PUBLICATIONS DE L'INSTITUT MATHÉMATIQUE
Nouvelle série, tome 31 (45) 1982, 51—63

ПРАВИЛО ИНДУКЦИИ В ДОКАЗАТЕЛЬСТВАХ ОПРОВЕРЖЕНИЕМ С ПРИМЕНЕНИЕМ К АВТОМАТИЧЕСКОМУ ДОКАЗАТЕЛЬСТВУ ТЕОРЕМ

Петар З. Хотомски

Работа состоит из двух частей. В первой части, исходя от схемы-аксиом индукции принадлежащей теории первого порядка $\mathcal{K}$, выводится правило индукции в теории $\mathcal{K}^*$, аксиомы которой полученны из аксиом теории $\mathcal{K}$ с помощью сколемизации. Рассматриваются обобщенные правила. Приводится правило, применимое к членам дизьюнкции. Устанавливается полнота приведенных правил. В приложении к первой части сформулирован „принцип обратной индукции" для метатеоретических доказательств.

Во второй части, в контексте автоматического доказательства теорем, на основании результатов первой части, приводится правило бинарной индукции которое, совместно с правилом резолюции, применимо для автоматического доказательства теорем.

I. Правила индукции в теориях первого порядка

1. Правила $P1$ и $P2$. Пусть теория первого порядка содержит следующую схему-аксиом индукции:

(1) $$A(0) \Rightarrow (\forall x (A(x) \Rightarrow A(Sx)) \Rightarrow \forall x A(x))$$

где $A(x)$ произвольная формула, Sx — непосредственно следующий за x, а формулы $A(0)$ и $A(Sx)$ полученны из $A(x)$ замещением всех свободных вхождений переменной x на терм 0, т.е. Sx, соотвественно.

Обозначим через $A_x(t)$ формулу полученную из $A(x)$ замещением каждого свободного вхождения переменной x на терм t, который свободен для x в $A(x)$.

Теперь (1) можно записать в виде

$$A_x(0) \Rightarrow (\forall x (A(x) \Rightarrow A_x(Sx)) \Rightarrow \forall x A(x))$$

Пусть переменная y не входит в формулу $A(x)$. Тогда формула (1) эквивалентна формуле

(2) $$A_x(0) \Rightarrow (\forall y (A_x(y) \Rightarrow A_x(Sy)) \Rightarrow \forall x A(x))$$

В дальнейшем, для всех формул в настоящей работе будем считать что никакая переменная не входит в формулу и свободно и связанно, так как это всегда можно получить переименованием переменных, также и что различные вхождения кванторов связывают различные переменные.

Формула (2) эквивалентна формуле

(3) $$\forall x \exists y (A_x(0) \Rightarrow (\neg A(x) \Rightarrow (A_x(y) \wedge \neg A_x(Sy))))$$

Пусть $z_1, z_2, \ldots, z_s$ все свободные переменные в формуле (3), т.е. все свободные переменные в $A_x(0)$. Тогда формула

$$\forall z_1 \cdots \forall z_s \forall x \exists y (A_x(0) \Rightarrow (\neg A(x) \Rightarrow (A_x(y) \wedge \neg A_x(Sy)))) \tag{4}$$

является замыканием формулы (3).

Пусть $\mathcal{K}$ теория первого порядка в которой формула (4) является собственной схемой-аксиом индукции. Будем считать что все аксиомы теории $\mathcal{K}$ замкнуты.

Приведем сначала, согласно [1] и [2], описание процесса сколемизации. Формула в предваренной форме универсальна, если все кванторы в ее приставке являются кванторами всеобщности. Пусть A замкнутая формула в предваренной форме. Формула A^*, не содержащая кванторов получаестя следующим образом: Если A универсальна, то A^* получается из A вычеркиванием кванторной приставки. Если A имеет вид $\forall x_1 \ldots \forall x_n \exists y B$, $n \geqslant 0$, то вводится новый n-местный функциональный символ f; в случае $n=0$, f — новая константа. Обозначим через A^0 формулу $\forall x_1 \cdots \forall x_n B_y(f(x_1, \ldots, x_n))$ Формула A^0 содержит на один квантор существования меньше чем A. Если A^0 универсальна, то строятся A^{00}, A^{000} итд. пока не получится универсальная формула. Вычеркиванием кванторной приставки этой универсальной формулы получается формула A^*. Будем говорить что A^* полученна сколемизацией формулы A. Новую n-местную функциональую букву f называем функцией Сколема n аргументов, а для $n=0$ константной Сколема. При этом предполагается что для различных формул вводятся различные функциональные буквы.

В дальнейшем потребуется также следующее предложение: вторая ε-теорема ([1], стр. 111.).

Пусть τ^* *теория первого порядка, аксиомы которой полученны сколемизацией аксиом теории первого порядка* τ. *Тогда:* а) *если* ε *формула теории* τ и $\vdash_{\tau^*} \varepsilon$, *то* $\vdash_{\tau} \varepsilon$; б) *теория* τ *непротиворечива тогда и только тогда, когда непротиворечива теория* τ^*.

Сколемизируя формулу (4) получаем формулу

$$A_x(0) \Rightarrow (\neg A(x) \Rightarrow (A_x(g(x, z_1, \ldots, z_s)) \wedge \neg A_x(Sg(x, z_1, \ldots, z_s)))) \tag{4*}$$

где $z_1, \ldots, z_s$ все свободные переменные в $A_x(0)$, g — функция Сколема $(s+1)$ аргументов[1].

Принимаем формулу (4*) за собственную схему-аксиом в $\mathcal{K}^*$. Пусть остальные аксиомы теории $\mathcal{K}^*$ полученны сколемизацией остальных аксиом теории $\mathcal{K}$. Тогда для $\mathcal{K}$ и $\mathcal{K}^*$ справедлива вторая ε-теорема. Заметим что $\mathcal{K}^*$ является консервативным расширением теории $\mathcal{K}$, так как все аксиомы теории $\mathcal{K}$ становятся теоремами в $\mathcal{K}^*$.

