

РОССИЙСКАЯ АКАДЕМИЯ НАУК
ОРДЕНА ЛЕНИНА ИНСТИТУТ ПРИКЛАДНОЙ МАТЕМАТИКИ
ИМЕНИ М.В. КЕЛДЫША

С.В.Попов

ОБ УСТРАНИМОСТИ АКСИОМЫ ИНДУКЦИИ

Москва, 2005г.

УДК 517.5

Попов С.В. Об устранимости аксиомы индукции. Препринт Института прикладной математики им. М.В. Келдыша РАН. Москва, 2005г.

Устанавливается, что в арифметических доказательствах формул, которые не содержат индивидуальных переменных, устранима аксиома индукции.

Popov S.V. About eliminating of induction axiom. Preprint of the Keldysh Institute of Applied Mathematics of RAS. Moscow, 2005.

It is established, that in arithmetic proofs of formulas which do not contain individual variables, the axiom of an induction is eliminated.

Введение. Рассматривается формальная арифметика S , содержащая константу 0 , числовые переменные, равенство, функциональные символы $+$ (сложения), $\cdot$ (умножения) и $'$ (прибавления 1) и логические связки. Термы строятся из константы 0 и переменных с помощью функциональных символов. В частности, натуральные числа изображаются термами вида $0'' \dots'$. Атомарные формулы – это равенства термов; остальные формулы строятся с помощью логических связок и кванторов.

Исчисление базируется на классическом исчислении предикатов и включает следующие дополнительные аксиомы: $x' = y' \supset x = y$; $\neg(x' = 0)$; $x = y \supset .x = z \supset y = z$; $x = y \supset x' = y'$; $x + 0 = x$; $x + y' = (x = y)'$; $x \cdot 0 = 0$; $x \cdot y = (x \cdot y) + x$ и схему индукции (АИ): $A(0) \supset .\forall x(A(x) \supset A(x')) \supset \forall x A(x)$. Логическое исчисление первого порядка выглядит не совсем обычно, что объясняется требованием выделить характерные свойства выводов, которые позволяют сформулировать основной результат работы, состоящий в том, что при доказательстве фундаментальных формул (т.е. формул без переменных) можно обойтись без АИ.

Формулы первого порядка строятся над базисом $\supset, f, \forall$. Для наглядности, формулы вида $X_1 \supset .X_2 \supset . \dots \supset .X_n \supset X$, $n \geq 0$ представляются в виде $\Gamma \rightarrow X$, используя знак $\rightarrow$ в качестве многоместной импликации. При этом порядок посылок $\Gamma = \{X_1, X_2, \dots, X_n\}$ несущественен.

Единственная аксиомная схема логического исчисления имеет вид: $X \supset X$. При этом формула X называется *заключением* аксиомы. Правила исчисления следующие:

обобщенное правило *modus ponens*

$$\frac{\Gamma_1 \rightarrow .X \supset Y \quad \Gamma_2 \rightarrow X}{\Gamma \rightarrow Y} \quad (\text{здесь } \Gamma = \Gamma_1 \cup \Gamma_2)$$

снятие двойного отрицания

$$\frac{\Gamma \rightarrow .(X \supset f) \supset f}{\Gamma \rightarrow X}$$

положительное кванторное правило

$$\frac{\Gamma \rightarrow X(a)}{\Gamma \rightarrow \forall x X(x)} \quad (\text{переменная } a \text{ не входит в } \Gamma)$$

отрицательное кванторное правило

$$\frac{\Gamma \rightarrow .(\Delta \rightarrow \forall y X(y)) \supset .(\Delta \rightarrow X(t)) \supset Y}{\Gamma \rightarrow .(\Delta \rightarrow \forall y X(y)) \supset Y} \quad (t - \text{произвольный терм})$$

Достаточно просто показать, что это исчисление совпадает с классическим.

1. Определение синтаксического дерева. Определим более компактную форму вывода в приведенном исчислении (т.н. *синтаксическое дерево*), что позволит установить ряд свойств выводов, которые трудно заметить при обычном определении.

Синтаксическим деревом (с.д.) D_U для формулы U называется одно-корневое, растущее вверх дерево, которое построено следующим образом:

1. Корню с.д. D_U приписана формула U , висячим узлам - аксиомы, остальным узлам формулы, вид которых определяется типом узлов, которым они приписаны. В аксиоме $X \supset X$ обе формулы X называются *двойственными*.

2. Каждый не висячий узел D_U является либо В-узлом, либо З-узлом, либо положительным кванторным узлом, либо отрицательным кванторным узлом.

В-узлом называется следующая конструкция.

Самому В-узлу приписана формула $\Gamma \rightarrow (X_1 \supset X_2 \supset \dots \supset X_n \supset X) \supset X$, а непосредственно выше расположены в точности n узлов, каждому из которых приписана единственная формула, полученная из $\Gamma \rightarrow (X_1 \supset X_2 \supset \dots \supset X_n \supset X) \supset X_i$, $i = 1, 2, \dots, n$ отбрасыванием некоторых посылок. При этом для данного В-узла формула X называется *изменяемой*, а $X_1 \supset X_2 \supset \dots \supset X_n \supset X$ - *используемой*. Два вхождения формулы X – заключение используемой формулы и изменяемая формула, называются *двойственными*.

З-узлом называется следующая конструкция.

Самому З-узлу приписана формула $\Gamma \rightarrow X$, а непосредственно выше расположен в точности один узел, которому приписана формула, полученная выбрасыванием некоторых посылок из $\Gamma \rightarrow (X \supset f) \supset f$. При этом формула X называется *запоминаемой*.

Положительным кванторным узлом (обозначается $\forall^+$) называется следующая конструкция.

