ЛЕКЦИЯ 11

2.7 Автоматическое доказательство теорем (АДТ)

2.7.1 Постановка задачи

В общем случае алгоритм АДТ не возможен для любых формул **G**, любого множества формул **Г** и любой теории **τ**. Хотелось бы иметь алгоритм, который проверяет отношение $\Gamma \vdash_{\tau} G$ и говорит «ДА», если верен вывод $\Gamma \vdash_{\tau} G$ или говорит «НЕТ», если вывод $\Gamma \vdash_{\tau} G$ неверен.

Для ИВ (Исчисления Высказываний) и для ПИП (Прикладных Исчислений Предикатов) с одноместным предикатом, алгоритмы АДТ известны.

Для ИВ: алгоритм “Таблиц истинности” проверяет ее на “Тавтологичность”, т.е. это алгоритм АДТ, но это не алгоритм автоматического вывода теорем из аксиом.

Метод резолюции (MR) – Алгоритм выдает ПИП 1-го порядка “ДА”,

если верно $\Gamma \vdash_{\tau} G$, и “НЕТ, отсутствие ответа”, если неверно $\Gamma \vdash_{\tau} G$.

2.7.2 Доказательство «от противного» (основа метода резолюции)

Теорема:

Если $\Gamma, \neg G \vdash F$, где F -любое противоречие (тождественно-ложная формула), то тогда $\Gamma \vdash G$

Доказательство (для теории **L или** ИВ):

Согласно прямой дедукции переносим все из левой части со знаком импликации

$\Gamma, \neg G \vdash F \Leftrightarrow \vdash \Gamma \& \neg G \to F$ - тавтология.

Применяем правило ($A \to B => \neg A \vee B$) и правила де Моргана:

$\Gamma \& \neg G \to F = \neg(\Gamma \& \neg G) \vee F = \neg(\Gamma \& \neg G) = \neg\Gamma \vee G = \Gamma \to G$ – *тавтология, т.е.* $\vdash \Gamma \to G$*. По обратной теореме дедукции получаем* $\Gamma \vdash G$*, что и требовалось доказать.*

Замечание: в формуле F=0 просто опускается, т.к. логическое прибавление нуля не меняет смысл).

Это доказывает, что метод "от противного" логичен и его можно применять, т.е. прямую теорему можно доказывать косвенным способом.

2.7.3 Сведение к предложениям (бескванторная дизъюнкция литералов)

Любая формула ИП преобразуется во множество предложений после применения следующего алгоритма:

1. Элиминации импликации
   $(A \to B => \neg A \vee B)$

2. Протаскивание отрицаний
   $\neg\forall_X(A) => \exists_X \neg(A)$

3. Разделение связанных переменных
   $Q_{1X}A(\dots Q_{2X}B(\dots X \dots)\dots) => Q_{1X}A(\dots Q_{2Y}B(\dots Y \dots)\dots)$

4. Приведение к предваренной форме
   $Q_X A \vee B => Q_X(A \vee B)$

5. Элиминация кванторов существования
   $\exists_X Q_2 x_2 A(x_1, x_2, \dots, x_n) => Q_2 x_2 A(a, x_1, x_2, \dots, x_n)$

6. Элиминация кванторов всеобщности
   $\forall_X A(x) => A(x)$

7. Приведение к конъюнктивной нормальной форме
   $A \vee (B \wedge C) \Rightarrow (A \vee B) \wedge (A \vee C)$

8. *Элиминация конъюнкции*
   "$A \wedge B$ эквивалентна записи *A,B». Т.*е распадение $\wedge$ (формулы) на множество предложений.

2.7.4 Правило резолюции для ИВ

Пусть C_1 и C_2 - два предложения ИВ и пусть

$C_1 = P \vee C'_1$

$C_2 = \neg P \vee C'_2$,

где P - пропозициональная переменная а C_1, C_2 –любые произвольные предложения.