С помощью правила MP (modus ponens) из схемы-аксиом (4*) в $\mathcal{K}^*$ получаем следующее правило:

$$P1' \quad A_x(0), \neg A(x) \vdash_{\mathcal{K}^*} A_x(g(x, z_1, \ldots, z_s)) \wedge \neg A_x(Sg(x, z_1, \ldots, z_s))$$

где $z_1, \ldots, z_s$ все свободные переменные в $A_x(0)$, g — функция Сколема $(s+1)$ аргументов.

[1] $A_x(g(x, z_1, \ldots, z_s)) \equiv [A_x(y)]_y (g(x, z_1, \ldots, z_y))$

Пусть z_i одна из переменных $z_1, \dots, z_s$. Из (4*) подстановкой $x \to z_i$, (z_i свободна для x, так как ни одна из переменных не входит в формулу и свободно и связанно), выводим теорему:

$$A_x(0) \Rightarrow (\neg A_x(z_i) \Rightarrow (A_x(g(z_i, z_1, \dots, z_s)) \wedge \neg A_x(Sg(z_i, z_1, \dots, z_s))))$$

из которой по MP получаем правило:

$$P1'' \quad A_x(0),\ \neg A_x(z_i) \vdash_{\mathcal{K}^*} A_x(g(z_i, z_1, \dots, z_s)) \wedge \neg A_x(Sg(z_i, z_1, \dots, z_s))$$

Правила $P1'$ и $P1''$ можно объединить в более общее правило:

$$P1 \quad A_x(0),\ \neg A_x(z) \vdash_{\mathcal{K}^*} A_x(g(z, z_1 \dots, z_s)) \wedge \neg A_x(Sg(z, z_1 \dots, z_s))$$

где z переменная, свободна для x в $A(x)$; $z_1, \dots, z_s$ все свободные переменные в $A_x(0)$; g — функция Сколема. В случае когда z совпадает с x, правило $P1$ становится $P1'$.

Дальше, из (4*) подстановкой $x \to t$, t произвольный терм свободен для x в $A(x)$, выводим теорему

$$A_x(0) \Rightarrow (\neg A_x(t) \Rightarrow (A_x(g(t, z_1, \dots, z_s)) \wedge \neg A_x(Sg(t, z_1, \dots, z_s))))$$

С помощью MP получаем следующее правило:

$$P2 \quad A_x(0),\ \neg A_x(t) \vdash_{\mathcal{K}^*} A_x(g(t, z_1, \dots, z_s)) \wedge \neg A_x(Sg(t, z_1 \dots, z_s))$$

где терм t свободен для x в $A(x)$; $z_1, \dots, z_s$ все свободные переменные в $A_x(0)$; g - функция Сколема $(s+1)$ аргументов. Значительный частный случай правила $P2$ получается когда $A_x(0)$ не содержит свободных переменных:

$$A_x(0), \neg A_x(t) \vdash_{\mathcal{K}^*} A_x(g(t)) \wedge \neg A_x(Sg(t))$$

где $A_x(0)$ замкнутая формула, терм t свободен для x в $A(x)$, g — функция Сколема одного аргумента.

Правило $P2$ можно трактовать как обобщение правила $P1$, так как если терм t свободная переменная, то $P2$ становится $P1$.

Проилюстрируем применение правила $P2$ на примерах.

Пример 1. Доказательство reductio ad absurdum для теоремы формальной арифметики: $\forall x\,(x = 0 + x)$, с помощью $P2$.

1. $a \neq 0 + a$ отрицание формулы $\forall x\,(x = 0 + x)$ и сколемизация, a - конст.
2. $0 = 0 + 0$ теорема $t = t + 0$
3. $ga = 0 + ga$
4. $(ga)' \neq 0 + (ga)'$ — (3, 4:) 2 и 1, правило $P2$ для терма a. Мы писали ga вместо $g(a)$, и $(ga)'$ вместо $Sg(a)$
5. $(ga)' = (0 + ga)'$ 3, теорема $t = r \Rightarrow t' = r'$
6. $(ga)' = 0 + (ga)'$ 5, теоремы $(t + r)' = t + r'$ и $t = r \wedge r = s \Rightarrow t = s$
7. противоречие 4 и 6.

Пример 2. Пусть $F_x(0)$ и $\forall x(F(x) \Rightarrow F_x(Sx))$ теоремы теории первого порядка с индукцией. Будем считать что $F_x(0)$ замкнута. С помощью $P2$ докажем $\forall x F(x)$.

а. Доказательство без сведения к противоречию

1. $F_x(0)$	
2. $\forall x(F(x) \Rightarrow F_x(Sx))$	данные теоремы
3. $\neg F(x)$	гипотеза
4. $F_x(g(x)) \wedge \neg F_x(Sg(x))$	1 и 3, правило $P2$ (в самом деле $P1'$)
5. $\neg F(x) \Rightarrow (F_x(g)) \wedge \neg F_x(Sg(x)))$	1, 3 и 4, теорема дедукции и MP для 1.
6. $(F_x(g(x)) \Rightarrow F_x(Sg(x))) \Rightarrow F(x)$	5, контрапозиция, тавтологии
7. $F_x(g(x)) \Rightarrow F_x(Sg(x))$	2, подстановка $x \to g(x)$
8. $F(x)$	6 и 7 по MP
9. $\forall x F(x)$	8, правило обобщения

б. Доказательство reductio ad absurdum

1. $F_x(0)$	
2. $\forall x(F(x) \Rightarrow F_x(Sx))$	данные теоремы
3. $\neg F_x(a)$	отрицание формулы $\forall x F(x)$; а — константа Сколема
4. $F_x(g(a))$	1 и 3, правило $P2$
5. $\neg F_x(Sg(a))$	
6. $F_x(g(a)) \Rightarrow F_x(Sg(a))$	2, подстановка $x \to g(a)$
7. $F_x(Sg(a))$	4 и 6 по MP
8. противоречие	5 и 7.