Самому $\forall^+$ -узлу приписана формула $\Gamma \rightarrow \forall x X(x)$, а непосредственно выше расположен единственный узел, которому приписана формула, полученная из $\Gamma \rightarrow X(a)$ выбрасыванием некоторого числа ее посылок. При этом переменная a (*собственная переменная* этого узла) не входит в Γ .

Отрицательным кванторным узлом (обозначается $\forall^-$) называется следующая конструкция.

Самому $\forall$ -узлу приписана формула $\Gamma \rightarrow .(\Delta \rightarrow \forall y X(y)) \supset Y$, а непосредственно выше расположен единственный узел, которому приписана формула, полученная из формулы

$$\Gamma \rightarrow .(\Delta \rightarrow \forall y X(y)) \supset .(\Delta \rightarrow X(t)) \supset Y$$

выбрасыванием некоторого числа посылок. При этом терм t называется *собственным* для этого узла.

Будем представлять синтаксические деревья в виде, который обычно принят при изображении выводов в виде деревьев. Так, если формулы $A_1, A_2, \dots, A_n$ располагаются непосредственно выше формулы B , то будем представлять это так:

$$\frac{A_1, A_2, \dots, A_n}{B}$$

Справедлива

Теорема 1.1. *Формула U общезначима тогда и только тогда, когда для нее существует с.д. D_U .*

Доказательство следует из сопоставления узлов с.д. и приведенных правил вывода.

2. Свойства синтаксических деревьев. Сформулируем несколько свойств с.д., которые будут использоваться в последующем. Эти свойства представлены в виде последовательности утверждений, каждое последующее добавляет некоторое новое свойство к уже установленным.

Лемма 2.1. *Всякое с.д. может быть преобразовано в такое, в котором формулы запоминаемые, изменяемые и заключительные в аксиомах суть атомарные.*

Доказательство. Пусть D_U есть с.д., в котором В-узлу N приписана формула

$$V = \Gamma \rightarrow .(X_1 \supset .X_2 \supset . \dots \supset .X_n \supset X) \supset X,$$

$X = A_1 \supset .A_2 \supset . \dots .A_m \supset B$ есть изменяемая формула и главная связка формулы B не импликация. Заменяем этот узел следующим. Ему приписана та же формула, используемая формула остается прежней, а изменяемой формулой является B . В результате, непосредственно выше к присутствующим узлам добавляются m новых, которым приписаны аксиомы $A_i \supset A_i$, $i = 1, 2, \dots, m$. Последние возникают из того, что как в самой формуле V имеются посылки A_i , так и в изменяемой формуле присутствуют те же посылки. Следовательно, после замены исходного В-узла на новый, получим с.д. формулы U .

Пусть теперь в с.д. D_U В-узлу N приписана формула

$$V = \Gamma \rightarrow .(X_1 \supset .X_2 \supset . \dots \supset .X_n \supset \forall x X(x)) \supset \forall x X(x),$$

и a — это индивидуальная переменная, которая не встречается в этом с.д. Заменяем В-узел N следующими тремя узлами. Сам узел N превращается в $\forall^+$ -узел с собственной переменной a . Непосредственно выше располагается $\forall^-$ -узел с собственным термом a . Наконец, третьим узлом является В-узел с изменяемой формулой $X(a)$ и используемой $X_1 \supset .X_2 \supset . \dots \supset .X_n \supset X(a)$. Очевидно, что такое преобразование превращает исходное с.д. в новое с.д. для формулы U .

Легко увидеть, что, используя подобные преобразования, каждое с.д. можно привести к такому с.д., в котором изменяемые формулы В-узлов суть атомарные.

Доказательство леммы для двойственных формул аксиом и запоминаемых формул осуществляется по аналогичной схеме.

Лемма доказана.

Лемма 2.2. *Всякое с.д. может быть преобразовано к следующему виду: если некоторая посылка какой-либо формулы выступает в качестве используемого выражения в В-узле, то нигде выше эта формула не используемая в другом В-узле.*

Доказательство. Пусть некоторому В-узлу N с.д. D_U приписана формула

$$V = \Gamma \rightarrow .(X_1 \supset .X_2 \supset . \dots \supset .X_n \supset X) \supset X,$$

и его используемая формула $X_1 \supset .X_2 \supset . \dots \supset .X_n \supset X$ также используется выше в В-узле N_1 , которому приписана формула

$$V_1 = \Gamma_1 \rightarrow .(X_1 \supset .X_2 \supset . \dots \supset .X_n \supset X) \supset X.$$

В силу леммы 2.1 полагаем, что X есть атомарная формула. Непосредственно выше N расположены n узлов $N^1, N^2, \dots, N^n$, которым приписаны формулы соответственно $\Delta_1 \rightarrow X_1, \Delta_2 \rightarrow X_2, \dots, \Delta_n \rightarrow X_n$. Пусть узел N_1 расположен выше узла $N^i, i \in \{1, 2, \dots, n\}$ и непосредственно выше узла N_1 расположены n узлов $N_1^1, N_1^2, \dots, N_1^n$ с приписанными формулами соответственно $\Theta_1 \rightarrow X_1, \Theta_2 \rightarrow X_2, \dots, \Theta_n \rightarrow X_n$.

Превратим узел N^i в 3-узел с запоминаемой формулой X_i . В результате появится новая посылка $X_i \supset f$. Теперь нетрудно увидеть, что можно построить с.д., в котором эта посылка будет встречаться везде выше узла N^i вплоть до узла N_1 , который мы заменяем следующим образом. Если X есть константа f , то N_1 становится В-узлом с используемой формулой $X_i \supset f$. Если X есть атомарная формула, отличная от константы, то этот узел превращается в 3-узел N_1' , выше которого расположен В-узел N_1'' с приписанной формулой

$$\Gamma_1 \rightarrow .(X_1 \supset .X_2 \supset . \dots \supset .X_n \supset X) \supset .X_i \supset f \supset .X \supset f \supset f.$$

и используемой формулой $X_i \supset f$. В результате получается импликация с заключением X_i , посылки которой включают все посылки формулы V_1 .

