В. И. Шалак, ИФ РАН

АНАЛИТИЧЕСКИЕ ТАБЛИЦЫ ДЛЯ ПОИСКА ГИПОТЕЗ

Центральным понятием логики является понятие вывода, а одной из важных задач является *поиск вывода* формулы *A* из множества гипотез *Γ*, что можно условно обозначить как ***Γ*<…?...>*A***. Именно к такому виду и сводят обычно решение задач. В то же время на практике решение задач часто имеет вид не поиска вывода из гипотез, а поиск для целевого высказывания *A* набора гипотез *Γ*, из которых оно выводимо, что можно обозначить как ***? <…> A***. Назовем это *поиском гипотез* для *A*.

В качестве иллюстрации вспомним историю с доказательством теоремы Ферма, то ее решение заключалось не в прямой дедукции из аксиом, а в анализе того, что утверждается в теореме, и сведении его к правдоподобной гипотезе о свойствах эллиптических кривых над рациональными числами, а уже затем эта гипотеза была сведена к ранее доказанным теоремам. В результате даже не понятно, кому конкретно принадлежит заслуга доказательства теоремы Ферма.

В связи с поиском гипотез естественно прибегнуть к методу аналитических таблиц, основанный на анализе логической структуры доказываемого высказывания. Однако в существующем виде этот метод рассчитан лишь на те случаи, когда анализируемое высказывание является теоремой логики, т.е. множество посылок *Γ* пусто или дано изначально, нас же интересует нахождение посылок *Γ*.

Реконструируя процесс поиска гипотез для некоторого высказывания *A*, мы должны обратить внимание на логическую структуру *A*, что позволит свести основную задачу к подзадачам. Для этого вполне подходят правила редукции, используемые при построения аналитических таблиц [1], [2].

Если все возможные правила логической редукции исчерпаны, но таблица не замкнута, остается лишь принять некоторое дополнительное высказывание *B*, которое может иметь отношение к решаемой задаче и в будущем войти в искомое множество *Γ*. Очевидно, что выбор конкретного *B* чем-то должен быть мотивирован. В порядке убывания приоритета, мотивом для принятия *B* может быть отнесение его к одному из следующих шести видов.

I. *B – явное определение* одного из предикатных или функциональных символов.
II. *B – неявное определение* одного из предикатных или функциональных символов.
III. *B – ранее доказанная теорема*.
IV. *B – эмпирически истинное высказывание*.
V. *B – описание результата некоторого действия*.
VI. *B – правдоподобная гипотеза*.

Локальные правила редукции

В качестве локальных возьмем правила редукции для исчисления предикатов первого порядка с равенством из [1], [2].

Глобальные правила редукции

$$(P)\quad \frac{A[P^n]}{B[P^n]} \qquad (DP)\quad \frac{A[P^n]}{\forall x_1..\forall x_n(P^n(x_1,\dots,x_n)\equiv D)} \qquad FV(D)\subseteq\{x_1,\dots,x_n\}$$

$$(f)\quad \frac{A[f^n]}{B[f^n]} \qquad (Df)\quad \frac{A[f^n]}{\forall x_1..\forall x_n(f^n(x_1,\dots,x_n)=u)} \qquad FV(u)\subseteq\{x_1,\dots,x_n\}$$

Ограничения на применение глобальных правил редукции

1. В правилах *(P), (f), (DP)* и *(Df)* формула под чертой не должна содержать индивидных констант, введенных ранее локальными правилами *(∃)* или *(¬∀)*.

2. В правиле *(DP)* формула D не содержит вхождений предикатного символа P^n, а в правиле *(Df)* терм u не содержит вхождений функционального символа f^n.

Понятие доказательства

Пусть U – некоторое множество замкнутых формул.

Конфигурацией будем называть семейство множеств формул $\{U_1, U_2, \ldots, U_n\}$.

Результатом применения к конфигурации $\{U_1, \ldots, U_n\}$ *локального правила редукции* R будем называть замену данной конфигурации на новую, отличающуюся от исходной лишь тем, что вместо одного из множеств U_i она содержит результат применения к нему правила R.

Если хотя бы одно из множеств формул конфигурации $\{U_1, \ldots, U_n\}$ содержит формулу над чертой глобального правила редукции $R \in \{(P), (f), (DP), (Df)\}$, то *результатом применения к конфигурации* $\{U_1, \ldots, U_n\}$ *данного правила* R будет новая конфигурация $\{U'_1, \ldots, U'_n\}$, в которой каждое множество U'_i получено из U_i путем ***добавления*** к нему формулы под чертой правила R. Т.е. глобальные правила редукции изменяют все множества формул данной конфигурации.

Таблицей будем называть конечную последовательность конфигураций $<C_1,..,C_n>$, в которой каждая конфигурация, кроме первой, получена из предшествующей конфигураций в результате применения локального или дефинициального правила редукции.

Множество формул U *замкнуто*, если оно содержат некоторую формулу A и ее отрицание $\neg A$.

Конфигурация $\{U_1, \ldots, U_n\}$ *замкнута*, если замкнуто каждое множество U_i.

Таблица $<C_1,..,C_n>$ *замкнута*, если замкнута одна из ее конфигураций C_i.

Доказательством для замкнутой формулы A будем называть замкнутую таблицу $<C_1,..,C_n>$ с начальной конфигурацией $C_1=\{\{\neg A\}\}$.

Будем говорить, что *для множества формул* S *существует замкнутая таблица относительно множества гипотез* Hyp, если существует замкнутая таблица $<C_1,..,C_n>$ с начальной конфигурацией $C_1=\{S\}$, и Hyp состоит из всех формул, добавленных при построении данной таблицы применением правил *(P)*, *(f)*, *(DP)* и *(Df)*.

Свойства построенного исчисления

Теорема 1. (Об элиминации глобальных правил редукции) Если существует замкнутая таблица для множества формул S относительно множества гипотез $Hyp=\{B_1, \ldots, B_m\}$, где $m \geq 0$, то существует замкнутая таблица для множества формул $S \cup Hyp$ без применения глобальных правил редукции.

Теорема 2. (Об элиминации явных определений) Если доказуема формула $(D_1 \& \ldots \& D_k \supset A)$, где D_i имеет вид, либо $\forall x_1.. \forall x_n(P_i(x_1, \ldots, x_n) \equiv B_i)$, либо $\forall x_1.. \forall x_n(f_i(x_1, \ldots, x_n) = u_i)$, где формула B_i не имеет вхождений предикатного символа P_i, а терм u_i не имеет вхождений функционального символа f_i, то доказуема формула A^*, полученная из формулы A путем подстановок $B_i(t_1/x_1, \ldots, t_n/x_n)$ вместо всех вхождений в нее $P_i(t_1/x_1, \ldots, t_n/x_n)$ и подстановок $u_i(t_1/x_1, \ldots, t_n/x_n)$ вместо всех вхождений $f_i(t_1/x_1, \ldots, t_n/x_n)$.

Литература

[1] Fitting M.C. *First-Order Logic and Automated Theorem Proving*. Springer-Verlag, Berlin, 1990. 242 p.

[2] Fitting M. *Intuitionistic Logic, Model Theory and Forcing*. North-Holland Publishing Company, Amsterdam, 1969. 192 p.