Математическая логика

А.М. Миронов

Содержание

Введение

Математическая логика (называемая ниже просто **логикой**) – это наука, которая изучает, каким образом мы выражаем мысли, делаем умозаключения, и как всё это можно представить формально.

Логика является основой всех остальных наук.

Одной из важнейших областей применения методов логики являются информационно–компьютерные системы, где логика является теоретическим фундаментом для разработки

- языка общения человека с компьютером, дающего возможность человеку представлять в компьютере знания, относящиеся к его области деятельности, наиболее естественным и удобным способом,
- методов автоматического поиска ответов на вопросы, исходя из имеющихся знаний,
- автоматического порождения новых знаний.

Логика состоит из нескольких разделов. В настоящем курсе мы изучим основы следующих из них:

1. логика высказываний
2. теория множеств
3. логика предикатов
4. теорема Гёделя
5. алгебраическая логика
6. интуиционистская логика
7. модальная логика
8. логика неполных знаний
9. логика ограниченных ресурсов
10. динамическая логика
11. вероятностная и нечёткая логика

В данном курсе мы рассмотрим также некоторые приложения логики к программированию - основы **логического программирования**.

Логическое программирование связано с построением и использованием **языков программирования высокого уровня**. Программа на языке высокого уровня представляет собой описание решаемой задачи, в отличие от программ на языках низкого уровня (которыми являются, например, Паскаль или Си), на которых программист описывает, какие именно действия следует выполнить для решения его задачи.

В логической программе

- описываются понятия (объекты, функции и отношения между ними), связанные с решаемой задачей,
- формулирутся утверждения (факты и правила), выражающие связи между этими понятиями, и
- ставится **цель**, т.е. указываются вопросы, связанные с понятиями, описанными в программе.

Решение поставленной задачи имеет вид логического вывода из той совокупности знаний, которыми располагает логическая программа. Последовательность действий, необходимых для решения задачи, поставленной в логической программе, синтезируется автоматически.

Основными областями, в которых логическое программирование даёт наибольший эффект по сравнению с другими методами программирования, являются

- извлечение информации из баз данных и знаний,
- решение задач планирования деятельности,
- обработка текстов на естественном языке.

Лекция 1

Высказывания

1.1 Понятие высказывания

Одной из простейших форм логического суждения является **логическое высказывание** (называемое ниже просто **высказыванием**).

Высказывание – это повествовательное предложение, о котором в каждой конкретной ситуации можно сказать, истинно оно или ложно.

Истинность или ложность высказываний зависит от интерпретации понятий, входящих в данное высказывание:

- в одной ситуации (т.е. при одной интерпретации понятий, входящих в данное высказывание) оно может быть истинным, в то время как
- в другой ситуации (т.е. при другой интерпретации понятий, входящих в данное высказывание) оно может быть ложным.

Например, высказывание

Город Одесса находится в Америке

является

- ложным, если под Одессой имеется ввиду известный город на Украине, и
- истинным, если под Одессой имеется ввиду город в штате Дэлавэр (США).

1.2 Структура высказываний

Рассмотрим следующие примеры высказываний:

$$\text{Москва - столица России.} \tag{1.1}$$

$$\text{Париж находится в Америке.} \tag{1.2}$$

$$\text{Число 5 больше 1 и меньше 10.} \tag{1.3}$$

$$\begin{array}{l}\text{Сегодня идёт дождь или}\\ \text{сегодня солнечная погода.}\end{array} \tag{1.4}$$

$$\begin{array}{l}\text{Если вода в кастрюле кипит, то температура}\\ \text{воды в кастрюле - 100 градусов по Цельсию.}\end{array} \tag{1.5}$$

$$\begin{array}{l}\text{Паша находится на улице тогда и только}\\ \text{тогда, когда он не находится дома.}\end{array} \tag{1.6}$$

Проанализируем структуру данных высказываний.

- Высказывания (1.1) и (1.2) можно считать **элементарными**, или **атомарными**, в том смысле, что они не представимы в виде комбинации более простых высказываний.
- Высказывание (1.3) можно представить в виде комбинации двух более простых высказываний:

$$\text{Число 5 больше 1.} \tag{1.7}$$

$$\text{Число 5 меньше 10.} \tag{1.8}$$

Если обозначить высказывание (1.7) символом A, а высказывание (1.8) символом B, то высказывание (1.3) можно представить в виде комбинации

$$A \text{ и } B.$$

- Высказывание (1.4) можно представить в виде комбинации двух более простых высказываний:

$$\text{Сегодня идёт дождь.} \tag{1.9}$$

$$\text{Сегодня солнечная погода.} \tag{1.10}$$

Если обозначить высказывание (1.9) символом A, а высказывание (1.10) символом B, то высказывание (1.4) можно представить в виде комбинации

$$A \text{ или } B.$$

- Высказывание (1.5) можно представить в виде комбинации двух более простых высказываний:

$$\text{Вода в кастрюле кипит.} \tag{1.11}$$

$$\begin{array}{l}\text{Температура воды в кастрюле -}\\ \text{100 градусов по Цельсию.}\end{array} \tag{1.12}$$

Если обозначить высказывание (1.11) символом A, а высказывание (1.12) символом B, то высказывание (1.5) можно представить в виде комбинации

$$\text{если } A, \text{ то } B.$$

- Высказывание (1.6) можно представить в виде комбинации двух более простых высказываний:

$$\text{Паша находится на улице.} \qquad (1.13)$$

$$\text{Паша находится дома.} \qquad (1.14)$$

Если обозначить высказывание (1.13) символом A, а высказывание (1.14) символом B, то высказывание (1.6) можно представить в виде комбинации

$$A \text{ равносильно (не } B).$$

Данные примеры наводят на мысль, что все высказывания можно разделить на два класса -

1. **простые** (или **атомарные**) высказывания, и
2. **составные** высказывания, которые являются комбинациями атомарных высказываний.

1.3 Атомарные высказывания

Атомарное высказывание – это высказывание, которое мы рассматриваем как не представимое в виде комбинации более простых высказываний.

При формальном анализе высказываний каждое атомарное высказывание будет обозначаться некоторым символом, который называется **булевой переменной**. Как правило, это - строчная буква латинского алфавита (возможно, с индексом внизу). Булевы переменные, обозначающие атомарные высказывания, должны быть выбраны так, чтобы разным атомарным высказываниям соответствовали разные булевы переменные.

1.4 Составные высказывания

Из высказываний путём соединения их различными способами можно составлять новые, более сложные высказывания.

Истинность или ложность новых высказываний будет определяться истинностью или ложностью составляющих их высказываний.

Если высказывание A является истинным, то мы будем говорить, что оно имеет значение 1, а если ложным, то будем говорить, что оно имеет значение 0.

1.4.1 Отрицание

Для каждого высказывания A знакосочетание $\neg A$ обозначает высказывание, которое называется **отрицанием** высказывания A, и читается "не A" или "неверно, что A".

Значение высказывания $\neg A$ определяется следующей таблицей:

A	$\neg A$
0	1
1	0

(1.15)

т.е.

- если высказывание A ложно, то высказывание $\neg A$ истинно, и
- если высказывание A истинно, то высказывание $\neg A$ ложно.

1.4.2 Конъюнкция

Если A и B – высказывания, то знакосочетание $A \wedge B$ обозначает высказывание, которое называется **конъюнкцией** высказываний A и B, и читается "A и B".

Значение высказывания $A \wedge B$ определяется следующей таблицей:

A	B	$A \wedge B$
0	0	0
0	1	0
1	0	0
1	1	1

(1.16)

т.е.

- если хотя бы одно из высказываний A и B ложно, то высказывание $A \wedge B$ ложно, и
- если оба высказывания A и B истинны, то высказывание $A \wedge B$ истинно.

1.4.3 Дизъюнкция

Если A и B – высказывания, то знакосочетание $A \vee B$ обозначает высказывание, которое называется **дизъюнкцией** высказываний A и B, и читается "A или B".

Значение высказывания $A \vee B$ определяется следующей таблицей:

A	B	$A \vee B$
0	0	0
0	1	1
1	0	1
1	1	1

(1.17)

т.е.

- если оба высказывания A и B ложны, то высказывание $A \vee B$ ложно, и
- если хотя бы одно из высказываний A и B истинно, то высказывание $A \vee B$ истинно.

Отметим, что иногда в разговорных языках слово "или" в высказывании "A или B" употребляется в "исключающем" смысле, т.е. высказывание "A или B" считается истинным в том и только в том случае, когда истинно одно и только одно из высказываний: или A, или B.

Если интерпретировать связку “или” в исключающем смысле, то тогда значение высказывания $A \vee B$ будет определяться следующей таблицей:

A	B	$A \vee B$
0	0	0
0	1	1
1	0	1
1	1	0

Ниже мы будем рассматривать употребление связки “или” только в первом (в “неисключающем”) смысле.

1.4.4 Импликация

Если A и B – высказывания, то знакосочетание $A \to B$ обозначает высказывание, которое называется **импликацией** высказываний A и B, и читается “из A следует B”, или “если истинно A, то истинно B”.

Высказывание A называется **посылкой** имликации $A \to B$, а высказывание B называется **заключением** имликации $A \to B$.

Значение высказывания $A \to B$ определяется следующей таблицей:

A	B	$A \to B$
0	0	1
0	1	1
1	0	0
1	1	1

(1.18)

т.е. импликация ложна в том и только в том случае, когда её посылка истинна, а её заключение - ложно. Во всех остальных случаях, т.е. когда

- посылка импликации ложна, или
- заключение импликации истинно

импликация по определению является истинной.

Например, высказывание

$$\text{если } (2 \cdot 2 = 5) \text{ то (Рим – столица Бразилии)} \quad (1.19)$$

следует считать истинным, т.к. посылка $(2 \cdot 2 = 5)$ является ложным высказыванием.

Заметим, что, согласно общепринятому пониманию смысла высказываний типа “если - то”, нет никаких причин считать высказывание (1.19) истинным, т.к. оно абсурдно – в нём нет никакой связи между посылкой и заключением.

Тем не менее, мы считаем высказывание (1.19) истинным, поскольку, согласно нашему определению, значение импликации “если A, то B” определяется не наличием причинно-следственной связи между A и B, а только лишь значениями A и B.

Некоторым обоснованием определения (1.18) может служить следующий довод. Рассмотрим высказывание

$$\begin{array}{l}\text{если натуральное число } x \text{ делится на 4,}\\ \text{то число } x \text{ является чётным.}\end{array} \quad (1.20)$$

Согласно здравому смыслу, высказывание (1.20) следует считать истинным независимо от значения x. В частности,

- если $x = 5$, то посылка и заключение будут иметь значение 0,
- если $x = 6$, то посылка будет иметь значение 0, а заключение – значение 1,

а всё высказывание (1.20), согласно сказанному выше, должно в обеих ситуациях иметь значение 1.

1.4.5 Эквиваленция

Если A и B – высказывания, то знакосочетание $A \leftrightarrow B$ обозначает высказывание, которое называется **эквиваленцией** высказываний A и B, и читается “A равносильно B”.