Из этих преобразований очевидно, как построить с.д. выше этой формулы, основываясь на исходном с.д.

Лемма доказана.

Лемма 2.3. *Всякое с.д. может быть преобразовано к следующему виду: если в последнем $\forall^-$ -узел с собственным термом t расположен ниже $\forall^+$ -узла с собственной переменной a , то терм t не содержит переменной a .*

Доказательство. Пусть в с.д. D_U $\forall^-$ -узел N с собственным термом $t(a)$ расположен ниже $\forall^+$ -узла N_1 с собственной переменной a . По определению $\forall^+$ -узла формула, приписанная узлу N_1 не содержит переменной a . Поэтому заменим в поддереве с корнем N_1 все вхождения переменной a на новую переменную b , не встречающуюся в исходном с.д. В результате получим новое с.д. для формулы U . Прделав подобные преобразования со всем с.д. получим искомое с.д.

Лемма доказана.

Следствие 1. *Если формула U не содержит свободных переменных, и в с.д. D_U $\forall^-$ -узел с собственным термом t расположен ниже любого $\forall^+$ -узла, то терм t фундаментальный (т.е. не содержит переменных).*

Следствие 2. *Если формула U не содержит положительных кванторов, то в с.д. D_U все собственные термы $\forall^-$ -узлов фундаментальные.*

На множестве термов с.д. введем частичный порядок: будем говорить, что некоторый терм *зависит* от собственной переменной положительного кванторного узла, если он ее содержит. Если терм есть собственный терм

отрицательного кванторного узла, то будем говорить о зависимости между кванторными узлами: назовем $\forall^-$ -узел *зависимым* от $\forall^+$ -узла с собственной переменной a , если собственный терм $\forall^-$ -узла содержит a .

Всякий терм с.д. (в том числе и собственный отрицательного кванторного узла) может зависеть от нескольких переменных. Покажем, что при этом можно ограничиться рассмотрением только таких с.д., для которых выполняются определенные условия.

Лемма 2.4. *Всякое с.д. может быть преобразовано к следующему виду: все собственные переменные положительных кванторных правил попарно различны, и собственная переменная любого $\forall^+$ -узла встречается лишь в поддереве с корнем в этом $\forall^+$ -узле.*

Доказательство следует из того, что если N есть $\forall^+$ -узел с собственной переменной a , то a не входит в формулу, приписанную этому узлу. Поэтому, заменив везде в поддереве с корнем N переменную a на новую переменную, которая не встречается в исходном с.д., получим также с.д. для исходной формулы.

Лемма доказана.

Следствие. *Всякое с.д. может быть преобразовано к следующему виду: каждый отрицательный кванторный узел располагается выше того положительного, от которого он зависит.*

Доказательство. Все $\forall^+$ -узлы с.д. имеют различные собственные переменные, которые встречаются только выше этих узлов. Поэтому, если собственная переменная a $\forall^+$ -узла N входит в собственный терм $t(a)$ $\forall^-$ -узла N_1 , то N располагается ниже N_1 .

Следствие доказано.

Замечание. Обратное, в общем случае, неверно. Собственный терм отрицательного кванторного узла может не зависеть от положительного кванторного узла, выше которого он располагается.

Из последних рассуждений вытекает, что для замкнутой формулы U в с.д. D_U собственные термы отрицательных кванторных узлов суть суперпозиции функциональных символов и собственных переменных положительных кванторных узлов. При этом суперпозиция определяется видом двойственных выражений, т.к. в этом случае требуется полное совпадение двух формул, что предполагает совпадение соответствующих термов. Из определения с.д. видно, что глубина суперпозиции, главным образом, определяется числом В-узлов, которые встречаются в одной ветви с.д.

Нас интересует возможность вхождения в один собственный терм отрицательного кванторного узла собственных переменных положительных кванторных узлов.

Введем следующие определения.

Пусть N_1 и N_2 – два положительных кванторных узла, элиминирующие кванторы, соответственно, $\forall x$ и $\forall y$. Тогда эти узлы *зависимы*, если один из этих кванторов в выводимой формуле управляет другим. В противном случае узлы *независимые*.

Пусть в с.д. D_U каждый положительный кванторный узел имеет свою уникальную собственную переменную, и N_1 и N_2 – два независимых положительных кванторных узла, устраняющие кванторы соответственно $\forall x$ и $\forall y$, причем узел N_2 расположен выше N_1 , и собственными переменными узлов N_1 и N_2 являются соответственно a и b . При устранении квантора $\forall x$ узлом N_1 могут появиться термы лишь вида $t_1(a)$, а узлом N_2 – вида $t_2(b)$. Но не могут появиться термы, зависящие сразу от двух переменных a и b , так как кванторы $\forall x$ и $\forall y$ не зависимы. И поэтому после появления собствен-

ной переменной a , порожденной узлом N_1 , она никак не может встречаться в подформуле, начинающейся с квантора $\forall u$. Покажем, что в этом случае можно ограничиться рассмотрением лишь с.д., в которых отсутствуют термы вида $t(a, b)$.

Справедлива

Теорема 2.5. *Всякое с.д. можно преобразовать так, что собственные термы любого отрицательного кванторного узла не зависят ни от каких двух независимых положительных кванторных узлов.*

Доказательство. Пусть в с.д. N есть отрицательный кванторный узел с собственным термом $t(a, b)$, где a и b суть собственные переменные независимых положительных кванторных узлов. Если терм $t(a, b)$ не встречается в двойственных формулах, то собственный терм узла N можно заменить на терм $t(a, a)$, не содержащий переменную b . Легко увидеть, что при такой замене мы вновь получим с.д.