2. **Правило** $P3$ Определение 1. а) Вместо $x \to t$ будем писать t/x и называть *подстановочной компонентой*, где x переменная и t терм который не содержит x. б) Множество подстановочных компонент $\sigma = \{t_1/x_1, \ldots, t_n/x_n\}$, $x_i \neq x_j$, называется *подстановкой*. в) *Применение подстановки* к некоторой формуле A, это одновременное замещение всех свободных вхождений переменных x_i в A на термы t_i. г) Формула A_σ, полученная в результате применения подстановки σ к формуле A, называется *σ-примером формулы A* тогда и только тогда, когда термы t_i подстановки σ свбодны для переменных x_i в формуле A; $1 \leqslant i \leqslant n$. д) Подстановка σ называется *унификатором* для формул A и B тогда и только тогда, когда σ-примеры этих формул совпадают (т.е. $A_\sigma \equiv B_\sigma$).

Предложение. *Пусть формулы A и $\neg B_x(t)$ теории $\mathcal{K}^*$ удовлетворяют условиям:* (i) *для формул A и $B_x(0)$ существует унификатор σ, т.е. $A_\sigma \equiv (B_x(0))_\sigma$. (Можно считать что переменная x не входит в A, поэтому не входит в σ)* (ii) *применением подстановки σ к формуле $B_x(g(t,z_1,\ldots,z_s))$, (где g — функция и $z_1,\ldots,z_s$ все свободные переменные в $B_x(0)$) получается σ-пример, т.е. $(B_x(g(t,z_1,\ldots,z_s)))_\sigma$.*

Тогда в теории $\mathcal{K}^*$ выводима формула $(B_x(g(t,z_1,\ldots,z_s)))_\sigma \wedge (\neg B_x(Sg(t, z_1,\ldots,z_s)))_\sigma$

Доказательство. Так как по определению унификатора и σ-примера, термы t_i подстановочных компонент t_i/x_i свободны для переменных x_i в формулах A, $B_x(0)$ и $B_x(g(t,z_1,\ldots,z_s))$, то σ-примеры этих формул выводимы в теории $\mathcal{K}^*$. Из условия (ii) следует, что применение σ к формуле $B_x(t)$ приводит к σ-примеру $(B_x(t))_\sigma$. Действительно, если какой нибудь терм t_i подстановочной компоненты t_i/x_i, не был бы свободен для x_i в $B_x(t)$, тогда этот терм t_i небыл бы свободен для x_i и в $B_x(g(t,z_1,\ldots,z_s))$, что противоречит требованию в (ii). Напомним, что t свободен для x в $B(x)$. Поэтому в теории $\mathcal{K}^*$ существует следующой вывод:

1. A
2. $\neg B_x(t)$
3. $(\neg B_x(t))_\sigma$ — σ — пример формулы 2. (условие (ii))
4. $(B_x(0))_\sigma$ — σ — пример формулы 1. (условие (i))
5. $B_x(0) \Rightarrow (\neg B(x) \Rightarrow (B_x(g(x,z_1,\ldots,z_s)) \wedge \neg B_x(Sg(x,z_1,\ldots,z_s))))$

   аксиома (4*) для формулы $B(x)$; $z_1,\ldots,z_s$ свободные переменные в $B_x(0)$.
6. $B_x(0) \Rightarrow (\neg B_x(t) \Rightarrow (B_x(g(t,z_1,\ldots,z_s)) \wedge \neg B_x(Sg(t,z_1,\ldots,z_s))))$

   из 5, подстановка $x \to t$; так как t свободен для x в $B(x)$, следовательно t свободен для x и в $B(g(x,z_1,\ldots,z_s))$.
7. $(B_x(0))_\sigma \Rightarrow ((\neg B_x(t))_\sigma \Rightarrow ((B_x(g(t,z_1,\ldots,z_s)))_\sigma \wedge (\neg B_x(Sg(t,z_1,\ldots,z_s)))_\sigma))$

   σ — пример формулы 6.
8. $(B_x(g(t,z_1,\ldots,z_s)))_\sigma \wedge (\neg B_x(Sg(t,z_1,\ldots,z_s)))_\sigma$ — из 7,4 и 3 по МР

На основании предложения 1. получается следующее правило:

Р3 $\quad A, \neg B_x(t) \vdash_{\mathcal{K}^*} (B_x(g(t,z_1,\ldots,z_s)))_\sigma \wedge (\neg B_x(Sg(t,z_1,\ldots,z_s)))_\sigma$

(при условиях (i) и (ii)).

Пример 3. Доказательство reductio ad absurdum для теоремы формальной арифметики $\forall x \forall y\,(x+y=y+x)$, с помощью $P3$.

1. $a+b \neq b+a$ — отрицание данной формулы; a, b — константы Сколема
2. $x+0=0+x$ — теорема

3. $a+gb=gb+a$ } 2 и 1, правило $P3$ для терма b и $\sigma=\{a/x\}$.
4. $a+(gb)'\neq(gb)'+a$ } $(gb)'$ стоит вместо $Sg(b)$.
5. $(a+gb)'=(gb+a)'$ 3, теорема $t=r\Rightarrow t'=r'$
6. $a+(gb)'=(gb+a)'$ 5, теорема $t+r'=(t+r)'$ и теоремы о равенстве
7. $(gb)'+a=(gb+a)'$ теорема $t'+r=(t+r)'$
8. $a+(gb)'=(gb)'+a$ 6 и 7, теоремы о равенстве
9. противоречие 8 и 4.