Значение высказывания $A \leftrightarrow B$ определяется следующей таблицей:

A	B	$A \leftrightarrow B$
0	0	1
0	1	0
1	0	0
1	1	1

(1.21)

т.е. высказывание $A \leftrightarrow B$ истинно тогда и только тогда, когда A и B имеют одно и то же значение.

1.5 Задачи

1. Записать следующие высказывания с использованием булевых переменных и связок:
   (a) Если г-н Иванов счастлив, то г-жа Иванова несчастлива, и если г-н Иванов несчастлив, то г-жа Иванова счастлива.
   (b) Или Петя пойдёт на дискотеку, и Саша не пойдёт на неё; или Петя не пойдёт на дискотеку, и Саша отлично проведёт время.
   (c) Необходимое и достаточное условие счастья для дедушки состоит в том, чтобы иметь хорошее вино и слушать классическую музыку.
   (d) Если студент ложится поздно спать и пьёт на ночь кофе, то утром он встаёт в дурном расположении духа или с головной болью.
   (e) Таня смотрит фильм только в том случае, когда этот фильм - комедия.
   (f) Для того, чтобы целое число x было нечётным, достаточно, чтобы x было простым.
   (g) “Красные” выиграют приз, если “Жёлтые ” его не выиграют.

Лекция 2

Формулы логики высказываний

2.1 Синтаксис формул логики высказываний

2.1.1 Знакосочетания

Знакосочетанием называется произвольная символьная строка, которая может быть пустой. Пустая строка обозначается символом ε.

Конкатенацией знакосочетаний u и v называется знакосочетание, обозначаемое символом $u \cdot v$, и получаемое приписыванием v справа к u, т.е. если $u = a_1 \dots a_n$ и $v = b_1 \dots b_m$, то $u \cdot v = a_1 \dots a_n b_1 \dots b_m$. По определению, $\varepsilon \cdot u = u \cdot \varepsilon = u$.

2.1.2 Понятие формулы логики высказываний

Формула логики высказываний (называемая ниже **формулой ЛВ**, а в данной главе – просто **формулой**) – это знакосочетание, которое

- является булевой переменной, или
- совпадает с одним из знакосочетаний из списка
  $$(\neg A),\ (A \wedge B),\ (A \vee B),\ (A \to B),\ (A \leftrightarrow B) \qquad (2.1)$$
  где A и B – формулы.

Символы $\neg, \wedge, \vee, \to, \leftrightarrow$ называются **связками**.

Для каждой формулы A совокупность всех булевых переменных, входящих в A, обозначается знакосочетанием $Var(A)$.

2.1.3 Представление формул деревьями

Каждую формулу A можно представить в виде дерева, обозначаемого символом $tree(A)$, и называемого **деревом синтаксического разбора** формулы A. В данном параграфе под деревом мы понимаем

- совокупность **вершин**, где каждая вершина изображается кружочком, внутри которого нарисована булева переменная или связка, называемая **меткой** этой вершины, и
- совокупность **рёбер**, где каждое ребро представляет собой стрелочку, соединяющую некоторую пару вершин.

причём одна из вершин дерева является выделенной: она называется **корнем** этого дерева, и удовлетворяет следующему условию: для каждой вершины N дерева существует единственная последовательность рёбер, ведущая из корня в вершину N.

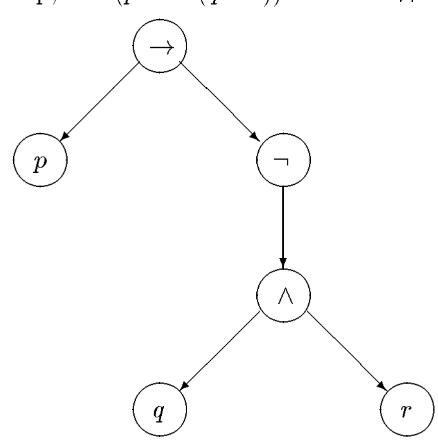
Дерево $tree(A)$ определяется следующим образом.

1. Если A является булевой переменной, то $tree(A)$ состоит из единственной вершины с меткой A, и не имеет рёбер. Корнем дерева $tree(A)$ в данном случае является эта единственная вершина.

2. Если A имеет вид $\neg B$, то $tree(A)$ получается добавлением к дереву $tree(B)$ новой вершины с меткой $\neg$, и нового ребра из этой вершины в корень дерева $tree(B)$. Корнем дерева $tree(A)$ является новая вершина.

3. Если A совпадает с одним из высказываний вида
   $$B \wedge C, \quad B \vee C, \quad B \to C, \quad B \leftrightarrow C$$
   то $tree(A)$ получается путём добавления к деревьям $tree(B)$ и $tree(C)$ новой вершины с меткой $\wedge$, $\vee$, $\to$, или $\leftrightarrow$ соответственно, и пары новых рёбер из этой вершины в корни деревьев $tree(B)$ и $tree(C)$. Корнем дерева $tree(A)$ является новая вершина.

Например, $tree(p \to \neg(q \wedge r))$ имеет вид



2.1.4 Соглашения об экономном использовании скобок

Для облегчения чтения сложных формул используются следующие соглашения:

1. В формуле можно опустить внешнюю пару скобок.

2. Связки $\neg, \wedge, \vee, \to, \leftrightarrow$ упорядочены по силе связывания в той же последовательности, в которой они выписаны (т.е. $\neg$ связывает сильнее всего, и далее - по убыванию).

   Это означает, что можно опускать в формуле все те пары скобок, без которых возможно восстановление этой формулы на основе следующего правила.

   - Просматриваются все вхождения связки $\neg$ в последовательности “слева направо”.

     Для каждого вхождения связки $\neg$ определяется наименьшее знакосочетание справа от этого вхождения, которое является формулой.

     Это знакосочетание заключается в скобки.

   - Затем просматриваются все вхождения связки $\wedge$ в последовательности “слева направо”.

     Для каждого вхождения связки $\wedge$ определяется наименьшая пара знакосочетаний, окружающих данное вхождение слева и справа, которые являются формулами.

     Данная пара знакосочетаний заключается в скобки.

   - Затем выполняются аналогичные действия для связок $\vee, \to$ и $\leftrightarrow$.

Например, в знакосочетании

$$A \vee \neg B \to C \wedge A$$

скобки восстанавливаются следующими шагами:

$$\begin{array}{l} A \vee (\neg B) \to C \wedge A \\ A \vee (\neg B) \to (C \wedge A) \\ (A \vee (\neg B)) \to (C \wedge A) \\ ((A \vee (\neg B)) \to (C \wedge A)) \end{array}$$

Отметим, что не всякая формула может быть записана без употребления скобок. Например, невозможно опустить скобки в формулах

$$A \to (B \to C) \quad \text{и} \quad A \wedge (B \vee C)$$

2.1.5 Главные связки в формулах

Если формула A содержит хотя бы одну связку, то одна из связок, входящих в данную формулу, называется **главной**:

- если A имеет вид $\neg B$, то главной является связка $\neg$ перед формулой B,

- если A совпадает с одним из знакосочетаний вида

  $$B \wedge C, \quad B \vee C, \quad B \to C, \quad B \leftrightarrow C$$

  то главной является соответствующая связка между B и C.

Другими словами, главной связкой формулы называется та входящая в неё связка, которая при построении этой формулы применяется последней.

Отметим, что под главной связкой в формуле A понимается не только символ, являющийся данной связкой, но и позиция этого символа в формуле A.

2.1.6 Подформулы

Пусть задана пара формул A, B.

B называется **подформулой** формулы A, если A можно представить в виде конкатенации $C \cdot B \cdot D$.

Например, если A имеет вид

$$\neg(p \wedge \neg q) \to r$$

то её подформулами являются следующие формулы:

$$\begin{array}{l} p \\ q \\ r \\ \neg q \\ p \wedge \neg q \\ \neg(p \wedge \neg q) \\ \neg(p \wedge \neg q) \to r \end{array}$$

Совокупность всех подформул формулы A обозначается символом $\langle A \rangle$.

Нетрудно доказать, что

1. (a) если A является булевой переменной, то $\langle A \rangle$ состоит из одной формулы A,

   (b) если A имеет вид $\neg B$, то $\langle A \rangle$ состоит из формулы A, и всех подформул формулы B,

   (c) если A совпадает с одним из знакосочетаний из списка

   $$B \wedge C, \quad B \vee C, \quad B \to C, \quad B \leftrightarrow C$$

   то совокупность $\langle A \rangle$ состоит из формулы A, всех подформул B, и всех подформул C

2. каждой связке в формуле A соответствует некоторая подформула формулы A (в которой данная связка является главной).

3. существует взаимно однозначное соответствие между подформулами формулы A и вершинами дерева $tree(A)$.

2.1.7 Обозначения

Для каждой формулы A формула $\neg A$ может также записываться в виде $\overline{A}$.

Для произвольного списка $A_1, \ldots, A_k$ формул знакосочетания

$$A_1 \wedge A_2 \wedge \ldots \wedge A_k \;\text{ и }\; A_1 \vee A_2 \vee \ldots \vee A_k$$

являются сокращённой записью формул

$$A_1 \wedge (A_2 \wedge (\ldots \wedge A_k)\ldots) \;\text{ и }\; A_1 \vee (A_2 \vee (\ldots \vee A_k)\ldots)$$

соответственно. Данные формулы также могут обозначаться соответственно знакосочетаниями

$$\left\{ \begin{array}{c} A_1 \\ \ldots \\ A_k \end{array} \right\} \quad \text{и} \quad \left[\begin{array}{c} A_1 \\ \ldots \\ A_k \end{array} \right]$$

2.2 Значения формул

2.2.1 Значение формулы при оценке переменных

Пусть X – некоторая совокупность булевых переменных.

Оценка переменных из X – это соответствие ξ, которое сопоставляет каждой переменной p из X значение $\xi(p)$, равное 0 или 1.

Нетрудно доказать, что если X состоит из n булевых переменных, то тогда возможны 2^n оценок переменных из X.

Для

- каждой формулы A,
- каждой совокупности X булевых переменных, содержащей все переменные из $Var(A)$, и
- каждой оценки ξ переменных из X

знакосочетание $\xi(A)$ обозначает значение A при оценке ξ, равное 0 или 1, которое вычисляется так же, как вычисляются значения составных высказываний в пункте 1.4, т.е. для этого вычисляются значения всех подформул из $\langle A\rangle$:

- значения переменных из $Var(A)$ определяются оценкой ξ,
- если для подформулы из $\langle A\rangle$ вида $B \wedge C$ значения $\xi(B)$ и $\xi(C)$ уже вычислены, то значение $\xi(B\wedge C)$ вычисляется по таблице (1.16)
- и т.д.

Определение значения сложных формул можно сформулировать более компактно с использованием следующих обозначений.

Пусть a, b – пара чисел, равных 0 или 1. Будем считать, что знакосочетания

$$\overline{a}, \quad a \wedge b, \quad a \vee b, \quad a \to b, \quad a \leftrightarrow b$$

обозначают числа, определяемые в соответствии с таблицами (1.15), (1.16), (1.17), (1.18), (1.21), т.е.

$$\overline{0} = 1, \quad \overline{1} = 0$$
$$0 \wedge 0 = 0 \wedge 1 = 1 \wedge 0 = 0, \quad 1 \wedge 1 = 1$$
и т.д.