В противном случае в с.д. встречаются двойственные пары, включающие терм $t(a, b)$. Если оба соответствующие терма каждой такой двойственной пары суть собственные термы узла N , то их также можно заменить на терм $t(a, a)$, не содержащий переменную b . Легко увидеть, что при такой замене вновь получим с.д.

Если в с.д. встречается двойственная пара $X(t(a, b)), X(t(a, b))$ и в одной из этих формул (пусть первой) терм $t(a, b)$ является собственным для узла N , а во второй – нет, то рассмотрим предшественников этого терма во второй формуле. По условию a и b суть собственные переменные независимых положительных кванторных узлов. Поэтому рассматриваемый терм $t(a, b)$ в с.д. мог возникнуть лишь как собственный терм некоторого отрицательного кванторного узла. Но тогда, выделив все такие отрицательные

кванторные узлы, в которых $t(a,b)$ есть собственный терм, можно везде в них заменить $t(a,b)$ на $t(a,a)$, не содержащий переменную b . Легко увидеть, что при такой замене вновь получим с.д.

Разобраны все случаи. Теорема доказана.

Следствие. *Собственный терм отрицательного кванторного узла может зависеть от двух различных собственных переменных положительных кванторных узлов лишь, когда один из этих кванторов управляет другим.*

Лемма 2.6. *Всякое с.д. может быть преобразовано к следующему виду: если его некоторому узлу приписана формула $\Gamma \rightarrow \forall x X(x)$, то это $\forall^+$ -узел.*

Доказательство. Пусть узлу N с.д. приписана формула $\Gamma \rightarrow \forall x X(x)$, и этот узел не является $\forall^+$ -узлом. По лемме 2.1 этот узел может быть лишь $\forall^-$ -узлом с собственным термом t . Этот терм не содержит собственной переменной a того $\forall^+$ -узла, в котором снимается квантор $\forall x$. Следовательно, если переставить эти узлы, то также получится с.д. Прделав подобные преобразования со всем с.д. получим искомое с.д.

Лемма доказана.

Следствие. *Если в с.д. имеется $\forall^+$ -узел, котором приписана формула $\Gamma \rightarrow \forall x X(x)$, то выводима любая формула $\Gamma \rightarrow X(t)$, где t - произвольный терм. При этом с.д. для формулы $\Gamma \rightarrow X(t)$ получается из поддерева с корнем в узле, расположенном непосредственно выше $\forall^+$ -узла, простой заменой собственной переменной указанного $\forall^+$ -узла на терм t .*

Таким образом, с.д. для формулы $\Gamma \rightarrow X(t)$ не содержит новых дополнительных термов, по сравнению с с.д. для формулы $\Gamma \rightarrow \forall x X(x)$, за исключением t .

Следствие (аналог теоремы о средней формуле). Пусть U есть формула, в которой каждая посылка и заключение находятся в предваренной форме. Тогда существует с.д. D_U , в котором присутствует формула, ниже которой расположены лишь кванторные узлы, а выше лишь B -узлы и 3 -узлы. (Эта формула называется средней для с.д. D_U).

3. Преобразования синтаксических деревьев. В этом разделе опишем схемы преобразований синтаксических деревьев, которые позволяют получить новые с.д. Это позволит в дальнейшем получать с.д. с определенными свойствами.

Лемма 3.1. Пусть

$$U_1 = \Gamma_1 \rightarrow X \supset Y, U_2 = \Gamma_2 \rightarrow X, U = \Gamma \rightarrow Y, \text{ где } \Gamma = \Gamma_1 \cup \Gamma_2$$

и D_{U_1}, D_{U_2} суть с.д. Тогда существует с.д. D_U , полученное перестройкой двух предыдущих конечным числом локальных преобразований. (Обозначим перестройку указанных с.д. в искомое с.д. через $\Gamma_1 \rightarrow X \supset Y + \Gamma_2 \rightarrow X$.)

Доказательство состоит в том, что приводится система схем преобразований с.д., которая позволяет с.д. D_{U_1}, D_{U_2} преобразовать в искомое. Полнота системы вытекает из того, что осуществляется разбор всех случаев, которые могут встречаться в результате подобной перестройки. Смысл преобразований легко понять из их вида. Эти преобразования аналогичны преобразованиям секвенциальных выводов при устранении правила сечения.

$$1. X \supset X \quad + \quad \Delta \rightarrow X \quad \sim \quad \Delta \rightarrow X$$

2.

$$\frac{\Delta_{11} \rightarrow .X \supset Y_1 \dots \Delta_{1h} \rightarrow .X \supset Y_h}{\Delta_1 \rightarrow .X \supset Y} \quad + \quad \Delta_2 \rightarrow X \quad \sim$$

$$\frac{\Delta_{11} \rightarrow .X \supset Y_1 \quad + \quad \Delta_2 \rightarrow X \quad \dots \quad \Delta_{1h} \rightarrow .X \supset Y_h \quad + \quad \Delta_2 \rightarrow X}{\Delta \rightarrow Y}$$

где $\Delta = \Delta_{11} \cup \dots \cup \Delta_{1h} \cup \Delta_2$.