3. Применение к членам дизьюнкции — правило $P4$. Предложение 2. *Пусть* D_1: $A\vee C_1$ *и* D_2: $\urcorner B_x(t)\vee C_2$ *формулы в* $\mathcal{K}^*$, *такие что к формулам* A *и* $\urcorner B_x(t)$ *применимо правило* P3, *причем* σ *унификатор для* A *и* $B_x(0)$ *и его применением к формулам* C_1 *и* C_2 *получаются* σ — *примеры* $C_{1\sigma}$ *и* $C_{2\sigma}$. *Тогда из* D_1 *и* D_2 *выводимы формулы*

$$(B_x(g(t,z_1,\ldots,z_s)))_\sigma\vee C_{1\sigma}\vee C_{2\sigma}\quad и\quad (\urcorner B_x(Sg(t,z_1,\ldots,z_s)))_\sigma\vee C_{1\sigma}\vee C_{2\sigma}$$

где $z_1,\ldots,z_s$ *все свободные переменные в* $B_x(0)$; g — *функция Сколема.*

Доказательство. Условиями предложения обеспеченно что термы которыми замещаются свободные вхождения переменных, свободны для этих переменных. Поэтому в теории $\mathcal{K}^*$ существует следующий вывод:

1. $\urcorner C_1\Rightarrow A$ формула D_1 записанна с помощью импликаци
2. $\urcorner C_2\Rightarrow\urcorner B_x(t)$ формула D_2 записанна с помощью импликации
3. $\urcorner C_1\wedge\urcorner C_2\Rightarrow A\wedge\urcorner B_x(t)$ 1 и 2, тавтология
4. $\urcorner C_{1\sigma}\wedge\urcorner C_{2\sigma}\Rightarrow(B_x(0))_\sigma\wedge(\urcorner B_x(t))_\sigma$ 3, σ — пример $(A_\sigma\equiv(B_x(0))_\sigma)$
5. $(B_x(0))_\sigma\Rightarrow((\urcorner B_x(t))_\sigma\Rightarrow((B_x(g(t,z_1,\ldots,z_s)))_\sigma\wedge(\urcorner B_x(Sg(t,z_1,\ldots,z_s)))_\sigma))$
   теорема (шаги 5, 6 и 7 доказательства предложения 1.)
6. $(B_x(0))_\sigma\wedge(\urcorner B_x(t))_\sigma\Rightarrow(B_x(g(t,z_1,\ldots,z_s)))_\sigma\wedge(\urcorner B_x(Sg(t,z_1,\ldots,z_s)))_\sigma$
   из 5, тавтология
7. $\urcorner C_{1\sigma}\wedge\urcorner C_{2\sigma}\Rightarrow(B_x(g(t,z_1,\ldots,z_s)))_\sigma\wedge(\urcorner B_x(Sg(t,z_1,\ldots,z_s)))_\sigma$
   из 4 и 6, транзитивность импликации
8. $(B_x(g(t,z_1,\ldots,z_s)))_\sigma\vee C_{1\sigma}\vee C_{2\sigma}$ } из 7, тавтологии
9. $(\urcorner B_x(Sg(t,z_1,\ldots z_s)))_\sigma\vee C_{1\sigma}\vee C_{2\sigma}$ } из 7, тавтологии

На основании предложений 1. и 2. получается правило $P4$: Пусть D_1: $A\vee C_1$ и D_2: $\urcorner B_x(t)\vee C_2$ теоремы в $\mathcal{K}^*$ такие что: (i) для формул A и $B_x(0)$ существует унификатор σ, (ii) применением σ к формулам $B_x(g(t,z_1,\ldots,z_s))$, C_1 и C_2, (где g — функция Сколема и $z_1,\ldots,z_s$ все свободные переменные в $B_x(0)$), получаются σ — примеры.

Тогда следующие формулы теоремы в $\mathcal{K}^*$:

$(B_x(g(t, z_1, \ldots, z_s)))_\sigma \vee C_{1\sigma} \vee C_{2\sigma}$ и $(\neg B_x(Sg(t, z_1, \ldots, z_s)))_\sigma \vee C_{1\sigma} \vee C_{2\sigma}$

Записываем:

$$P4 \quad D_1, D_2 \mid\!\overline{\,_{\mathcal{K}^*}}\, (B_x(g(t, z_1, \ldots, z_s)))_\sigma \vee C_{1\sigma} \vee C_{2\sigma}, (\neg B_x(Sg(t, z_1, \ldots, z_s)))_\sigma \vee C_{1\sigma} \vee C_{2\sigma}$$

(при условиях (i) и (ii))

Пример 4. В примере 3. для доказательства $\forall x \forall y (x+y=y+x)$ мы использовали и теоремы которые также доказываются с помощью индукции. Приведем здесь доказательство с помощью $P4$, которое опирается только на теоремы — доказуемы без индукции.

1. $a+b \neq b+a$ отрицание и сколемизация данной формулы; a, b — конст.
2. $z \neq y \vee z+0=y$ теорема (доказуема без индукции)
3. $a \neq 0+a \vee a+gb=gb+a$
4. $a \neq 0+a \vee a+(gb)' \neq (gb)'+a$ } из 2 и 1 по $P4$ для терма b. $\sigma=\{a/z, (0+a)/y\}$, $z \neq y$ в качестве C_1; C_2 не существует.
5. $0=0+0$ теорема (доказуема без индукции)
6. $ha=0+ha \vee a+gb=gb+a$
7. $(ha)' \neq 0+(ha)' \vee a+gb=gb+a$ } из 5 и 3 по $P4$ для терма a, $\sigma=\varnothing$, C_1 не существует, а C_2: $a+gb=gb+a$.
8. $(ha)'=(0+ha)' \vee a+gb=gb+a$ из 6, теорема $t=r \Rightarrow t'=r'$
9. $(ha)'=0+(ha)' \vee a+gb=gb+a$ из 8, теорема $(t+r)'=t+r'$
10. $a+gb=gb+a$ из 7 и 9, тавтология $(p \vee q) \wedge (\neg p \vee q) \Leftrightarrow q$
11. $a+(gb)' \neq (gb)'+a$ шаги 6—9 беря 4 вместо 3 на шаге 6.
12. $a+(gb)'=gb+a'$ из 10, теоремы использованные на шагах 8 и 9.
13. $gb+a' \neq (gb)'+a$ из 12 и 11, теорема $(t=r \wedge t \neq s) \Rightarrow r \neq s$
14. $x+0'=x'+0$ теорема (доказуема без индукции)
15. $gb+(wa)'=(gb)'+wa$
16. $gb+(wa)'' \neq (gb)'+(wa)'$ } из 14 и 13 по $P4$ для терма a, $\sigma=\{gb/x\}$ C_1 и C_2 не существуют — $P4$ становится $P3$
17. $gb+(wa)''=(gb)'+(wa)'$ из 15, теоремы использованные в 8 и 9.
18. противоречие 16 и 17.