Тогда значение сложных формул определяется следующим образом:

$$\begin{array}{lcl} \xi(\,\overline{B}\,) & = & \overline{\xi(B)} \\ \xi(B \wedge C) & = & \xi(B) \;\wedge\; \xi(C) \\ \xi(B \vee C) & = & \xi(B) \;\vee\; \xi(C) \\ \xi(B \to C) & = & \xi(B) \to\; \xi(C) \\ \xi(B \leftrightarrow C) & = & \xi(B) \;\leftrightarrow\; \xi(C) \end{array} \tag{2.2}$$

2.2.2 Таблицы значений для формул

Пусть A – некоторая формула.

Таблица значений для A – это таблица,

1. строки которой (начиная со второй) соответствуют оценкам переменных из $Var(A)$, и
2. столбцы которой соответствуют подформулам A,

причём для

- каждой оценки ξ переменных из $Var(A)$, и
- каждой подформулы B формулы A

на пересечении строки, соответствующей оценке ξ, и столбца, соответствующего B, стоит значение $\xi(B)$.

Так как существует 2^n всевозможных оценок переменных из $Var(A)$, где n – число этих переменных, то данная таблица содержит $2^n + 1$ строк (в первой строке записываются подформулы A).

Результирующим столбцом данной таблицы называется тот столбец, который соответствует всей формуле A.

Например, формуле $(\overline{p} \vee q) \to r$ соответствует следующая таблица значений:

p	q	r	$\overline{p}$	$\overline{p} \vee q$	$(\overline{p} \vee q) \to r$
0	0	0	1	1	0
0	0	1	1	1	1
0	1	0	1	1	0
0	1	1	1	1	1
1	0	0	0	0	1
1	0	1	0	0	1
1	1	0	0	1	0
1	1	1	0	1	1

2.3 Подстановки в формулы

Подстановкой называется знакосочетание θ вида

$$\theta \;=\; [p_1 := B_1, \ldots, p_k := B_k] \tag{2.3}$$

где $p_1, \ldots, p_k$ – список различных булевых переменных, и $B_1, \ldots, B_k$ – список формул.

Подстановка (2.3) действует на каждую формулу A путём замены для каждого $i \in \{1, \ldots, k\}$ каждого вхождения переменной p_i в A на формулу B_i. Формула, которая получается после такой замены, обозначается знакосочетанием $\theta(A)$.

Утверждение.

Пусть заданы

- формула A,
- подстановка θ вида (2.3),
- совокупность X булевых переменных, содержащая все переменные, входящие в A и θ, и
- оценка ξ переменных из X.

Обозначим символом $\xi\theta$ оценку переменных из X, определяемую следующим образом: для каждой переменной p из X $\quad (\xi\theta)(p) \stackrel{\text{def}}{=} \xi(\theta(p))$.

Тогда имеет место равенство

$$(\xi\theta)(A) \;=\; \xi(\theta(A)). \tag{2.4}$$

Доказательство.

Докажем, что для каждой формулы A' из $\langle A \rangle$ имеет место равенство

$$(\xi\theta)(A') \;=\; \xi(\theta(A')). \tag{2.5}$$

Отсюда будет следовать (2.4), т.к. A входит в $\langle A \rangle$.

Если A' – булева переменная, то (2.5) верно по определению оценки $\xi\theta$.

Предположим, что для всех подформул, длина которых меньше, чем длина A', это утверждение является верным.

Если A' имеет вид $B \wedge C$, то, поскольку длина B и C меньше, чем длина A', то, по предположению,

$$\begin{array}{l} (\xi\theta)(B) = \xi(\theta(B)) \\ (\xi\theta)(C) = \xi(\theta(C)) \end{array} \tag{2.6}$$

Нам нужно доказать соотношение

$$(\xi\theta)(B \wedge C) \;=\; \xi(\theta(B \wedge C))$$

которое, согласно (2.2) и равенству

$$\theta(B \wedge C) = \theta(B) \wedge \theta(C)$$

эквивалентно соотношению

$$(\xi\theta)(B) \wedge (\xi\theta)(C) \;=\; \xi(\theta(B)) \wedge \xi(\theta(C)) \tag{2.7}$$

Истинность (2.7) следует из (2.6).

Другие случаи возможной структуры A' разбираются аналогично. ■

2.4 Тавтологии и выполнимые формулы

Формула A называется

- **тавтологией**, если она имеет значение 1 при всех оценках переменных из $Var(A)$,
- **выполнимой** формулой, если она имеет значение 1 хотя бы при одной оценке переменных из $Var(A)$.

Примеры тавтологий: $p \vee \overline{p}$, $\overline{p \wedge \overline{p}}$, $p \leftrightarrow \overline{\overline{p}}$.

Один из возможных способов проверки того, является ли A тавтологией (или выполнимой формулой), заключается в построении её таблицы значений:

- A – тавтология, если все значения в результирующем столбце равны 1, и
- A – выполнима, если существует элемент результирующего столбца, равный 1.

Если A – тавтология, то для любой подстановки θ формула $\theta(A)$ – тоже тавтология, потому что для каждой оценки ξ переменных, входящих в A и θ, имеет место равенство (2.4), и поскольку левая часть в нём по предположению равна 1, то и правая тоже равна 1.

2.5 Эквивалентность формул

Пусть A_1, A_2 – пара формул, и X – некоторая совокупность переменных, содержащая все переменные из $Var(A_1)$ и $Var(A_2)$.

Формулы A_1 и A_2 называются **эквивалентными**, если их значения совпадают при каждой оценке переменных из X.

Знакосочетание $A_1 \sim A_2$ выражает тот факт, что A_1 и A_2 эквивалентны.

Нетрудно доказать, что $\sim$ является **конгруэнцией**, т.е. если $A_1 \sim A_2$, то

- $\overline{A_1} \sim \overline{A_2}$
- $A_1 \wedge B \sim A_2 \wedge B, \quad B \wedge A_1 \sim B \wedge A_2$
- $A_1 \vee B \sim A_2 \vee B, \quad B \vee A_1 \sim B \vee A_2$
- $A_1 \to B \sim A_2 \to B, \quad B \to A_1 \sim B \to A_2$
- $A_1 \leftrightarrow B \sim A_2 \leftrightarrow B, \quad B \leftrightarrow A_1 \sim B \leftrightarrow A_2$

Эти соотношения позволяют доказать **теорему об эквивалентной замене**, которая утверждает, что если

- формула A содержит некоторую подформулу B,
- B эквивалентна некоторой формуле C, и
- формула A' получается из A заменой B на C

то A эквивалентна A'.

Действительно, A и A' можно рассматривать как результат нескольких приписываний слева или справа к B и C одних и тех же знакосочетаний (каждое из которых является либо знаком отрицания, либо формулой со связкой). Согласно приведённым выше соотношениям, каждое приписывание сохраняет отношение эквивалентности между получающимися формулами.

Очевидно, что все тавтологии эквивалентны, и, следовательно, в любой формуле можно заменять любую подформулу, являющуюся тавтологией, на любую другую тавтологию.

Все невыполнимые формулы тоже эквивалентны, и, следовательно, в любой формуле можно заменять любую подформулу, являющуюся невыполнимой, на любую другую невыполнимую формулу.

Тавтологию иногда обозначают символом **1**, а невыполнимую формулу – символом **0**.

Эквивалентные формулы иногда называют **равными**, т.е. если $A \sim B$, то говорят, что A **равна** B, и вместо $A \sim B$ иногда пишут $A = B$.

2.6 Задачи

2.6.1 Синтаксис формул ЛВ

1. Восстановить скобки в знакосочетаниях
   - $s \leftrightarrow r \leftrightarrow p \wedge s \wedge q \vee \overline{s} \to q$
   - $r \to \overline{p \vee r} \wedge p \leftrightarrow q$
   - $r \to p \to p \leftrightarrow \overline{p} \vee q$
2. Исключить как можно больше скобок в формулах
   - $((q \leftrightarrow (\overline{r} \vee (s \wedge p))) \leftrightarrow (q \to q))$
   - $(((p \wedge \overline{q}) \wedge r) \vee s)$
3. Построить алгоритм нахождения главной связки в формуле, основанный на понятии скобочного баланса (скобочным балансом в знакосочетании называется разность между количеством открывающихся скобок и количеством закрывающихся скобок в этом знакосочетании). Указание: сначала следует восстановить все опущенные скобки.
4. Доказать утверждение в конце пункта 2.1.6.
5. Выписать все подформулы формул
   (a) $((p \to q) \wedge (r \to s)) \to (\overline{q} \vee s)$
   (b) $(p \to q) \to ((p \to \overline{q}) \to \overline{q})$
6. Доказать, что для каждой формулы A и каждой подстановки θ $\theta(A)$ тоже является формулой.
7. Пусть θ_1 и θ_2 – подстановки вида
$$\theta_1 = [p_1 := B_1, \ldots, p_k := B_k]$$
$$\theta_2 = [q_1 := C_1, \ldots, q_l := C_l]$$
   Найти подстановку θ, такую, что для каждой формулы A имеет место равенство $\theta(A) = \theta_1(\theta_2(A))$.

2.6.2 Значения формул

1. Построить таблицы значений для формул
   (a) $(p \to q) \vee \overline{p}$
   (b) $(p \to (q \to r)) \to ((p \to q) \to (q \to r))$
   (c) $(p \to q) \wedge p$
   (d) $(p \vee \overline{r}) \leftrightarrow q$
   (e) $(p \to q) \vee (p \to (q \wedge p))$
   (f) $(\overline{p \to \overline{q \wedge p}}) \to (p \vee r)$
   (g) $(p \wedge (q \to p)) \to \overline{p}$
   (h) $((p \wedge \overline{q}) \to q) \to (p \to q)$
   (i) $(p \to (q \to r)) \to ((p \to q) \to (p \to r))$
   (j) $(p \wedge (q \vee \overline{p})) \wedge ((\overline{q} \to p) \vee q)$
   (k) $((p \to (q \wedge r)) \to (\overline{q} \to \overline{p})) \to \overline{q}$
   (l) $(p \vee q \vee r) \to ((p \vee q) \wedge (p \vee r))$
   (m) $\Big((p \vee q) \wedge (q \vee r) \wedge (r \vee p)\Big) \to (p \wedge q \wedge r)$
   (n) $(p \vee q) \to ((\overline{p} \wedge q) \vee (p \wedge \overline{q}))$

2.6.3 Тавтологии и выполнимые формулы

1. Доказать, что
   (a) A – тавтология тогда и только тогда, когда $\overline{A}$ невыполнима
   (b) A – выполнима тогда и только тогда, когда $\overline{A}$ – не тавтология
   (c) $A \wedge B$ тавтология тогда и только тогда, когда A тавтология и B тавтология
   (d) $A \vee B$ выполнима тогда и только тогда, когда A выполнима или B выполнима
   (e) если A – тавтология и $A \to B$ – тавтология, то B – тавтология
   (f) если $A \vee B$ и $\overline{A} \vee C$ – тавтологии, то $B \vee C$ – тоже тавтология
   (g) если $A \vee B$, $A \to C$ и $B \to D$ – тавтологии, то $C \vee D$ – тоже тавтология
2. Верно ли, что
   (a) если A – выполнима и $A \to B$ выполнима то B – тоже выполнима?
   (b) если $A \vee B$ и $\overline{A} \vee C$ выполнимы, то $B \vee C$ выполнима?
   (c) если $A \vee B$, $A \to C$ и $B \to D$ выполнимы, то $C \vee D$ выполнима?
3. Доказать выполнимость формул
   (a) $\overline{p \to \overline{p}}$