3.

$$\frac{\Delta_1 \rightarrow .(Y_1 \supset \dots \supset .Y_h \supset X) \supset Y_1 \dots \Delta_1 \rightarrow .(Y_1 \supset \dots \supset .Y_h \supset X) \supset Y_h}{\Delta_1 \rightarrow .(Y_1 \supset \dots \supset .Y_h \supset X) \supset X} \quad + \quad \Delta_2 \rightarrow .Y_1 \supset \dots \supset .Y_h \supset X \quad \sim$$

$$\frac{\Delta_2 \rightarrow .Y_1 \supset \dots \supset .Y_h \supset X + \{\Delta_1 \rightarrow .(Y_1 \supset \dots \supset .Y_h \supset X) \supset Y_1 \dots \Delta_1 \rightarrow .(Y_1 \supset \dots \supset .Y_h \supset X) \supset Y_h\}}{\Delta \rightarrow X}$$

где $\Delta = \Delta_1 \cup \Delta_2$.

4.

$$\frac{\Delta_1 \rightarrow .(\Theta \rightarrow \forall x X(x)) \supset .(\Theta \rightarrow X(t)) \supset Y}{\Delta_1 \rightarrow .(\Theta \rightarrow \forall x X(x)) \supset Y} \quad + \quad \Delta_2 \rightarrow .\Theta \rightarrow \forall x X(x) \quad \sim$$

$$\frac{\Delta_1 \rightarrow .(\Theta \rightarrow \forall x X(x)) \supset .(\Theta \rightarrow X(t)) \supset Y + \{\Delta_2 \rightarrow .\Theta \rightarrow \forall x X(x), \Delta_2 \rightarrow .\Theta \rightarrow X(t)\}}{\Delta \rightarrow Y}$$

где $\Delta = \Delta_1 \cup \Delta_2$. Здесь с.д. для формулы $\Delta_2 \rightarrow .\Theta \rightarrow X(t)$ получается из с.д. для формулы $\Delta_2 \rightarrow .\Theta \rightarrow \forall x X(x)$, т.к. самым нижним узлом последнего является положительный кванторный, которому предшествует с.д. для формулы $\Delta_2 \rightarrow .\Theta \rightarrow X(c)$. Такое с.д. легко перестроить в искомое, устранив нижний положительный кванторный узел и заменив его собственную переменную c на терм t .

Разобраны все случаи. Лемма доказана.

4. Некоторые свойства арифметических термов. Числом n называется терм $0''''''$, содержащий n штрихов. Говорим, что фундаментальный терм равен числу, если они равны в стандартной арифметической модели.

В последующих рассуждениях мы обозначим E совокупность четырех формул: правило *подстановки*: $x = y \supset t(x) = t(y)$, аксиомы *рефлексивности*: $x = x$, *коммутативности*: $x = y \supset y = x$ и *транзитивности*: $x = y \supset .y = z \supset x = z$.

Глубина арифметического терма t , обозначается $d(t)$, вычисляется следующим образом.

1. Если t есть переменная или константа 0 , то $d(t) = 0$.
2. Если $t = (t_1)'$, то $d(t) = d(t_1) + 1$.
3. Если $t = t_1 + t_2$ или $t = t_1 t_2$ то $d(t) = \max\{d(t_1), d(t_2)\} + 1$.

Лемма 4.1. Если терм t равен числу n , то равенство $t = n$ выводимо из E без АИ.

Доказательство индукцией по глубине терма t .

Базис индукции. Терм t есть константа 0 . Тогда равенство $0 = 0$ элементарно следует из аксиомы рефлексивности.

Индукционный переход. Разберем все возможные случаи для внешнего функционального символа терма t .

Если это символ $'$, то случай легко сводится к индукционной гипотезе, используя аксиому $x = y \supset x' = y'$.

Допустим, что t имеет вид $t_1 + t_2$, и по индукционной гипотезе равенства $t_1 = n_1$ и $t_2 = n_2$ доказуемы без использования АИ.

В силу рефлексивности имеем $t = t_1 + t_2$. Далее, используя два раза правило подстановки с посылками $t_1 = n_1$ и $t_2 = n_2$, получаем $t = n_1 + n_2$. Затем, используя n_2 раз аксиому $x + y' = (x + y)'$, и единственный раз аксиому $x + 0 = x$, получаем равенство $t = n$.

Случай, когда t имеет вид $t_1 \cdot t_2$, разбирается аналогично с использованием аксиом $x \cdot y' = (x \cdot y) + y$ и $x \cdot 0 = 0$.

Разобраны все случаи. Лемма доказана.

Лемма 4.2. Если A есть арифметическая формула, терм t равен числу n , то импликации $A(t) \supset A(n)$ и $A(n) \supset A(t)$ выводимы в исчислении первого порядка из E и равенства $t = n$.

Доказательство. Структуры формул $A(t)$ и $A(n)$ подобны. Поэтому для каждой из приведенных импликаций можно построить конструкцию наподобие с.д., висячими узлами которой служат либо аксиомы вида $X \supset X$, либо выражения вида:

- а) $t = x \supset n = x$;
- б) $x = t \supset x = n$,
- в) $n = x \supset t = x$;
- г) $x = n \supset x = t$.

В каждом из этих выражений в точности одно вхождение переменной x есть собственная переменная некоторого положительного кванторного

правила, а другое – отрицательного. Любое из них выводимо в исчислении первого порядка из посылок E и $t = n$.

Лемма доказана.

Следствие 1. Если A есть арифметическая формула, терм t равен n , то для формул $E \rightarrow .t = n \supset .A(t) \supset A(n)$ и $E \rightarrow .t = n \supset .A(n) \supset A(t)$ существуют с.д., множества термов которых содержат помимо индивидных переменных лишь термы собственно формулы A и пару термов t и n .

Таким образом, перечисленные две формулы принадлежат исчислению первого порядка.

Следствие 2. Если A есть арифметическая формула, терм t равен n , и имеется с.д. для формулы $A(n)$ ($A(t)$), то для формулы $E \rightarrow .t = n \supset A(t)$ ($E \rightarrow .t = n \supset A(n)$) существует с.д., множество термов которого содержит помимо индивидных переменных лишь термы с.д. для формулы $A(n)$ ($A(t)$), термы формулы A и пару термов t и n .