Примечание. Так как переменная x не входит в унификатор σ, то справедливо: $(B(x))_\sigma \equiv B_\sigma(x)$ и $(B_x(0))_\sigma \equiv B_{\sigma x}(0)$, где $B_{\sigma x}(0)$ формула, полученна замещением каждого свободного вхождения x в $B_\sigma(x)$, на терм 0. Также, $(B_x(g(x, z_1, \ldots, z_s)))_\sigma \equiv B_{\sigma x}(g(x, z_1\sigma, \ldots, z_s\sigma))$, где $g(x, z_1\sigma, \ldots, z_s\sigma) \equiv (g(x, z_1, \ldots, z_s))_\sigma$. Поэтому, применением σ к аксиоме (4*) для формулы $B(x)$, получается следующая теорема в $\mathcal{K}^*$:

$$B_{\sigma x}(0) \Rightarrow (\neg B_\sigma(x) \Rightarrow (B_{\sigma x}(g(x, z_1\sigma, \ldots, z_s\sigma)) \wedge \neg B_{\sigma x}(Sg(x, z_1\sigma, \ldots, z_s\sigma))))$$

С другой стороны, если в (4*) взять формулу $B_\sigma(x)$ в качестве $A(x)$, то получится следующая аксиома в $\mathcal{K}^*$:

$$B_{\sigma x}(0) \Rightarrow (\neg B_\sigma(x) \Rightarrow (B_{\sigma x}(f(x, y_1, \ldots, y_k)) \wedge \neg B_{\sigma x}(Sf(x, y_1, \ldots, y_k))))$$

где $y_1, \ldots, y_k$ все свободные переменные в $B_{\sigma x}(0)$; f — функция Сколема $(k+1)$ аргументов. Легко убедится что $\{y_1, \ldots, y_k\} = Pr(z_1\sigma, \ldots, z_s\sigma)$ где $Pr(z_1\sigma, \ldots, z_s\sigma)$ множество переменных, входящих в $\{z_1\sigma, \ldots, z_s\sigma\}$. Поэтому можно считать что $f(x, y_1, \ldots, y_k)$ является другим обозначением для $g(x, z_1\sigma, \ldots, z_s\sigma)$. В связи с этим, правило $P4$ можно переформулировать следующим образом:

$P4'$ $D_1, D_2 \vdash_{\mathcal{K}^*} B_{\sigma x}(f(t\sigma, y_1, \ldots, y_k)) \vee C_{1\sigma} \vee C_{2\sigma}, \quad \neg B_{\sigma x}(Sf(t\sigma, y_1, \ldots, y_k)) \vee C_{1\sigma}$ $\vee C_{2\sigma}$ (при условиях (i) и (ii))

где f — функция Сколема $(k+1)$ аргументов; $y_1, \ldots, y_k$ все свободные переменные в $B_{\sigma x}(0)$; $t\sigma$ — терм полученный применением σ к терму t.

4. Правило $P5$. Предложение 3. *Пусть* D_1: $A \vee C_1$ и D_2: $\neg B \vee C_2$ *формулы такие что:* (i) *существует подстановка* σ, *такая что к* A_σ *и* $\neg B_\sigma$ *применимо* $P2$, *т.е.* A_σ *формула вида* $F_x(0)$ *и* $\neg B_\sigma$ *вида* $\neg F_x(t)$, (*терм* t *свободен для* x *в* $F(x)$; (ii) *применением* σ *к формула* A, B, C_1, C_2 *получаются* σ — *примеры. Тогда* $\mathcal{K}^*$ *выводимы формулы:*

$$F_x(g(t, z_1 \ldots, z_s)) \vee C_{1\sigma} \vee C_{2\sigma} \quad и \quad \neg F_x(Sg(t, z_1, \ldots, z_s)) \vee C_{1\sigma} \vee C_{2\sigma}$$

где — функция Сколема $(s+1)$ *аргументов и* $z_1, \ldots z_s$ *все свободные переменные в* $F_x(0)$.

Доказательство. При условиях (i) и (ii) в $\mathcal{K}^*$ существует вывод:

1. $\neg C_1 \Rightarrow A$ — формула D_1 записанна с помощью импликации
2. $\neg C_2 \Rightarrow \neg B$ — формула D_2 записанна с помощью импликации
3. $\neg C_1 \wedge \neg C_2 \Rightarrow A \wedge \neg B$ — 1 и 2, тавтологии
4. $\neg C_{1\sigma} \wedge \neg C_{2\sigma} \Rightarrow F_x(0) \wedge \neg F_x(t)$ — σ — пример формулы 3
5. $F_x(0) \wedge \neg F_x(t) \Rightarrow F_x(g(t, z_1, \ldots, z_s)) \wedge \neg F_x(Sg(t, z_1, \ldots, z_s))$
   теорема из которой полученно $P2$
6. $\neg C_{1\sigma} \wedge \neg C_{2\sigma} \Rightarrow F_x(g(t, z_1, \ldots, z_s)) \wedge \neg F_x(Sg(t, z_1, \ldots, z_s))$ — 4 и 5, транзитивность импликации
7. $F_x(g(t, z_1, \ldots, z_s)) \vee C_{1\sigma} \vee C_{2\sigma}$
8. $\neg F_x(Sg(t, z_1, \ldots, z_s)) \vee C_{1\sigma} \vee C_{2\sigma}$ — из 6, тавтологии

На основании предложения 3. получается правило:

$P5$ $A \vee C_1, \neg B \vee C_2 \vdash_{\mathcal{K}^*} F_x(g(t, z_1, \ldots, z_s)) \vee C_{1\sigma} \vee C_{2\sigma}, \neg F_x(Sg(t, z_1, \ldots, z_s))$ $\vee C_{1\sigma}, \vee C_{2\sigma}$ (при условиях (i) и (ii)).

