли по придумыванию доказательства в рамках понимания доказательства как игры.

Заключительные примеры с четырьмя и пятью пропозициональными буквами, демонстрирующие преимущества дедуктивного подхода к установлению тождественной истинности формулы (объектной теоремы).

В плане развития изложенных здесь методических идей следует рассмотреть проблемы, связанные с понятием эквивалентных формул и методику изложения метода резолюций как для исчисления высказываний, так и для исчисления предикатов 1-го порядка.

Ссылки на источники

1. Леденева Т.М., Аристова Е.М. Формальные аксиоматические теории. Исчисление высказываний. – Ч.1.- Воронеж, Воронежский государственный университет. – 2016.- 27 с.
2. Леденева Т.М. Формальные аксиоматические теории. Исчисление высказываний. – Ч.2.- Воронеж, Воронежский государственный университет. – 2020.- 42 с.
3. Белоусов А.И. О методике изложения некоторых разделов теории алгоритмов: проблема применимости для нормальных алгорифмов Маркова // Modern European Researches. – 2019. - №5. – С. 17-36.
4. Белоусов А.И. О методике изложения некоторых разделов теории алгоритмов: некоторые приемы разработки схем нормальных алгорифмов Маркова// Modern European Researches. – 2020. - №2 (Т.1). – С. 38-49.
5. Mendelson E. Introduction to Mathematical Logic. – 6 ed. – N.Y., CRC Perss.- 2015. – 499 pp.
6. Мендельсон Э. Введение в математическую логику. - М.: Наука, 1971. – 320 с.
7. Волосова А.В., Матюхина Е.Н. Логическое программирование. – М.: Изд-во «Спутник+», 2019. – 56 с.
8. Касьянов В.Н. Смешанные вычисления и оптимизация программ //Кибернетика. – 1980. - №2. – С. 51-54.
9. Белоусов А.И., Ткачев С.Б. Дискретная математика// Учеб. для вузов. – 6-е изд. – М.: Изд. МГТУ им. Н.Э. Баумана, 2020. – 703 с.
10. Чень Ч, Ли Р. Математическая логика и автоматическое доказательство теорем. – М.: Мир, 1983. – 360 с.
11. Мендельсон Э. Указ. соч.
12. Колмогоров А.Н., Драгалин А.Г. Математическая логика.- М.: КомКнига, 2006.- 240 с.

Alexey I. Belousov,

Candidate of Physical-Mathematical Sciences, Associate Professor,
Bauman Moscow State Technical University, Moscow
al_belous@bk.ru

On some methodological issues of teaching mathematical logic to students-programmers

Abstract.

The relevance of the methodological problem under consideration is due to the fact that mathematical logic occupies an essential place in the curricula of students-programmers, and it is required to develop a methodology of a rigorous and at the same time accessible to the specified contingent of exposition of the foundations of mathematical logic.

The article discusses the general concept of formal theory and provides a specific example of the theory associated with some programming concepts. Some methodological questions of the presentation of the propositional calculus are considered, in particular, the concept of a formula scheme is discussed in detail, as well as some methods of constructing formal proofs, examples of solving logical problems are given.

Keywords: *mathematical logic, formal theory, propositional calculus, methodological problems*.