5. Некоторые свойства арифметических выводов. Пусть фундаментальная формула R выводима в арифметике. Тогда имеется с.д. D_U для формулы U , которая имеет вид $\mathfrak{R} \rightarrow R$, где $\mathfrak{R}$ есть совокупность арифметических аксиом. В силу конечности с.д. D_U уместно допустить, что оно содержит конечное число различных термов. Определим на множестве термов этого с.д. частичный порядок, как это определено в разд.2. Этот порядок индуцирует следующий частичный порядок на множестве АИ, используемых в с.д.

Пусть посылка вида $A(0) \supset .\forall x(A(x) \supset A(x')) \supset A(t)$ есть пример АИ, полученный в результате отрицательного кванторного узла, причем терм t содержит переменную s , которая является собственной для расположенного ниже положительного кванторного узла вида

$$\frac{\Gamma \rightarrow B(c) \supset B(c')}{\Gamma \rightarrow \forall x(B(x) \supset B(x'))}$$

и заключение $\forall x(B(x) \supset B(x'))$ появилось в результате использования ниже в В-узле примера АИ $B(0) \supset .\forall x(B(x) \supset B(x')) \supset B(t_1)$. (Это пояснено на рис.5.1.) Согласно ранее введенного частичного порядка терм t зависит от переменной c . Будем говорить, что в этом случае пример $B(0) \supset .\forall x(B(x) \supset B(x')) \supset B(t_1)$ *предшествует* примеру $A(0) \supset .\forall x(A(x) \supset A(x')) \supset A(t)$.

В силу Теоремы 2.6 *всякий пример АИ может предшествовать нескольким примерам АИ, но одному примеру АИ предшествует не более одного примера АИ.*

$$\frac{\Delta \rightarrow .A(0) \supset .\forall x(A(x) \supset A(x')) \supset .A(t) \supset X}{\Delta \rightarrow .\forall y(A(0) \supset .\forall x(A(x) \supset A(x')) \supset A(y)) \supset X}$$

$$\frac{\frac{\Gamma \rightarrow .B(c) \supset B(c')}{\Gamma \rightarrow \forall x(B(x) \supset B(x'))}}{\Gamma \rightarrow .(B(0) \supset .\forall x(B(x) \supset B(x')) \supset B(t_1)) \supset B(t_1)}$$

Рис. 5.1

Изобразим отношение предшествования, определенное на множестве примеров АИ в любом с.д. в виде растущего вверх *дерева зависимостей*. Для простоты полагаем, что оно однокорневое и связное, его корень не помечен никак, а каждый оставшийся узел помечен единственным примером АИ. Очевидно, что каждый узел, расположенный непосредственно

над корнем, помечен тем примером АИ, который не зависит ни от какого другого примера АИ.

Из преобразований разд.3 вытекает

Теорема 5.1. *Всякое преобразование, описанное в разд.3, не приводит к появлению новых зависимостей между примерами АИ. Т.е. глубина дерева зависимостей результирующего с.д. не превосходит глубины дерева зависимостей исходного с.д.*

Доказательство осуществляется простой проверкой каждого из преобразований.

6. Устранение АИ из выводов фундаментальных формул. В этом разделе мы покажем, что вывод всякой фундаментальной арифметической формулы может быть получен без использования АИ, но с использованием правила подстановки.

Справедлива

Теорема 6.1. *Пусть фундаментальная формула R выводима в системе S . Тогда существует ее вывод в S , в котором используется правило подстановки, но отсутствуют АИ.*

Доказательство. Так как R выводима в арифметике, то в исчислении первого порядка выводима формула U вида $\mathfrak{R} \rightarrow R$, где $\mathfrak{R}$ есть некоторая совокупность аксиом арифметики. Полагаем, что $\mathfrak{R}$ также содержит законы рефлексивности, коммутативности и транзитивности для равенства. Тем самым для этой формулы существует с.д. D_U . В силу конечности с.д. D_U уместно допустить, что оно содержит конечное число различных термов.

Полагаем, что отношение предшествования, определенное на множестве примеров АИ в с.д. D_U представимо в виде растущего вверх дерева

зависимостей. Дальнейшее доказательство состоит в том, что мы покажем, как перестроить исходный вывод, чтобы результирующий не включал АИ. Перестройка на каждом шаге приводит к уменьшению длины ветвей дерева зависимостей с одновременным увеличением его ширины. Поэтому доказательство проводим индукцией по числу различных примеров АИ, присутствующих в дереве зависимостей.

Базис индукции, когда в с.д. D_U нет примеров АИ, элементарен.

Индукционный шаг. Выделим в с.д. D_U самый нижний В-узел N , в котором используемым выражением служит пример АИ. В этом случае фрагмент с.д. D_U с узлом N в качестве корня имеет такой вид, как на рис.6.1.

$$\begin{array}{c}
 \dots \\
 \Gamma \rightarrow .(A(0) \supset .\forall x(A(x) \supset A(x')) \supset A(t)) \supset \Delta(t) \\
 \Gamma \rightarrow .(A(0) \supset .\forall x(A(x) \supset A(x')) \supset A(t)) \supset \forall x(A(x) \supset A(x')) \\
 \Gamma \rightarrow .(A(0) \supset .\forall x(A(x) \supset A(x')) \supset A(t)) \supset A(0) \\
 \hline
 \Gamma \rightarrow .(A(0) \supset .\forall x(A(x) \supset A(x')) \supset A(t)) \supset A^*(t)
 \end{array}$$

Рис. 6.1.