Можно считать что теоремы которые в $\mathcal{K}^*$ выведенны с помощью любого из правил $P1$, $P2$, $P3$, $P4$, в самом деле выведенны с помощью $P5$. Действительно, не трудно убедится что каждое из правил $P1$—$P4$ является частным случаем правила $P5$. Также, каждое из них является обобщением всех ему предшествующих правил.

Для иллюстрации специфики правила $P5$ приводим пару формул к которым применимо $P5$, но $P4$ не применимо:

D_1: $P(0, h(x), x) \vee Q(x)$ где P, Q, R — предикатные буквы

D_2: $\neg P(f(y,z), w, f(0,w)) \vee R(w,y)$ h, f — функциональные буквы

x, y, z, w — переменные

Применяя подстановку $\sigma = \{0/y, h(0)/w, 0/x, h(0)/z\}$ получаем

$D_{1\sigma}$: $P(0, h(0), 0) \vee Q(0)$, $D_{2\sigma}$: $\neg P(f(0, h(0)), h(0), f(0, h(0))) \vee R(h(0), 0)$

Поэтому из D_1 и D_2 по $P5$ выводятся формулы:

$$P(g(f(0, h(0))), h(0), g(f(0, h(0)))) \vee Q(0) \vee R(h(0), 0)$$

$$\neg P(Sg(f(0, h(0))), h(0), Sg(f(0, h(0)))) \vee Q(0) \vee R(h(0), 0)$$

где g — функция Сколема одного аргумента.

5. Полнота правил $P1$—$P5$. Так как полнота правил $P1$—$P4$ востонавливается аналогично доказательству полноты для $P5$, то приводим только предложение для $P5$.

Предложение 4. *Правило $P5$ полно в смысле вывода в теории $\mathcal{K}^*$.*

Доказательство. Применение правила $P5$ к теоремам теории $\mathcal{K}^*$ приводит к теоремам теории $\mathcal{K}^*$, это следует из предложения 3. Нужно еще доказать что с помощью $P5$ выводимы все те теоремы которые выводимы с помощью правила $P1'$. Правило $P1'$ непосредственно следует из схемы-аксиом (4*), а (4*) может быть получена с помощью правила $P1'$ и теоремы дедукции, следовательно правило $P1'$ полно в смысле вывода в $\mathcal{K}^*$. Однако, $P1'$ является частным случаем $P5$, так как в случае когда подстановка σ пустая, C_1 и C_2 не существуют и терм t в формуле $\neg F_x(t)$ совпадает с переменной x, т.е. когда формулы D_1 и D_2 имеют вид $F_x(0)$ и $\neg F(x)$, тогда $P5$ превращается в $P1'$: Следовательно, правило $P5$ обладает полнотой в смысле вывода в $\mathcal{K}^*$.

Рассмотрим еще корректность доказательств reductio ad absurdum для теорем теории $\mathcal{K}$, когда в них используется правило $P5$.

Предложение 5. *Замкнутая формула B теории $\mathcal{K}$ теорема в $\mathcal{K}$ тогда и только тогда, когда в теории полученной из $\mathcal{K}^*$ добавлением аксиомы $(\neg B)^*$ и вычеркиванием схемы-аксиом индукции, с помощью $P5$ выводимо противоречие.*

Доказательство. Пусть B теорема в $\mathcal{K}$. Если $\mathcal{K}$ непротиворечива, то из множества аксиом теории $\mathcal{K}$ дополненного аксиомой $\neg B$, выводимо противоречие. Тогда согласно второй ε-теореме, противоречива и теория полученная расширением теории $\mathcal{K}^*$ путем добавления аксиомы $(\neg B)^*$. Так как правило $P5$ полно в смысле вывода в теории $\mathcal{K}^*$ (полнста доказана независимо от остальных аксиом в $\mathcal{K}^*$) ,следует что в расширеной теории $\mathcal{K}^*$ можно вывести противоречие с помощью $P5$. Следовательно, каждая теорема теории $\mathcal{K}$ может быть таким образом доказана в расширеной теории $\mathcal{K}^*$, из которой вычеркнута схема-аксиом индукции.

Обратно, пусть B замкнутая формула теории $\mathcal{K}$ и пусть теория $\mathcal{K}^*$ доплнена аксиомой $(\neg B)^*$. Если в так расширеной теории выведено противоречие с помощью $P3$, то благодаря полноте правила $P3$ и на основании второй ε - теоремы, противоречива и теория, полученна из $\mathcal{K}$ добавлением аксиомы $\neg B$. Так как, по предположению, $\mathcal{K}$ непротиворечива, то B теорема в $\mathcal{K}$.

Приложение: Применение в метатеории — принцип „Обратной индукции"

Формула (3) эквивалентна формуле

$$(3') \qquad \forall x\,(A_x(0) \Rightarrow (\neg A(x) \Rightarrow \exists y\,(A_x(y) \wedge \neg A_x(Sy))))$$

Из нее подстановкой $x \to t$, терм t свободен для x в $A(x)$, выводится

$$(3'') \qquad A_x(0) \Rightarrow (\neg A_x(t) \Rightarrow \exists y\,(A_x(y) \wedge \neg A_x(Sy)))$$

Формула (3''), с точностью до счетного множества свойств, формализирует следующий принцип „обратной индукции" для натуральных чисел:

Если натуральное число 1 обладает свойством P и натуральное число m не обладает свойством P, тогда существует натуральное число k, обладающее свойством P, таксе что $(k+1)$ не обладает свойством P.

Не трудно уверится в „естественность" этого принципа и возможность его применения в метатеоретических доказательствах типа reductio ad absurdum.