(b) $(p \to q) \to (q \to p)$

(c) $(q \to (p \wedge r)) \wedge \overline{(p \vee r) \to q}$

4. Определить без построения таблиц значений, являются ли следующие формулы тавтологиями

   (a) $(((p \to q) \to q)) \to q$

   (b) $(p \leftrightarrow q) \leftrightarrow (p \leftrightarrow (q \leftrightarrow p))$

   (c) $p \leftrightarrow (p \vee p)$

   (d) $(p \to q) \to ((q \to r) \to (r \to p))$

   (e) $((p \to q) \wedge q) \to p$

   (f) $\overline{p} \to (p \wedge q)$

   (g) $p \wedge \overline{p \vee q}$

   (h) $(p \to q) \leftrightarrow (\overline{p} \vee q)$

   (i) $(p \to q) \leftrightarrow \overline{p \wedge \overline{q}}$

5. Доказать без построения таблиц значений, что следующие формулы являются тавтологиями:

   (a) $(p \to q) \vee (q \to p)$

   (b) $(p \to q) \vee (p \to \overline{q})$

   (c) $p \to (q \to (p \wedge q))$

   (d) $(p \to q) \to ((q \to r) \to (p \to r))$

   (e) $(p \to q) \to ((r \to p) \to (r \to q))$

   (f) $(\overline{p} \to \overline{q}) \to (q \to p)$

   (g) $p \to (q \to p)$

   (h) $p \vee \overline{p}$

   (i) $\overline{p \wedge \overline{p}}$

   (j) $(p \to q) \to ((p \to (q \to r)) \to (p \to r))$

   (k) $(p \wedge q) \to p$

   (l) $(p \wedge q) \to q$

   (m) $p \to (p \vee q)$

   (n) $q \to (p \vee q)$

   (o) $(p \to r) \to ((q \to r) \to ((p \vee q) \to r))$

   (p) $(p \to q) \to ((p \to \overline{q}) \to \overline{p})$

   (q) $\overline{\overline{p}} \to p$

   (r) $p \to \overline{\overline{p}}$

   (s) $(\overline{q} \to \overline{p}) \to ((\overline{q} \to p) \to q)$

   (t) $(p \vee p) \to p$

   (u) $(q \to r) \to ((p \vee q) \to (p \vee r))$

   (v) $((p \to q) \to p) \to p$

   (w) $\overline{p} \to (p \to q)$

6. Пусть формула содержит только связки вида $\leftrightarrow$. Доказать, что эта формула является тавтологией тогда и только тогда, когда каждая переменная входит в неё чётное число раз.

7. Пусть формула содержит только связки вида $\leftrightarrow$ и $\neg$. Доказать, что эта формула является тавтологией тогда и только тогда, когда каждая переменная и каждый знак отрицания входит в неё чётное число раз.

2.6.4 Эквивалентность формул

1. Доказать, что если $A \sim B$ то для любой подстановки θ имеет место соотношение $\theta(A) \sim \theta(B)$.

2. Доказать эквивалентности

   (a) $\mathbf{1} \wedge A \sim A$, $\mathbf{1} \vee A \sim \mathbf{1}$, $\mathbf{0} \wedge A \sim \mathbf{0}$, $\mathbf{0} \vee A \sim A$

   (b) $\mathbf{1} \to A \sim A$, $\quad \mathbf{0} \to A \sim \mathbf{1}$
   $A \to \mathbf{1} \sim \mathbf{1} \quad A \to \mathbf{0} \sim \overline{A}$

   (c) $A \wedge A \sim A$, $\quad A \vee A \sim A$

   (d) $A \wedge B \sim B \wedge A$, $\quad A \vee B \sim B \vee A$

   (e) $A \wedge (B \wedge C) \sim (A \wedge B) \wedge C$

   (f) $A \vee (B \vee C) \sim (A \vee B) \vee C$

   (g) $A \wedge (B \vee C) \sim (A \wedge B) \vee (A \wedge C)$

   (h) $A \vee (B \wedge C) \sim (A \vee B) \wedge (A \vee C)$

   (i) $A \wedge (B \vee A) \sim A$, $\quad A \vee (B \wedge A) \sim A$

   (j) $A \leftrightarrow B \sim (A \to B) \wedge (B \to A)$

   (k) $A \leftrightarrow B \sim (A \wedge B) \vee (\overline{A} \wedge \overline{B})$

   (l) $A \to B \sim \overline{A} \vee B$

   (m) $\overline{A \wedge B} \sim \overline{A} \vee \overline{B}$, $\quad \overline{A \vee B} \sim \overline{A} \wedge \overline{B}$, $\quad \overline{\overline{A}} \sim A$

3. Доказать эквивалентности:

   (a) $A \to B \sim \overline{B} \to \overline{A}$

   (b) $\overline{A \to B} \sim A \wedge \overline{B}$

   (c) $A \to (B \to C) \sim (A \wedge B) \to C$

   (d) $A \to \overline{A} \sim \overline{A}$

   (e) $A \vee (\overline{A} \wedge B) \sim A \vee B$

   (f) $A \leftrightarrow (B \leftrightarrow C) \sim (A \leftrightarrow B) \leftrightarrow C$

   (g) $A \leftrightarrow B \sim B \leftrightarrow A$

   (h) $(A \vee B) \wedge (A \vee \overline{B}) \sim A$

   (i) $\left\{ \begin{array}{c} A \vee B \\ A \vee C \\ B \vee D \\ C \vee D \end{array} \right\} \sim \left[\begin{array}{c} A \wedge D \\ B \wedge C \end{array} \right]$

   (j) $\left\{ \begin{array}{l} A \\ A \vee C \\ B \vee C \end{array} \right\} \sim \left[\begin{array}{c} A \wedge C \\ B \wedge C \end{array} \right]$

   (k) $\left\{ \begin{array}{c} A \vee B \\ B \vee C \\ C \vee A \end{array} \right\} \sim \left[\begin{array}{c} A \wedge B \\ B \wedge C \\ C \wedge A \end{array} \right]$

   (l) $\left\{ \begin{array}{c} A \vee B \\ B \vee C \\ C \vee D \end{array} \right\} \sim \left[\begin{array}{c} A \wedge C \\ B \wedge C \\ B \wedge D \end{array} \right]$

   (m) $\left\{ \begin{array}{c} A \vee B \vee C \\ B \vee C \vee D \\ C \vee D \vee A \end{array} \right\} \sim \left[\begin{array}{l} A \wedge B \\ A \wedge D \\ B \wedge D \\ C \end{array} \right]$

   (n) $\left[\begin{array}{l} A \wedge B \\ \left\{ \begin{array}{c} A \vee B \\ \overline{A} \vee \overline{B} \end{array} \right\} \end{array} \right] \sim A \vee B$

Лекция 3

Анализ рассуждений

3.1 Логическая истинность

Высказывание называется **логически истинным**, если соответствующая ему формула ЛВ является тавтологией. Например, высказывание

Если идёт дождь или снег, и не идёт снег,
то идёт дождь

является логически истинным, т.к. соответствующая ему формула

$$((p \vee q) \wedge \overline{q}) \to p$$

является тавтологией.

Ниже мы будем обозначать формулы ЛВ, соответствующие высказываниям, теми же символами, которыми обозначены сами высказывания.

3.2 Логическое следствие

Пусть $A_1, \ldots, A_n$ и B – высказывания.

Высказывание B называется **логическим следствием** совокупности высказываний $A_1, \ldots, A_n$, если формула

$$(A_1 \wedge \ldots \wedge A_n) \to B$$

является тавтологией.

Если Γ – некоторая совокупность высказываний, и высказывание B является логическим следствием совокупности Γ, то этот факт выражается знакосочетанием

$$\Gamma \vdash B$$

которое называется **секвенцией**.

Совокупность Γ может быть пустой, в этом случае запись $\Gamma \vdash B$ означает, что высказывание B логически истинно.

3.3 Логическое рассуждение

Логическим рассуждением (или просто **рассуждением**) называется последовательность $A_1, \ldots, A_n$ высказываний, перед некоторыми из которых стоит слово "следовательно" (которое игнорируется при построении формул, соответствующих этим высказываниям).

Рассуждение является **логически правильным**, если для каждого входящего в него высказывания A_i, перед которым стоит слово "следовательно", A_i является логическим следствием некоторой совокупности высказываний вида $A_{j_1}, \ldots, A_{j_k}$ где $j_1, \ldots, j_k < i$.

3.4 Непротиворечивость

Набор высказываний $A_1, \ldots, A_n$ называется **непротиворечивым**, если существует оценка ξ переменных из $A_1, \ldots, A_n$, такая, что

$$\xi(A_1) = 1, \quad \ldots, \quad \xi(A_n) = 1$$

т.е. если формула $A_1 \wedge \ldots \wedge A_n$ выполнима.

3.5 Задачи

3.5.1 Логическое следствие

1. Доказать, что если

   - каждое высказывание из совокупности Γ содержится в совокупности Γ', и
   - $\Gamma \vdash B$

   то $\Gamma' \vdash B$.

2. Доказать эквивалентность соотношений:

   (a) $\Gamma \vdash A_1, \ \ldots, \ \Gamma \vdash A_n$

   (b) $\Gamma \vdash A_1 \wedge \ldots \wedge A_n$

3. Доказать эквивалентность соотношений:

   (a) $\Gamma, A \vdash B$

   (b) $\Gamma \vdash A \to B$

4. Доказать эквивалентность соотношений:

   - $\Gamma, A \vdash B$
   - $\Gamma, \overline{B} \vdash \overline{A}$

5. Доказать эквивалентность соотношений:

   (a) $\Gamma, A_1 \vdash B, \ \ldots, \ \Gamma, A_n \vdash B$

(b) $\Gamma, A_1 \vee \ldots \vee A_n \vdash B$

где для каждой совокупности Γ и формулы A знакосочетание Γ, A обозначает совокупность, содержащую все формулы из Γ и формулу A.

6. Доказать эквивалентность соотношений:
   - $\Gamma, A \vdash B$ и $\Gamma, B \vdash A$
   - $\Gamma \vdash A \leftrightarrow B$

7. Доказать эквивалентность соотношений
   (a) $\Gamma \vdash (A \to \bot) \to \bot$
   (b) $\Gamma \vdash A$.

8. Доказать, что если $\Gamma \vdash A$ и $\Gamma \vdash A \to B$, то $\Gamma \vdash B$.

9. Доказать, что если $A_1, \ldots, A_n \vdash B$, то для каждой подстановки θ имеет место соотношение

$$\theta(A_1), \ldots, \theta(A_n) \vdash \theta(B)$$

3.5.2 Логическое рассуждение

Выяснить, являются ли следующие рассуждения логическими правильными.

1. (a) Если Иван Иванович – коммунист, то Иван Иванович – атеист.
   (b) Иван Иванович – атеист.
   (c) Следовательно, Иван Иванович – коммунист.