Здесь для простоты предполагается, что $A(t) = \Delta(t) \supset A^*(t)$, где $A^*(t)$ – это атомарная фундаментальная формула, т.к. ниже рассматриваемого В-узла нет положительных кванторных узлов.

Обратим внимание на следующее.

1. Поддеревья

$$\begin{array}{l}
 D_\Gamma \rightarrow .(A(0) \supset .\forall x(A(x) \supset A(x')) \supset A(t)) \supset A(0), \\
 D_\Gamma \rightarrow .(A(0) \supset .\forall x(A(x) \supset A(x')) \supset A(t)) \supset \forall x(A(x) \supset A(x')) , \\
 D_\Gamma \rightarrow .(A(0) \supset .\forall x(A(x) \supset A(x')) \supset A(t)) \supset \Delta(t)
 \end{array}$$

не содержат формулу $(A(0) \supset .\forall x(A(x) \supset A(x')) \supset A(t))$ в качестве используемой в каком-либо своем В-узле. Следовательно, эти поддеревья, простым вычеркиванием посылки $(A(0) \supset .\forall x(A(x) \supset A(x')) \supset A(t))$ во всех формулах превращаются в с.д. соответственно

$$D_{\Gamma \rightarrow A(0)},$$

$$D_{\Gamma \rightarrow \forall x(A(x) \supset A(x'))},$$

$$D_{\Gamma \rightarrow A(t)}$$

Дальнейшее доказательство состоит в том, что мы некоторым образом преобразовываем эти поддеревья. В итоге с.д.

$$D_{\Gamma \rightarrow (A(0) \supset .\forall x(A(x) \supset A(x')) \supset A(t)) \supset A^*(t)}$$

будет преобразовано в с.д. $D_{\Gamma \rightarrow A^*(t)}$.

2. Так как R - фундаментальная формула, то между корнем исходного с.д. и узлом N нет положительных кванторных узлов. Следовательно, t есть фундаментальный терм, так как получается в результате суперпозиции собственных термов отрицательных кванторных узлов, ни одно из которых не зависит от положительного узла.

3. Из фундаментальности терма t вытекает, что он равен некоторому числу n , и равенство $n = t$ доказуемо без АИ.

4. Из существования с.д. для формулы

$$\Gamma \rightarrow \forall x(A(x) \supset A(x'))$$

вытекает, что это с.д. начинается с положительного кванторного узла, пусть с собственной переменной c :

$$\frac{\Gamma \rightarrow A(c) \supset A(c')}{\Gamma \rightarrow \forall x(A(x) \supset A(x'))}$$

Рассматриваемый пример $A(0) \supset .\forall x(A(x) \supset A(x')) \supset A(t)$ АИ является тем, который приписан узлу дерева зависимостей, расположенному непосредственно над корнем. Следовательно, в с.д. D_U имеются $h \geq 0$ различных примеров АИ, которые зависят от выделенного. Каждый из них в собственном терме, полученном снятием отрицательного квантора, во-первых, содержит переменную c и, во-вторых, не содержит никакой другой собственной переменной, полученной в результате снятия положительного квантора, порожденного другим примером АИ.

5. Из выводимости формулы

$$\Gamma \rightarrow .A(c) \supset A(c')$$

следует выводимость любой формулы

$$\Gamma \rightarrow .A(i) \supset A(i'),$$

где i - произвольное число. И с.д. для каждой такой формулы получается простой перестройкой с.д. для формулы

$$\Gamma \rightarrow .A(c) \supset A(c').$$

После замены собственной переменной c на число i получаем с.д. для формулы

$$\Gamma \rightarrow .A(i) \supset A(i'),$$

которое не содержит пример $A(0) \supset .\forall x(A(x) \supset A(x')) \supset A(t)$ АИ. Поэтому дерево зависимостей для с.д.

$$D_{\Gamma \rightarrow .A(i) \supset A(i')}$$

имеет во всех своих ветвях на один ярус меньше, чем соответствующее поддереву дерева зависимостей для с.д.

$$D_{\Gamma \rightarrow (A(0) \supset .\forall x(A(x) \supset A(x')) \supset A(t)) \supset .A(c) \supset A(c')}.$$

При этом в с.д.

$$D_{\Gamma \rightarrow .A(i) \supset A(i')}$$

множество термов по сравнению с множеством термов в с.д.

$$D \Gamma \rightarrow .(A(0) \supset .\forall x(A(x) \supset A(x')) \supset A(t)) \supset .A(c) \supset A(c')$$

отличается в точности тем, что во всех термах переменная c заменена числом i , $i = 0, 1, \dots, n$.

6. Из этого вытекает существование первопорядкового вывода формулы

$$\Gamma \rightarrow A(n)$$

из формул

$$\Gamma \rightarrow A(0)$$

$$\Gamma \rightarrow .A(0) \supset A(1),$$

...

$$\Gamma \rightarrow .A(n-1) \supset A(n).$$

Этот вывод имеет вид, как на рис.6.2.

$$\begin{array}{c} \frac{\Gamma \rightarrow .A(0) \supset A(1) \quad \Gamma \rightarrow A(0)}{\Gamma \rightarrow .A(1) \supset A(2)} \quad \Gamma \rightarrow A(1) \\ \vdots \\ \frac{\Gamma \rightarrow .A(n-1) \supset A(n) \quad \Gamma \rightarrow A(n-1)}{\Gamma \rightarrow A(n)} \end{array}$$

Рис. 6.2.

С.д. для каждой из формул

$$\Gamma \rightarrow .A(0) \supset A(1)$$

$$\Gamma \rightarrow .A(1) \supset A(2)$$

. . .

$$\Gamma \rightarrow .A(n-1) \supset A(n)$$

определяет дерево зависимостей, которое совпадает с деревом зависимостей, определенного с.д. для формулы

$$\Gamma \rightarrow .A(c) \supset A(c').$$

Дерево зависимостей, определяемое с.д. для формулы

$$\Gamma \rightarrow A(0),$$

такое же, как для соответствующего поддеревья исходного с.д.