Такое доказательство начинается с „существует натуральное число m такое что $\neg P(m)$", что получается из предполсжения что утверждение, подлежащее доказательству $\forall n P(n)$, не верно. Когда доказанно $P(1)$, то из $P(1)$ и $\neg P(m)$ по принципу обратной индукции получаем $P(k)$ и $\neg P(k+1)$, из чего надо вывести противоречие.

Заметим что принцип обратной индукции дает возможность вывести противоречие из $P(1)$ и $\neg P(m)$ прямым путем, т.е. без предварительного вывода $\forall n\, P(n)$ с помощью полной индукции.

Пример. Пусть $P(n)$: $2+4+\cdots+2n=n(n+1)$. Докажем: для каждого натурального числа n справедлизо $P(n)$. Предположим противное, т.е. что утверждение не верно. Тогда существует натуральное число m такое что $\neg P(m)$. $P(1)$ верно, потому что $2=1\,(1+1)$. Так как $P(1)$ и $\neg P(m)$, то на основании принципа обратной индукции, существует натуральное число k, для которого $P(k)$ и $\neg P(k+1)$, т.е. $2+\cdots+2k=k(k+1)$ и $2+{}+\cdots+2(k+1)\neq(k+1)(k+1+1)$. Следовательно, $k(k+1)+2(k+1)\neq(k+1)(k+1+1)$ и $(k+1)(k+2)\neq(k+1)(k+2)$, что приводит к противоречию. Этим утверждение доказанно.

Отметим что принцип обратной индукции является вариантом принципа наименьшего числа.

II Правило индукции в автоматическом доказательстве теорем

1. Введение. Пусть аксиомы теории $\mathcal{K}^*$ полученны сколемизацией аксиом теории первого порядка $\mathcal{K}$. Каждая собственная аксиома теории $\mathcal{K}^*$ может быть представлена в виде $A_1 \wedge \cdots \wedge A_n$, где A_i имеют вид $L_1^i \vee \ldots \vee L_r^i$, а L_j^i — атомные формулы или их отрицания. Атомная формула или ее отрицание называется *литерой*. Дизъюнкция литер называется *дизъюнктом*. Пустой дизъюнкт $\varnothing$, это дизъюнкт не содержащий литер. Множество литер $L=\{L_1, \ldots, L_k\}$ называется *унифицируемым*, если существует такая подстановка σ, что в результате ее применения к каждому элементу множества L, получается одноэлементное множество L_σ, т.е. $L_{1\sigma}=L_{2\sigma}=\cdots=L_{k\sigma}$. *Наиболее общим унификатором* (НОУ) для множества литер L, называется такой унификатор σ, что если θ какой-нибудь унификатор для L, дающий L_θ, то найдется подстановка δ для которой $L_{\sigma\delta}=L_\theta$. С точностью до алфавитных вариантов существует единственный НОУ. Существует *алгоритм унификации*, [6], который находит НОУ для унифицируемого множества литер и сообщает о неудаче, если множество неунифицируемо.

Пусть S множество дизъюнктов, полученных из собственных аксиом теории $\mathcal{K}^*$. Для случая когда в S находятся дизъюнкты полученные из схемы-аксиом выражающей подстановочность равенства, либо схемы-аксиом математической индукции, в [8] продемострирована особая f-техника (f-matcing technique), обоснованная на аксиомах второго порядка, которая используется совместно с правилом резолюции.

Однако, присуствие в исходном множестве S, дизъюнктов полученных из схемы-аксиом, кроме того что удлиняет вывод, дает возможность порождения большого количества лишних следствий. Появившиеся таким образом, бесполезные дизъюнкты приводят в свою очередь, к появлению новых бесполезных дизъюнктов, что приводит к рассширению и „загрязнению" пространства поиска, чем понижается эффективность метода. В случае теорий с равенством эти недостатки устраненны в [7] путем введения правила парамодуляции, которое дает возможность осуществить опровержение без использования аксиом равенства.

Здесь вводим правило индукции, которое позволяет выключить из исходного множества дизъюнкты, представляющие аксиому индукции. Это освобождает от работы с произвольной формулой, входящей в схему-аксиом, и приводит к уменьшению количества порождаемых дизъюнктов.

2. Правило бинарной индукции. Пусть D_1: $P(t_1, \ldots, t_i, \ldots, t_n) \vee C_1$; D_2: $\neg P(v_1, \ldots, v_i(t), \ldots, v_n) \vee C_2$

дизъюнкты (где C_1 и C_2 дизъюнкты, t — некоторый из термов v_i, либо их подтерм, $1 \leqslant i \leqslant n$) такие, что для литер $P(t_1, \ldots, t_i, \ldots, t_n)$ и $P(v_1, \ldots, v_i(0), \ldots, v_n)$ существует НОУ σ. Так как D_1 и D_2 не содержат кванторов, то выполненны все условия для применения правила $P4$, введенного в первой части. Поэтому, получается правило:

Из дизъюнктов D_1 и D_2, не имеющих общих переменных, и таких что для литер $P(t_1, \ldots, t_i, \ldots, t_n)$ и $P(v_1, \ldots, v_i(0), \ldots, v_n)$ существует НОУ σ, т.е. $P(t_1\sigma, \ldots, t_i\sigma, \ldots, t_n\sigma) \equiv P(v_1\sigma, \ldots, (v_i(0))\sigma, \ldots, v_n\sigma)$ выводятся дизъюнкты:

$$P(v_1\sigma, \ldots, (v_i(g(t, z_1, \ldots, z_s)))\sigma, \ldots, v_n\sigma) \vee C_{1\sigma} \vee C_{2\sigma}$$

$$\neg P(v_1\sigma, \ldots, (v_i(Sg(t, z_1, \ldots, z_s)))\sigma, \ldots, v_n\sigma) \vee C_{1\sigma} \vee C_{2\sigma}$$

где $z_2, \ldots, z_s$ все переменные в литере $P(v_1, \ldots, v_i(0), \ldots, v_n)$, g — функция Сколема $(s+1)$ аргументов. Когда $P(v_1, \ldots, v_i(0), \ldots, v_n)$ не содержит переменных, получается частный случай:

$$D_1, D_2 \vdash P(v_1\sigma, \ldots, (v_i(g(t)))\sigma, \ldots, v_n\sigma) \vee C_{1\sigma} \vee C_{2\sigma}, \urcorner P(v_1\sigma, \ldots$$
$$\ldots, (v_i(Sg(t)))\sigma, \ldots, v_n\sigma) \vee C_{1\sigma} \vee C_{2\sigma}.$$

Пример. Вывод $P(x, b)$ из $P(0, b)$ и $\urcorner P(x, b) V P(Sx, b)$.