2. (a) Если строить противоатомные убежища, то
      - другие государства будут чувствовать себя в опасности, а
      - наш народ получит ложное представление о своей безопасности.
   (b) Если другие страны будут чувствовать себя в опасности, то они смогут начать превентивную войну.
   (c) Если наш народ получит ложное представление о своей безопасности, то он ослабит свои усилия, направленные на сохранение мира.
   (d) Если же не строить противоатомные убежища, то мы рискуем иметь колоссальные потери в случае войны.
   (e) Следовательно, либо
      - – другие страны могут начать превентивную войну, и
        – наш народ ослабит свои усилия, направленные на сохранение мира,

        либо
      - мы рискуем иметь колоссальные потери в случае войны.

3. (a) Если Джонс не встречал ночью Смита, то либо
      - Смит был убийцей, либо
      - Джонс лжёт.
   (b) Если Смит не был убийцей, то
      - Джонс не встречал Смита этой ночью, и
      - убийство имело место после полуночи.
   (c) Если убийство было после полуночи, то либо
      - Смит был убийцей, либо
      - Джонс лжёт.
   (d) Следовательно, Смит был убийцей.

4. (a) Если капиталовложения останутся постоянными, то
      - возрастут правительственные расходы, или
      - возникнет безработица.
   (b) Если правительственные расходы не возрастут, то налоги будут снижены.
   (c) Если
      - налоги будут снижены, и
      - капиталовложения останутся постоянными,

      то безработица не возникнет.
   (d) Следовательно, правительственные расходы возрастут.

5. (a) Если я поеду автобусом, и автобус опоздает, то я опоздаю на работу.
   (b) Если я опоздаю на работу, то я не попадусь на глаза моему начальнику.
   (c) Если я не сделаю в срок важную работу, то я начну огорчаться и попадусь на глаза моему начальнику.
   (d) Следовательно, если я поеду автобусом, а автобус опоздает, то я сделаю в срок важную работу.

3.5.3 Непротиворечивость

1. Проверить непротиворечивость набора высказываний.
   (a) Либо свидетель не был запуган, либо, если Генри покончил жизнь самоубийством, то записка была найдена.
   (b) Если свидетель был запуган, то Генри не покончил жизнь самоубийством.
   (c) Если записка была найдена, то Генри покончил жизнь самоубийством.

2. Проверить непротиворечивость набора высказываний.

   (a) Если вечер скучен, то или

      - Алиса начинает плакать, или
      - Анатоль рассказывает смешные истории.

   (b) Если Сильвестр приходит на вечер, то или

      - вечер скучен, или
      - Алиса начинает плакать.

   (c) Если Анатоль рассказывает смешные истории, то Алиса не начинает плакать.

   (d) Сильвестр приходит на вечер тогда и только тогда, когда Анатоль не рассказывает смешные истории.

   (e) Если Алиса начинает плакать, то Анатоль рассказывает смешные истории.

3. Проверить непротиворечивость набора высказываний.

   (a) Если

      - курс ценных бумаг растёт, или
      - процентная ставка снижается,

      то либо

      - падает курс акций, либо
      - налоги не повышаются.

   (b) Курс акций понижается тогда и только тогда, когда

      - растёт курс ценных бумаг, и
      - налоги растут.

   (c) Если процентная ставка снижается, то либо

      - курс акций не понижается, либо
      - курс ценных бумаг не растёт.

   (d) Либо повышаются налоги, либо

      - курс акций понижается, и
      - снижается процентная ставка.

Лекция 4

Метод резолюций для ЛВ

4.1 КНФ

Литералом называется формула ЛВ вида p или $\overline{p}$ где p – булева переменная.

Дизъюнктом называется дизъюнкция некоторого множества литералов. Если это множество пусто, то соответствующий ему дизъюнкт называется **пустым**.

Формула ЛВ называется **конъюнктивной нормальной формой (КНФ)**, если она имеет вид

$$D_1 \wedge \ldots \wedge D_k \tag{4.1}$$

где $D_1, \ldots, D_k$ – дизъюнкты.

При помощи эквивалентных замен каждую формулу ЛВ можно преобразовать в эквивалентную ей КНФ.

Алгоритм приведения к виду КНФ состоит из перечисленных ниже этапов. Каждый этап состоит из замен подформул на эквивалентные им, которые выполняются до тех пор, пока их будет возможно выполнять. Когда выполнение действий, связанных с текущим этапом, становится невозможным, происходит переход к следующему этапу.

1. **Удаление стрелок.**
   (a) Каждая подформула вида $A \leftrightarrow B$ заменяется на $(A \wedge B) \vee (\overline{A} \wedge \overline{B})$.
   (b) Каждая подформула вида $A \rightarrow B$ заменяется на $\overline{A} \vee B$.
2. **Пронесение отрицаний к переменным.**
   (a) Каждая подформула вида $\overline{\overline{A}}$ заменяется на A.
   (b) Каждая подформула вида $\overline{A \wedge B}$ заменяется на $\overline{A} \vee \overline{B}$.
   (c) Каждая подформула вида $\overline{A \vee B}$ заменяется на $\overline{A} \wedge \overline{B}$.
3. **Вынесение конъюнкций наружу.**
   Подформулы вида $(A \wedge B) \vee C$ или $C \vee (A \wedge B)$ заменяются на $(A \vee C) \wedge (B \vee C)$.
4. **Удаление лишних скобок.**
   Подформулы вида $(A \wedge B) \wedge C$ или $A \wedge (B \wedge C)$ переписываются в виде $A \wedge B \wedge C$, а подформулы вида $(A \vee B) \vee C$ или $A \vee (B \vee C)$ – в виде $A \vee B \vee C$.

4.2 Метод резолюций для ЛВ

Метод резолюций даёт ответ на вопрос, является ли анализируемая формула ЛВ тавтологией.

4.2.1 Понятие резольвенты

Пусть задана пара дизъюнктов вида

$$p \vee D_1, \ \ \overline{p} \vee D_2 \tag{4.2}$$

где p – булева переменная, и D_1, D_2 – некоторые дизъюнкты, такие, что $D_1 \vee D_2 \neq \mathbf{1}$ (т.е. совокупность литералов, входящих в $D_1 \vee D_2$, не содержит пары противоположных литералов $q, \overline{q}$). Отметим, что каждый из дизъюнктов D_1, D_2 может быть пустым, и если дизъюнкт пуст, то он по определению равен формуле $\mathbf{0}$.

Резольвентой пары (4.2) называется дизъюнкт, состоящий из всех литералов, которые входят в D_1 или D_2.

Одна пара дизъюнктов может иметь несколько различных резольвент, в зависимости от выбора пары $p, \overline{p}$ удаляемых противоположных литералов в данных дизъюнктах.

4.2.2 Описание метода резолюций

Применение метода резолюций к формуле A заключается в том, что $\overline{A}$ приводится к КНФ, и составляется набор дизъюнктов, который сначала имеет вид

$$D_1, \ldots, D_k \tag{4.3}$$

(если КНФ для $\overline{A}$ имеет вид (4.1)), а затем к нему добавляются резольвенты произвольных пар дизъюнктов из текущего набора.

При построении резольвент могут использоваться как исходные дизъюнкты, так и добавленные.

Если к текущему набору в некоторый момент добавился пустой дизъюнкт, то A является тавтологией.

Если же к текущему набору невозможно добавить ни одной новой резольвенты, и среди дизъюнктов текущего набора нет пустого дизъюнкта, то A не является тавтологией.

4.2.3 Корректность метода резолюций

Свойство **корректности** метода резолюций заключается в том, что если в некоторый момент к текущему набору добавился пустой дизъюнкт, то анализируемая формула A является тавтологией.

Для доказательства этого свойства предположим, что A – не тавтология, т.е. существует означивание ξ, такое, что $\xi(A) = 0$, откуда следует, что $\xi(\overline{A}) = 1$.

Т.к. $\overline{A}$ эквивалентна своей КНФ (4.1), то

$$\xi(D_1 \wedge \ldots \wedge D_k) = 1 \tag{4.4}$$

т.е. для каждого дизъюнкта D_i из исходного набора (4.3) имеет место соотношение $\xi(D_i) = 1$.

Нетрудно доказать, что если пара дизъюнктов была истинной при означивании ξ, то их резольвента тоже является истинной при означивании ξ. Следовательно, все дизъюнкты, которые были добавлены к первоначальному набору (4.3), истинны при означивании ξ.

По предположению, в некоторый момент к текущему набору добавился пустой дизъюнкт.

Пустой дизъюнкт может быть получен только из такой пары (4.2), в которой дизъюнкты D_1 и D_2 являются пустыми. Следовательно, среди дизъюнктов, которые были добавлены к первоначальному набору (4.3), содержатся дизъюнкты вида p и $\overline{p}$, где p – булева переменная.

Как отмечено выше, оба этих дизъюнкта (p и $\overline{p}$) должны быть истинными при означивании ξ. Согласно нашим определениям, такого не может быть. Следовательно, наше предположение о том, что A – не тавтология, является ошибочным.

4.2.4 Полнота метода резолюций

Полнота метода резолюций заключается в том, что если анализируемая формула A является тавтологией, то из набора (4.3), можно вывести пустой дизъюнкт.

Если A – тавтология, то $\overline{A} = \mathbf{0}$. Поскольку формула (4.1) эквивалентна $\overline{A}$, то она тоже равна $\mathbf{0}$.

Докажем, что если некоторая формула вида (4.1) равна $\mathbf{0}$, то из набора (4.3) входящих в неё дизъюнктов можно вывести пустой дизъюнкт. Это свойство будет доказываться индукцией по числу переменных в (4.1).

Пусть (4.1) содержит только одну переменную p. Если она равна $\mathbf{0}$, то это возможно только тогда, когда $D_1 = p$ и $D_2 = \overline{p}$. Очевидно, что из этой пары можно вывести пустой дизъюнкт.

Пусть теперь (4.1) содержит n булевых переменных $p_1, \ldots, p_n$ (где $n > 1$). Все дизъюнкты из совокупности (4.3) можно разделить на следующие 3 группы:

$$\begin{array}{lll} p_1 \vee D_1^1, & \ldots, & p_1 \vee D_s^1 \\ \overline{p_1} \vee D_1^2, & \ldots, & \overline{p_1} \vee D_q^2 \\ D_1^3, & \ldots, & D_r^3 \end{array}$$

где все поддизъюнкты вида $D_j^{(i)}$ не содержат p_1.

Рассмотрим КНФ, состоящую из некоторых резольвент дизъюнктов первой и второй группы, а также из всех дизъюнктов третьей группы:

$$\left\{ \begin{array}{lllll} (D_1^1 \vee D_1^2) & \wedge & \ldots & \wedge & (D_1^1 \vee D_q^2) \\ \ldots & & & & \\ (D_s^1 \vee D_1^2) & \wedge & \ldots & \wedge & (D_s^1 \vee D_q^2) \\ D_1^3 & \wedge & \ldots & \wedge & D_r^3 \end{array} \right\} \tag{4.5}$$

Если хотя бы один из дизъюнктов, входящих в (4.5), является пустым, то требуемое утверждение доказано. Если все они непусты, то докажем, что (4.5) равна $\mathbf{0}$. Заметим, что, поскольку число переменных в (4.5) меньше, чем в (4.1), то, по индуктивному предположению, из дизъюнктов, входящих в (4.5), можно вывести пустой дизъюнкт, а поскольку каждый из них либо входит в (4.3), либо является резольвентой дизъюнктов из (4.3), то из (4.3) тоже можно вывести пустой дизъюнкт.