Правило «резолюции»

$$\frac{C1, C2}{C'_1 \vee C'_2} R$$

C_1, C_2 – резольвируемые предложения (родительские).

$C'_1 \vee C'_2$- резольвента. P и $\neg P$ контрарные литералы.

Частные случаи правила «резолюции»

а) $\frac{A, A \to B}{B} MP$ или $\frac{A, \neg A \vee B}{B} R$

б) $\frac{A \to B, B \to C}{A \to C}$ Правило транзитивности, или $\frac{\neg A \vee B, \neg B \vee C}{\neg A \vee C} R$

в) $\frac{A \vee B, A \to B}{B}$ Правило слияния , или $\frac{A \vee B, \neg A \vee B}{\neg A \vee C} R$

Теорема:

Правило резолюции логично, т.е. резольвента является логическим следствием резольвируемых предложений

Доказательство теоремы:

Пусть даны следующие интерпретации I(C1)=И; I(C2)=И

(И-истина, Л-ложь).Тогда если I(P)=И, то $I(C'_2) \neq 0$ и $I(C'_2)$=И, а значит I($C'_1 V C'_2$)=И.

Если же I(P)=Л, то $I(C'_1) \neq 0$ и $I(C'_1)$=И, а значит I($C'_1 V C'_2$)=И.

2.7.5 Правило резолюции для ИП

$$\frac{C1, C2}{(C'_1 V C'_2)\delta} R$$

C_1,C_2– предложения ИП, в которых существуют унифицируемые контрарные литералы P_1 *и* $\neg P_2$,тоесть:

$C1 = P_1 V C'_1$ $C2 = \neg P_2 V C'_2$

Причем атомарные формулы P_1 *и* P_2 разные, но являются унифицируемыми наиболее общим унификатором δ. Таким образом, резольвентой предложений C_1, и C_2 является предложение $(C'_1 V C'_2)\delta$, полученное из предложения $C'_1 V C'_2$ с применением унификатора δ**.**

Литералы - это атомарные формулы и их отрицания, т.е. A и ¬A.

Унификатор δ – это набор подстановок $\{B_i \ // \ X_i\}_{i=1}^{n}$ в формулу A(x1,x2,…,xn), т.е. применение унификатора δ дает в итоге, что результаты подстановок совпадают: $(P_1)\delta$=$(P_2)\delta$.

2.7.6 Алгоритм АДТ – Опровержение методом резолюций.

Пусть нужно доказать вывод: $\Gamma \vdash G$, где Г - множество гипотез (формул), а G - конкретная формула.

Алгоритм АДТ сводится к следующему:

1) Каждая из формул множества Г и формула $\neg G$ независимо преобразуются в множество предложений**С**, согласно алгоритму сведения к предложениям.

2) В полученном совокупном множестве предложений **С** отыскивается пара резольвируемых предложений, к которым применяется правило резолюции, а резольвента добавляется во множество предложений **С** до тех пор, пока не будет получено «пустое» предложение (т.е. $(C_1' \vee C_2')\delta$=0 , имеется противоречие).

В процессе применения такого алгоритма АДТ, возможны три случая:

1) Среди текущего множества предложений **С** нет резольвируемых предложений. Тогда вывод $\Gamma, \neg G \vdash F <=> \Gamma \vdash G$ неверен т.е. формула G не выводима.

2) В результате очередного применения Пр. резолюции получено «пустое» предложение (противоречие). Тогда, согласно теореме о методе от противного, вывод $\Gamma \vdash G$ доказан.

3) Если процесс пополнения резольвентами, среди которых нет пустых предложений, не заканчивается, т.е. зацикливается. Тогда вопрос вывода $\Gamma \vdash G$ остается открытым: нельзя точно сказать, верен вывод или неверен.

Так как существует третий случай, то ИП - полуразрешимая теория, а метод резолюции - частичный алгоритм АДТ, т.е. завершаемость алгоритма не гарантируется.