Поэтому дерево зависимостей, которое определяется выводом на рис.6.1 для формулы

$$\Gamma \rightarrow A(n)$$

шире, чем исходное, но оно имеет более короткие ветви в тех поддеревьях, которые имеют своими самым нижними узлами, узлы, помеченные выделенным примером АИ.

7. Формула

$$E \rightarrow .t = n \supset .A(n) \supset A(t)$$

выводима в исчислении первого порядка, причем множество термов ее вывода, помимо переменных, которые служат собственными термами кванторных правил, и термов собственно формулы A , включает лишь два: t и n . Теперь, используя полученный вывод формулы

$$\Gamma \rightarrow A(n),$$

получаем вывод формулы

$$\Gamma \rightarrow .E \rightarrow .t = n \supset A(t),$$

который содержит множество термов, состоящее из множества термов вывода формулы

$$\Gamma \rightarrow A(n).$$

Для этого вывода дерево зависимостей совпадает с деревом зависимостей поддерева из п.6, т.к. вывод формулы

$$E \rightarrow .t = n \supset .A(n) \supset A(t)$$

не содержит АИ.

8. Для дальнейшего доказательства полагаем, что $\Delta(t)$ есть формула. Тогда по Следствиям из леммы 4.2 следует, выводимость формулы $E \rightarrow .t = n \supset .\Delta(t) \supset \Delta(n)$. Напомним, что $A(t) = \Delta(t) \supset A^*(t)$, поэтому $A(n) = \Delta(n) \supset A^*(n)$ и $\Gamma \rightarrow A(n) = \Gamma \rightarrow .\Delta(n) \supset A^*(n)$.

9. Теперь вывод формулы $\Gamma \rightarrow . E \rightarrow .t = n \supset A^*(t)$ выглядит, как на рис. 6.3.

$$\frac{\frac{\frac{E \rightarrow .t = n \supset .\Delta(t) \supset \Delta(n)}{\Gamma \rightarrow .\Delta(n) \supset A^*(n)} \quad \Gamma \rightarrow .E \rightarrow .t = n \supset \Delta(n)}{E \rightarrow .t = n \supset .A^*(n) \supset A^*(t)} \quad \Gamma \rightarrow .E \rightarrow .t = n \supset A^*(n)}{\Gamma \rightarrow . E \rightarrow t = n \supset A^*(t)}$$

Рис. 6.3.

Результирующий вывод определяет дерево зависимостей, которое выглядит как на рис.6.4.

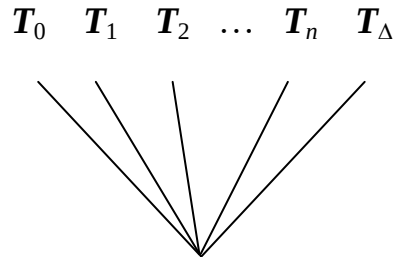


Рис.6.4

Здесь T_0 – это дерево зависимостей, определяемое с.д. формулы

$$\Gamma \rightarrow A(0),$$

T_i - это дерево зависимостей, определяемое результирующим выводом формулы

$$\Gamma \rightarrow A(i),$$

$i = 1, 2, \dots, n$, T_Δ - это дерево зависимостей, определяемое с.д. для формулы

$$\Gamma \rightarrow \Delta(t).$$

Как видно, каждая из посылок результирующего вывода имеет в заключении фундаментальную формулу, а дерево зависимостей содержит на один пример АИ меньше, чем дерево зависимостей исходного с.д. Следовательно, для результирующего вывода выполняется индукционная гипотеза.

Так как множество Γ посылок включает аксиомы для равенства, то получаем, что если расширить множество посылок исходной формулы посылкой $t = n$, то получим с.д. для формулы $\Gamma \rightarrow .t = n \supset A^*(t)$, которое не содержит выделенного примера АИ. Кроме того, исходный вывод перестраивается таким образом, что к нему применима индукционная гипотеза.

Тем самым, мы показали, что для формулы, получаемой из $\mathfrak{R} \rightarrow R$ за счет исключения всех АИ и добавления конечного множества $t_1 = n_1, t_2 = n_2, \dots, t_q = n_q$ посылок, где $t_1, t_2, \dots, t_q$ суть фундаментальные термы исходного вывода, и $n_1, n_2, \dots, n_q$ - равные им числа, существует первопорядковый вывод. Но тогда формула R выводима без АИ лишь с правилом подстановки.

Теорема доказана.

Следствие. Система S непротиворечива.

Доказательство. Допустим противное. Тогда в S имеется вывод формулы R вида $0 = 1$. Элиминируем АИ из доказательства формулы $\mathfrak{R} \rightarrow R$. В итоге получится первопорядковый вывод формулы $t_1 = n_1, t_2 = n_2, \dots, t_q = n_q, \mathfrak{R}^* \rightarrow R$, где $\mathfrak{R}^*$ отличается от $\mathfrak{R}$ лишь отсутствием АИ. Из существования для этой формулы с.д. со средней секвенцией следует, что имеется пропозициональный вывод формулы $t_1 = n_1, t_2 = n_2, \dots, t_q = n_q, \mathfrak{R}^{**} \rightarrow R$, где $\mathfrak{R}^{**}$ есть совокупность фундаментальных примеров аксиом системы S за исключением АИ.

Но каждый из примеров этих аксиом, так же, как и равенства $t_1 = n_1, t_2 = n_2, \dots, t_q = n_q$ истины в стандартной интерпретации, а $0 = 1$ - ложна. Противоречие.

Следствие доказано.