Предположим, что (4.5) не равна $\mathbf{0}$. Тогда существует означивание ξ переменных из списка $p_2, \ldots, p_n$, при котором все дизъюнкты, входящие в (4.5), имеют значение 1.

Возможен один из двух случаев:

$$\xi(D_1^1) = \ldots = \xi(D_s^1) = 1 \tag{4.6}$$

$$\xi(D_1^2) = \ldots = \xi(D_q^2) = 1 \tag{4.7}$$

т.к. если неверно ни (4.6), ни (4.7), то для некоторых i и j имеет место соотношение

$$\xi(D_i^1 \vee D_j^2) = 0$$

которое противоречит предположению о том, что все дизъюнкты, входящие в (4.5), являются истинными на означивании ξ.

Доопределим ξ до означивания переменных из списка $p_1, \ldots, p_n$, полагая $\xi(p_1) \stackrel{\text{def}}{=} 0$, если имеет место (4.6), и $\xi(p_1) \stackrel{\text{def}}{=} 1$, если имеет место (4.7). Нетрудно видеть, что при таком означивании все дизъюнкты из набора (4.3) принимают значение 1, что противоречит предположению о том, что формула (4.1) равна $\mathbf{0}$.

4.3 Задачи

1. Доказать, что метод резолюций обладает свойством завершаемости, т.е. при любом способе построения резольвент после конечного числа шагов выдаёт ответ, является ли анализируемая формула A тавтологией, или нет. Оценить число этих шагов в зависимости от числа переменных, входящх в A.

2. Решить методом резолюций все задачи из главы 2, в которых требуется проверить, является ли некоторая формула ЛВ тавтологией или выполнимой формулой.

Лекция 5

Введение в теорию множеств

5.1 Понятие множества

Под **множеством** понимается произвольная совокупность каких-либо **объектов**, например

- совокупность всех математиков в России, или
- совокупность всех звёзд во Вселенной.

Объекты, из которых состоит множество, называются его **элементами**.

Тот факт, что объект a является элементом множества M, обозначается знакосочетанием $a \in M$, которое читается следующим образом:

"a принадлежит множеству M".

Если объект a не является элементом множества M, то данный факт записывается знакосочетанием $a \notin M$, которое читается следующим образом:

"a не принадлежит множеству M".

Элементы множества сами могут являться множествами. Например, пусть M есть множество групп студентов. В данном случае элементами M являются **группы** (а не сами студенты). Элементами каждой группы являются студенты.

5.2 Способы задания множеств

5.2.1 Перечисление

Множество можно задать например путём перечисления всех объектов, которые являются его элементами.

Например, множество всех арабских цифр можно задать путём перечисления всех принадлежащих ему элементов:

$$1, 2, 3, 4, 5, 6, 7, 8, 9, 0$$

Данный способ задания годится не для всех множеств. Множества, которые можно задать путём перечисления всех входящих в них элементов, называются **конечными**. Все остальные множества называются **бесконечными**.

Если множество M является конечным, и состоит из элементов a_1, $a_2, \ldots$, a_n, то данный факт обозначается знакосочетанием

$$M = \{a_1, a_2, \ldots, a_n\}. \qquad (5.1)$$

Порядок перечисления элементов множества M в записи (5.1) не имеет никакого значения. Кроме того, не имеет никакого значения наличие лишних копий в списке (5.1): даже если некоторый элемент a_i встречается в этом списке несколько раз, в множество M он всё равно входит только в одном экземпляре.

Множество может состоять только из одного элемента, т.е. иметь вид $\{a\}$, где a – некоторый объект. Не следует считать одинаковыми сам объект a и множество $\{a\}$. В частности, утверждение $a \in \{a\}$ является истинным, в то время как утверждение $a \in a$ – абсурдно. Кроме того, $\{a\} \in \{\{a\}\}$ но неверно, что $a \in \{\{a\}\}$, поскольку единственным элементом множества $\{\{a\}\}$ является множество $\{a\}$.

Примером бесконечного множества является совокупность $\mathbf{N}$ всех натуральных чисел:

$$\mathbf{N} = \{1, 2, 3, \ldots\}$$

5.2.2 Указание свойства

Другой способ определить множество – указать свойство, выделяющее элементы определяемого множества среди элементов некоторого множества.

Пусть имеются некоторое множество A, и некоторое свойство P, такое, что для каждого элемента a множества A можно установить, обладает ли a свойством P, или нет.

Знакосочетание

$$\{x \in A \mid a \text{ обладает свойством } P\} \qquad (5.2)$$

обозначает множество, элементами которого являются все элементы множества A, обладающие свойством P.

Например, пусть

- A – множество всех целых чисел, и
- P есть свойство делимости нацело на 2.

Тогда (5.2) есть множество всех чётных чисел.

5.3 Подмножества

5.3.1 Понятие подмножества

Множество A называется **подмножеством** множества B, если каждый элемент множества A является элементом множества B.

Если A является подмножеством B, то этот факт записывается знакосочетанием $A \subseteq B$. Если имеет место $A \subseteq B$, то говорят также, что A **содержится** (или **включается**) в B, а B **содержит** (или **включает**) A.

Множество A называется **собственным подмножеством** множества B, если $A \subseteq B$ и $A \neq B$.

Мы будем считать множества A и B одинаковыми (и обозначать этот факт знакосочетанием $A = B$), если имеют место соотношения

$$A \subseteq B \quad \text{и} \quad B \subseteq A \tag{5.3}$$

т.е. если A и B состоят из одних и тех же элементов.

Например, следующие множества A и B являются одинаковыми:

$$A \stackrel{\text{def}}{=} \{x \in \mathbf{R} \mid \sin(x) = 1\}$$

и

$$B \stackrel{\text{def}}{=} \{x \in \mathbf{R} \mid x = \frac{\pi}{2} + 2k\pi,\ k \in \mathbf{Z}\}$$

где $\mathbf{R}$ – множество всех действительных чисел, и $\mathbf{Z}$ – множество всех целых чисел.

5.3.2 Пустое множество

Мы будем предполагать, что существует единственное множество, такое, что никакой объект не является его элементом. Данное множество называется **пустым множеством**, и обозначается символом $\emptyset$.

Из определения отношения включения вытекает, что для каждого множества A имеет место соотношение

$$\emptyset \subseteq A$$

Заметим, что множество $\{\emptyset\}$ не является пустым, т.к. оно содержит один элемент. Данный элемент является пустым множеством.

5.3.3 Множество всех подмножеств

Пусть задано некоторое множество A.

Множество

$$\{B \mid B \subseteq A\} \tag{5.4}$$

элементами которого являются подмножества множества A, обозначается символом $\mathbf{2}^A$.

Например, если $A = \{1, 2, 3\}$ то

$$\mathbf{2}^A = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\}\}$$

Нетрудно доказать, что если множество A является конечным и состоит из n элементов, то множество $\mathbf{2}^A$ тоже является конечным и состоит из 2^n элементов.

5.4 Операции над множествами

5.4.1 Операции над парой множеств

Пусть задана пара множеств A, B.

Пересечение множеств A и B – это множество, обозначаемое знакосочетанием $A \cap B$, и определяемое следующим образом:

$$A \cap B \stackrel{\text{def}}{=} \{x \mid x \in A \ \text{ и } \ x \in B\}.$$

Объединение множеств A и B – это множество, обозначаемое знакосочетанием $A \cup B$, и определяемое следующим образом:

$$A \cup B \stackrel{\text{def}}{=} \{x \mid x \in A \ \text{ или } \ x \in B\}.$$

Разность множеств A и B – это множество, обозначаемое знакосочетанием $A \setminus B$, и определяемое следующим образом:

$$A \setminus B \stackrel{\text{def}}{=} \{x \mid x \in A \ \text{ и } \ x \notin B\}.$$

5.4.2 Операции над семействами множеств

Пусть $\Im$ – некоторое множество, элементы которого называются **индексами**.

$\Im$–индексированное семейство множеств – это некоторая совокупность множеств, такая, что с каждым индексом $i \in \Im$ связано некоторое множество A_i из данной совокупности. Допускается, что для разных индексов $i, j \in \Im$ множества A_i и A_j из семейства (5.5) могут совпадать.

$\Im$–индексированное семейство множеств обозначается знакосочетанием вида

$$(A_i \mid i \in \Im) \tag{5.5}$$

Пересечением семейства (5.5) называется множество, обозначаемое символом $\bigcap\limits_{i \in \Im} A_i$, и определяемое следующим образом:

$$\bigcap_{i \in \Im} A_i \stackrel{\text{def}}{=} \{x \mid \text{для любого } i \in \Im \quad x \in A_i\}.$$

Объединением семейства (5.5) называется множество, обозначаемое символом $\bigcup\limits_{i \in \Im} A_i$, и определяемое следующим образом:

$$\bigcup_{i \in \Im} A_i \stackrel{\text{def}}{=} \{x \mid \text{существует } \ i \in \Im, \text{ такой, что } \quad x \in A_i\}.$$

В том случае, когда множество индексов $\Im$ является конечным и имеет вид $\{1, 2, \ldots, n\}$, множества $\bigcap\limits_{i \in \Im} A_i$ и $\bigcup\limits_{i \in \Im} A_i$ могут обозначаться знакосочетаниями

$$A_1 \cap \ldots \cap A_n \quad \text{и} \quad A_1 \cup \ldots \cup A_n$$

соответственно.

5.5 Задачи

1. Доказать, что для любых множеств A, B, C
   (a) $A \subseteq A$
   (b) если $A \subseteq B$ и $B \subseteq C$, то $A \subseteq C$
   (c) $A \cap B \subseteq A$
   (d) $A \cap B \subseteq B$
   (e) $A \subseteq A \cup B$
   (f) $B \subseteq A \cup B$
   (g) $A \setminus B \subseteq A$

2. Доказать, что $\emptyset \neq \{\emptyset\}$.

3. Доказать, что $\{\{1,2\},\{2,3\}\} \neq \{1,2,3\}$.

4. Доказать, что для любого множества A
   (a) если $A \subseteq \emptyset$, то $A = \emptyset$
   (b) $A \cap \emptyset = \emptyset$
   (c) $A \cup \emptyset = A$

5. Доказать, что существует лишь одно множество, не имеющее элементов.