1. $P(0, b)$	
2. $\urcorner P(x, b) \vee P(Sx, b)$	
3. $\urcorner P(a, b)$	отрицание и сколемизация формулы $P(x, b)$; a — конст.
4. $P(ga, b)$	из 1 и 3 по правилу индукции для терма a; σ пустая.
5. $\urcorner P(Sga, b)$	
6. $P(Sga, b)$	из 2 и 4, резолюция
7. $\varnothing$	из 5 и 6, резолюция; $\varnothing$ — пустой дизъюнкт.

Этот вывод на четыре шага короче чем вывод полученный в [8] с применением f-техники. Преимущество относительно уменьшения общего количества порожденных дизъюнктов здесь скрыто, так как мы не рассматривали процедуры и стратегии поиска.

Приведенное правило потребует фиксации терма t в литере дизъюнкта D_2, что на практике может оказатся неудобным. Однако, этого можно избечь с помощью использования следующего обобщенного правила, которое получается на основании правила $P5$.

Правило бинарной индукции — правило Q:

Из дизъюнктов D: $P(t_1, \ldots, t_n) \vee C_1$ и D_2: $\urcorner P(v_1, \ldots, v_n) \vee C_2$ (где C_1 и C_2 дизъюнкты а $P(t_1, \ldots, t_n)$ и $\urcorner P(v_1, \ldots, v_n)$ литеры) не имеющих общих переменных и таких что: (i) существует подстановка σ, такая что

$$P(t_1\sigma, \ldots, t_n\sigma) \equiv L_x(0) \text{ и } \urcorner P(v_1\sigma, \ldots, v_n\sigma) \equiv \urcorner L_x(t),^{1)}$$

выводятся дизъюнкты

$$L_x(g(t, z_1, \ldots, z_s)) \vee C_{1\sigma} \vee C_{2\sigma} \text{ и } \urcorner L_x(Sg(t, z_1, \ldots, z_s)) \vee C_{1\sigma} \vee C_{2\sigma}$$

где g — функция Сколема $(z+1)$ аргументов и $z_1, \ldots, z_s$ все переменные в литере $L_x(0)$, t — терм.

Записываем

$$Q\ D_1, D_2 \vdash L_x(g(t, z_1, \ldots, z_s)) \vee C_\sigma \vee C_\sigma,\ \urcorner L_x(Sg(t, z_1, \ldots, z_s)) \vee C_{1\sigma} \vee C_{2\sigma}$$

(при условии (i)).

Основным препятствием для применения правила Q кажется способ отыскания требуемой подстановки σ. Однако, для этой цели, т.е. для определения дизъюнктов к которым применимо правило Q, можно использовать модифицированный алгоритм унификации. Пока что, приведем только общую

---

[1]) Очевидно что литеры $L_x(0)$ и $L_x(t)$ должны содержать предикатную букву P.

картину этой идеи. Когда алгоритм унификации закончит работу установив что множество литер неунифицируемо, тогда множество рассоглaсования, которое алгоритм порождает, не пусто. В множестве рассогласования находим терм, принадлежащий литере со знаком отрицания, и эту литеру заменяем на литеру, в которой вхождение этого терма замененно на 0. Применяем алгоритм унификации к таким образом, „поправленом" множестве литер. В случае когда это множество окажется унифицируемым, то тем самым определены и терм t и подстановка σ, потребующиеся для применения правила Q.

Подробное описание модифицированного алгоритма унификации и способ встроения правила Q в существующие процедуры автоматического доказательства теорем с резолюцией, будут рассмотренны в отдельной статье.

ЛИТЕРАТУРА

[1] Mendelson, *Introduction to Mathematical Logic*. Русский перевод: С. Мендельсон *Введение в математическую логику*, Наука, Москва, 1976.

[2] J. R. Shoenfield, *Mathematical Logic*, Addison-Wesley, 1967. Русский перевод: Дж. Шенфилд, *Математическая логика*, Наука, Москва, 1973.

[3] S. C. Kleene, *Mathematical Logic*, John Wiley & Sons, INC, 1967. Русский перевод: С. Клини, *Математическая логика*, Мир, Москва, 1973.

[4] G. Takeuti, *Proof Theory*. Русский перевод: Г. Такеути, *Теория доказательств*, Мир, Москва, 1908.

[5] Е. В. Попов, Г. Р. Фирдман, *Алгоритмические основы интеллектуальных роботов и искусстгенноio интеллекта*, Наука, Москва, 1976.

[6] J. A. Robinson, *A Machine-Oriented Logic Based on the Resolution Principle*, J. ACM, 12 (1965), 23—41. Русский перевод: Кибернетический сборник, 7, Новая серия, Мир, Москва, 1970.

[7] G. Robinson, L. Wos, *Paramodulation and Theorem-Proving in First Order Theories with Equality*, Machine Intelligence, 4, Dale E. and Michie D. (eds.) Oliver & Boyd, Edinburgh, 1969, pp. 135—150.

[8] J. L. Darlington, *Automatic Theorem Proving with Equality Substitutionsy and Mathematical Induction*, Machine Intelligence, 3, Michie D. (ed.), Edinburgh University Press, Edinburgh, 1968, pp. 113—127.

Педагошка академија
22000 Сремска Митровица
Југославија