6. Существуют ли множества A, B, C, такие что
$$A \cap B \neq \emptyset, \qquad A \cap C = \emptyset, \qquad (A \cap B) \setminus C = \emptyset$$

7. Доказать, что следующие соотношения эквивалентны:
   (a) $A \subseteq B$
   (b) $A \cup B = B$
   (c) $A \cap B = A$
   (d) $A \setminus B = \emptyset$

8. Доказать следующие тождества:
   (a) $A \cup A = A \cap A = A$
   (b) $A \cap B = B \cap A$
   (c) $A \cup B = B \cup A$
   (d) $A \cap (B \cap C) = (A \cap B) \cap C$
   (e) $A \cup (B \cup C) = (A \cup B) \cup C$
   (f) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
   (g) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
   (h) $(A \cap B) \cup (C \cap D) =$
   $(A \cup C) \cap (B \cup C) \cap (A \cup D) \cap (B \cup D)$
   (i) $A \cup (A \cap B) = A$
   (j) $A \cap (A \cup B) = A$

9. Доказать следующие тождества:
   (a) $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$
   (b) $A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C)$
   (c) $A \setminus (A \setminus B) = A \cap B$
   (d) $A \setminus B = A \setminus (A \cap B)$
   (e) $A \cap (B \setminus C) = (A \cap B) \setminus (A \cap C)$
   (f) $A \cap (B \setminus C) = (A \cap B) \setminus C$
   (g) $(A \setminus B) \setminus C = (A \setminus C) \setminus (B \setminus C)$
   (h) $A \cup B = A \cup (B \setminus A)$
   (i) $A \cap (B \setminus A) = \emptyset$
   (j) $(A \cup B) \setminus C = (A \setminus C) \cup (B \setminus C)$
   (k) $A \setminus (B \setminus C) = (A \setminus B) \cup (A \cap C)$
   (l) $(A \setminus B) \setminus C = A \setminus (B \cup C)$

10. Доказать, что
   (a) $A \cup B \subseteq C \quad \Leftrightarrow \quad A \subseteq C$ и $B \subseteq C$
   (b) $A \subseteq B \cap C \quad \Leftrightarrow \quad A \subseteq B$ и $A \subseteq C$
   (c) $(A \setminus B) \cup B = A \quad \Leftrightarrow \quad B \subseteq A$
   (d) $(A \cap B) \cup C = A \cap (B \cup C) \quad \Leftrightarrow \quad C \subseteq A$
   (e) $A \subseteq B \quad \Rightarrow \quad (A \cup C) \subseteq (B \cup C)$
   (f) $A \subseteq B \quad \Rightarrow \quad (A \cap C) \subseteq (B \cap C)$
   (g) $A \subseteq B \quad \Rightarrow \quad (A \setminus C) \subseteq (B \setminus C)$
   (h) $A \subseteq B \quad \Rightarrow \quad (C \setminus B) \subseteq (C \setminus A)$
   (i) $A \cup B = A \cap B \quad \Leftrightarrow \quad A = B$
   (j) $A = B \quad \Leftrightarrow \quad (A \setminus B) \cup (B \setminus A) = \emptyset$

11. Доказать, что множество из n элементов имеет 2^n подмножеств.

12. Найти все подмножества множеств
$$\emptyset, \quad \{\emptyset\}, \quad \{x\}, \quad \{1,2\}$$

13. Доказать, что
   (a) $\mathbf{2}^{A \cap B} = \mathbf{2}^A \cap \mathbf{2}^B$
   (b) $\mathbf{2}^{A \cup B} = \{A_1 \cup B_1 \mid A_1 \in \mathbf{2}^A, \quad B_1 \in \mathbf{2}^B\}$

14. Доказать, что для любых множеств $A_1, \ldots, A_n$
$$\begin{array}{ll} \text{если} & A_1 \subseteq A_2 \subseteq \ldots \subseteq A_n \subseteq A_1 \\ \text{то} & A_1 = A_2 = \ldots = A_n \end{array}$$

15. Решить систему уравнений
$$\begin{cases} A \cap X = B \\ A \cup X = C \end{cases}$$
где A, B и C – заданные множества, и
$$B \subseteq A, \quad A \subseteq C$$

16. Решить систему уравнений
$$\begin{cases} A \setminus X = B \\ X \setminus A = C \end{cases}$$
где A, B и C – заданные множества, и
$$B \subseteq A, \quad A \cap C = \emptyset$$

17. Решить систему уравнений

$$\begin{cases} A \setminus X = B \\ A \cup X = C \end{cases}$$

где A, B и C – заданные множества, и

$$B \subseteq A, \quad A \subseteq C$$

18. Решить системы уравнений

(a) $\begin{cases} A \cup X = B \cap X \\ A \cap X = C \cup X \end{cases}$

(b) $\begin{cases} A \setminus X = X \setminus B \\ X \setminus A = C \setminus X \end{cases}$

(c) $\begin{cases} A \cap X = B \setminus X \\ C \cup X = X \setminus A \end{cases}$

При каких A, B, C эти системы имеют решение?

19. Доказать, что для семейства $(A_i \mid i \in \Im)$ и произвольного множества B имеет место соотношение

$$\Big(\text{для каждого } i \in \Im \quad A_i \subseteq B\Big) \quad \Leftrightarrow \quad \bigcup_{i \in \Im} A_i \subseteq B$$

20. Доказать, что для семейства $(A_i \mid i \in \Im)$ и произвольного множества B имеет место соотношение

$$\Big(\text{для каждого } i \in \Im \quad B \subseteq A_i\Big) \quad \Leftrightarrow \quad B \subseteq \bigcap_{i \in \Im} A_i$$

21. Если семейства $(A_i \mid i \in \Im)$ и $(B_i \mid i \in \Im)$ таковы, что для каждого $i \in \Im \quad A_i \subseteq B_i$, то

$$\bigcap_{i \in \Im} A_i \subseteq \bigcap_{i \in \Im} B_i \quad \text{и} \quad \bigcup_{i \in \Im} A_i \subseteq \bigcup_{i \in \Im} B_i$$

Лекция 6

Отношения и функции

6.1 Списки

Списком называется упорядоченная совокупность объектов

$$(O_1, \dots, O_n) \tag{6.1}$$

причём некоторые из этих объектов могут совпадать. Порядок следования членов списка важен, т.е. списки

$$(O_1, \dots, O_n) \quad \text{и} \quad (O'_1, \dots, O'_n)$$

считаются равными только в том случае, когда

$$\text{для каждого} \quad i = 1, \dots, n \quad O_i = O'_i$$

Список (6.1) может быть пустым, т.е. иметь вид

$$(\,)$$

6.2 Декартовы произведения

Пусть задан некоторый список множеств

$$(A_1, \dots, A_n) \tag{6.2}$$

Декартовым произведением этого списка называется множество, обозначаемое знакосочетанием

$$A_1 \times \ldots \times A_n \tag{6.3}$$

и состоящее из всех списков вида $(a_1, \dots, a_n)$, где для каждого $i = 1, \dots, n \quad a_i \in A_i$.

Например, если $n = 2,\ A_1 = \{1, 2\},\ A_2 = \{3, 4\}$, то множество $A_1 \times A_2$ имеет вид

$$\{(1, 3), (2, 3), (1, 4), (2, 4)\}$$

Если все множества в списке (6.2) совпадают, т.е. $A_1 = \ldots = A_n = A$, то множество (6.3) можно обозначать символом A^n.

Если хотя бы одно из множеств, входящих в список (6.2), является пустым, то декартово произведение (6.3) по определению является одноэлементным множеством $\{1\}$. Аналогичный вид имеет декартово произведение пустого списка множеств.

Отношением на (6.2) называется произвольное подмножество R декартова произведения (6.3).

6.3 Бинарные отношения

6.3.1 Понятие бинарного отношения

Пусть задано некоторое множество A.

Бинарное отношение на множестве A (называемое ниже просто **отношением**) – это произвольное подмножество R множества A^2.

Отношение $R \subseteq A^2$ можно изобразить в виде графа, вершинами которого являются элементы множества A: для каждой пары a, b вершин данный граф содержит ребро из a в b тогда и только тогда, когда $(a, b) \in R$.

Ниже множество A предполагается фиксированным, и все рассматриваемые отношения являются бинарными отношениями на множестве A.

Для произвольной пары $(a, b) \in A^2$ утверждение о том, что данная пара принадлежит отношению R, записывают знакосочетанием $R(a, b)$ или aRb.

Отношение, состоящее из всех пар вида (a, a), где $a \in A$, обозначается символом id_A.

Если R – бинарное отношение на A, то для каждого $a \in A$ символ $R(a)$ обозначает множество, состоящее из всех $b \in A$, таких, что $(a, b) \in R$. Если изображать отношение R в виде графа, то множество $R(a)$ состоит из концов рёбер с началом в a.

6.3.2 Операции на отношениях

Для каждой пары отношений $R_1,\ R_2$

- **пересечение** $R_1 \cap R_2$ состоит из всех пар (a, b), которые принадлежат одновременно R_1 и R_2
- **объединение** $R_1 \cup R_2$ состоит из всех пар (a, b), каждая из которых принадлежит R_1 или R_2
- **произведение** $R_1 \circ R_2$ состоит из всех пар (a, b), для каждой из которых существует элемент c, такой, что $(a, c) \in R_1$ и $(c, b) \in R_2$.

Для каждого отношения R

- его **дополнение** $\overline{R}$ состоит из всех пар из A^2, не принадлежащих R
- **обратным** к R называется отношение R^{-1}, состоящее из всех пар (a, b), таких, что $(b, a) \in R$.

6.3.3 Специальные бинарные отношения

Отношение $R \subseteq A^2$ называется

- **рефлексивным**, если $id_A \subseteq R$, т.е. для каждого $a \in A \quad (a,a) \in R$
- **иррефлексивным**, если $id_A \cap R = \emptyset$, т.е. для каждого $a \in A \quad (a,a) \notin R$
- **симметричным**, если $R^{-1} = R$, т.е. если $(a,b) \in R$, то $(b,a) \in R$
- **антисимметричным**, если $R \cap R^{-1} \subseteq id_A$, т.е. если $(a,b) \in R$ и $(b,a) \in R$, то $a = b$
- **транзитивным**, если $R \circ R \subseteq R$, т.е. если $(a,b) \in R$ и $(b,c) \in R$, то $(a,c) \in R$

6.3.4 Эквивалентности

Бинарное отношение $R \subseteq A^2$ называется **отношением эквивалентности** (или просто **эквивалентностью**), если оно является одновременно рефлексивным, симметричным, и транзитивным.

Каждая эквивалентность $R \subseteq A^2$ порождает некоторое **разбиение** множества A, где под разбиением A понимается семейство

$$S = \{A_i \mid i \in \Im\} \tag{6.4}$$

непустых подмножеств множества A (называемых **классами** разбиения), такое, что каждый элемент множества A принадлежит ровно одному из этих классов. Каждый класс разбиения, которое соответствует отношению эквивалентности R, имеет вид $R(a)$, где a – произвольный элемент множества A. Докажем, что семейство подмножеств вида $R(a)$ действительно образует разбиение.

- Каждый элемент $a \in A$ принадлежит некоторому из этих подмножеств, а именно - $R(a)$, потому что R – рефлексивно.
- Элемент $a \in A$ не может принадлежать двум различным подмножествам $R(b)$ и $R(c)$, потому что если $a \in R(b)$ и $a \in R(c)$, т.е. $(b,a) \in R$ и $(c,a) \in R$, то $(a,b) \in R$ (т.к. R – симметрично), и, следовательно, $(c,b) \in R$ (т.к. R – транзитивно).

  Поэтому, если $d \in R(b)$, т.е. $(b,d) \in R$, то из транзитивности R следует, что $(c,d) \in R$, т.е. $d \in R(c)$. Таким образом, $R(b) \subseteq R(c)$, и аналогично доказывается, что $R(c) \subseteq R(b)$. Следовательно, подмножества $R(b)$ и $R(c)$ совпадают.

Обратно, каждое разбиение S вида (6.4) порождает эквивалентность на A, при которой элементы эквивалентны, если они принадлежат одному и тому же классу разбиения S.

Нетрудно видеть, что данные переходы (от эквивалентности к разбиению и от разбиения к эквивалентности) являются взаимно обратными.

Совокупность всех классов разбиения множества A, порождаемого эквивалентностью R, обозначается символом A/R, и называется **фактор-множеством** множества A относительно эквивалентности R. Для каждого элемента $a \in A$ символ $[a]$ обозначает тот класс из A/R, которому принадлежит a. Элемент a называется **представителем** этого класса.

6.3.5 Частичные порядки

Бинарное отношение на множестве A называется

- **квазипорядком**, если оно является одновременно рефлексивным, и транзитивным
- **частичным порядком** (или просто **порядком**), если оно является одновременно рефлексивным, антисимметричным, и транзитивным.

Порядок обычно обозначается символом $\leq$. Мы будем писать $a < b$, если $a \leq b$ и $a \neq b$.

Отношение $\leq^{-1}$ обозначается символом $\geq$. Оно тоже является порядком, и называется **двойственным** к порядку $\leq$.

Порядок $\leq$ на множестве A называется **линейным**, если для любых $a, b \in A$ либо $a \leq b$, либо $b \leq a$.

Множество A, на котором задан частичный порядок, называется **частично упорядоченным** (относительно данного частичного порядка). Если данный частичный порядок является линейным, то A называется **линейно упорядоченным** (относительно данного линейного порядка).

Пусть на множестве A задан частичный порядок $\leq \subseteq A^2$. Каждое подмножество $A' \subseteq A$ может рассматриваться как частично упорядоченное множество, порядок на котором **индуцирован** порядком на A, т.е. для каждой пары a, b элементов подмножества A' мы полагаем, что $a \leq b$, если пара (a,b) принадлежит отношению $\leq$ частичного порядка на A. Подмножество A' называется **цепью** в A, если оно является линейно упорядоченным относительно этого индуцированного порядка.

Элемент a частично упорядоченного множества A называется

- **максимальным**, если для каждого $b \in A$ из того, что $a \leq b$ следует, что $a = b$
- **минимальным**, если для каждого $b \in A$ из того, что $b \leq a$ следует, что $b = a$
- **наибольшим**, если для каждого $b \in A \quad b \leq a$
- **наименьшим**, если для каждого $b \in A \quad a \leq b$.

Пусть A' – подмножество частично упорядоченного множества A.

- **Нижней гранью** подмножества A' называется произвольный элемент $a \in A$, такой, что для каждого $b \in A'$ имеет место неравенство $a \leq b$.

Знакосочетание $a \le A'$ выражает тот факт, что a – нижняя грань A'.

- **Точной нижней гранью** подмножества A' называется элемент $\inf(A')$, обладающий свойством:

  $$\text{для каждого } b \in A \qquad b \le A' \quad \Leftrightarrow \quad b \le \inf(A')$$

- **Верхней гранью** подмножества A' называется произвольный элемент $a \in A$, такой, что для каждого $b \in A'$ имеет место неравенство $b \le a$.

  Знакосочетание $A' \le a$ выражает тот факт, что a – верхняя грань A'.

- **Точной верхней гранью** подмножества A' называется элемент $\sup(A')$, обладающий свойством:

  $$\text{для каждого } b \in A \qquad A' \le b \quad \Leftrightarrow \quad \sup(A') \le b$$

Отметим, что элементы $\inf(A')$ и $\sup(A')$ могут не принадлежать подмножеству A' (и могут вообще не существовать).

Если множество A' является конечным и имеет вид $\{a_1, \ldots, a_n\}$, то элементы $\inf(A')$ и $\sup(A')$ (если они существуют) обозначаются соответственно знакосочетаниями

$$a_1 \wedge \ldots \wedge a_n \quad \text{и} \quad a_1 \vee \ldots \vee a_n$$

Частично упорядоченное множество A называется **вполне упорядоченным**, если для каждого непустого подмножества $A' \subseteq A$ существует элемент $\inf(A')$, и этот элемент принадлежит A'.

Частично упорядоченное множество A называется **решёткой**, если для любых двух элементов $a, b \in A$ существует их точная нижняя грань $a \wedge b$ и их точная верхняя грань $a \vee b$. В любой решётке для произвольной конечной совокупности $a_1, \ldots, a_n$ элементов существуют её точная нижняя грань и точная верхняя грань:

$$\begin{aligned} a_1 \wedge \ldots \wedge a_n &= a_1 \wedge (a_2 \wedge (\ldots \wedge a_n)) \\ a_1 \vee \ldots \vee a_n &= a_1 \vee (a_2 \vee (\ldots \vee a_n)) \end{aligned}$$

Полной решёткой называется частично упорядоченное множество A, такое, что для каждого подмножества $A' \subseteq A$ существуют его точная нижняя грань $\inf(A')$ и его точная верхняя грань $\sup(A')$. В частности, существуют элементы $\inf(A)$ и $\sup(A)$, которые обозначаются символами 0 и 1 соответственно.

Полной алгеброй Гейтинга называется полная решётка A, в которой для каждой пары $a, b \in A$ определён элемент

$$a \to b \tag{6.5}$$

обладающий следующим свойством: для каждого $c \in A$

$$c \le (a \to b) \quad \Leftrightarrow \quad (c \wedge a) \le b \tag{6.6}$$

Полной булевой алгеброй называется полная алгебра Гейтинга, в которой для каждого элемента a имеет место равенство

$$(a \to 0) \to 0 \; = \; a$$

6.4 Функции

6.4.1 Понятие функции

Функцией из множества A в множество B называется произвольное соответствие f, которое сопоставляет каждому элементу a множества A некоторый элемент $f(a)$ множества B.

Функция f из A в B обозначается знакосочетанием $f : A \to B$ или

$$A \xrightarrow{f} B \tag{6.7}$$

Если f – функция из A в B, то для каждого $a \in A$ элемент $f(a)$ называется **значением** функции f при значении аргумента a (или просто значением f на a).

Если элемент b является значением f на a, то этот факт обозначается знакосочетанием

$$a \mapsto b$$

Пусть заданы функции f и g вида

$$A \xrightarrow{f} B \;, \quad B \xrightarrow{g} C$$

Композицией f и g называется функция gf вида

$$A \xrightarrow{gf} C$$

которая сопоставляет каждому элементу a множества A элемент $g(f(a))$ множества C.

Для каждого множества A символ id_A обозначает функцию вида

$$A \xrightarrow{id_A} A$$

которая сопоставляет каждому элементу $a \in A$ тот же элемент a, т.е.

$$id_A(a) \stackrel{\text{def}}{=} a$$

Множество всех функций из A в B обозначается символом B^A.

6.4.2 Образы и прообразы

Пусть f – функция вида (6.7).

Если для пары элементов $a \in A, \; b \in B$ имеет место соотношение $b = f(a)$, то

- b называется **образом** элемента a относительно функции f, и
- a называется **прообразом** элемента b относительно функции f.

Для каждого подмножества $A' \subseteq A$ символ $f(A')$ обозначает множество, называемое **образом** подмножества A' относительно функции f, и состоящее из всех элементов вида $f(a)$, где a – произвольный элемент множества A'.

Множество $f(A)$ обозначается символом $Im(f)$.

Для каждого подмножества $B' \subseteq B$ символ $f^{-1}(B')$ обозначает множество, называемое **прообразом** подмножества B' относительно функции f, и состоящее из всех элементов a множества A, таких, что $f(a) \in B$. Если множество B' состоит из одного элемента b, то вместо $f^{-1}(\{b\})$ пишут просто $f^{-1}(b)$.

6.4.3 Классы функций

Функция f вида (6.7) называется

- **инъективной**, если для каждой пары $a, a' \in A$ имеет место соотношение

$$a \neq a' \quad \Rightarrow \quad f(a) \neq f(a')$$

  т.е. если для каждого $b \in B$ множество $f^{-1}(b)$ или пусто, или состоит из одного элемента

- **сюръективной**, если для каждого $b \in B$ множество $f^{-1}(b)$ непусто

- **биективной** (или **биекцией**), если f является одновременно инъективной и сюръективной, т.е. если для каждого $b \in B$ множество $f^{-1}(b)$ состоит из одного элемента.

Заметим, что если $f : A \to B$ – биекция, то функция $f^{-1} : B \to A$, сопоставляющая каждому $b \in B$ единственный элемент множества $f^{-1}(b)$, обладает следующим свойством:

$$f^{-1}f = id_A, \quad ff^{-1} = id_B$$

6.4.4 Монотонные функции

Пусть A и B – частично упорядоченные множества, и f – функция из A в B. Функция f называется **монотонной**, если для любых $a, b \in A$ из $a \leq b$ следует $f(a) \leq f(b)$.

Если $f : A \to B$ – биекция, и f и f^{-1} – монотонные функции, то f называется **изоморфизмом** частично упорядоченных множеств A и B, а множества A и B называются **изоморфными**.

6.5 Задачи

6.5.1 Декартовы произведения

1. Пусть заданы два отрезка действительной прямой: $[a, b]$ и $[c, d]$. Найти геометрическую интерпретацию следующих множеств:
   (a) $[a, b] \times [c, d]$
   (b) $[a, b]^2$
   (c) $[a, b]^3$
2. Доказать, что
$$(A \times B) \cap (C \times D) = (A \cap C) \times (B \cap D)$$
3. Доказать, что
$$(A \times B) \cup (C \times D) \subseteq (A \cup C) \times (B \cup D)$$
   При каких условиях на A, B, C, D данное включение является равенством?
4. Доказать, что
   (a) $(A \cup B) \times C = (A \times C) \cup (B \times C)$
   (b) $A \times (B \cup C) = (A \times B) \cup (A \times C)$
   (c) $(A \cup B) \times (C \cup D) =$
   $(A \times C) \cup (B \times C) \cup (A \times D) \cup (B \times D)$
   (d) $(A \setminus B) \times C = (A \times C) \setminus (B \times C)$
   (e) $A \times (B \setminus C) = (A \times B) \setminus (A \times C)$
   (f) если $A \subseteq C$ и $B \subseteq D$, то
$$A \times B = (A \times D) \cap (C \times B)$$
5. Доказать, что если множества A, B, C, D удовлетворяют соотношению
$$(A \times B) \cup (B \times A) = C \times D$$
   то $A = B = C = D$

6.5.2 Бинарные отношения

1. Доказать, что для любых бинарных отношений
   (a) $(R^{-1})^{-1} = R$
   (b) $(R_1 \cap R_2)^{-1} = (R_1^{-1}) \cap (R_2^{-1})$
   (c) $(R_1 \cup R_2)^{-1} = (R_1^{-1}) \cup (R_2^{-1})$
   (d) $\overline{R^{-1}} = (\overline{R})^{-1}$
2. Доказать, что для любых бинарных отношений
   (a) $R_1 \circ (R_2 \circ R_3) = (R_1 \circ R_2) \circ R_3$
   (b) $(R_1 \circ R_2)^{-1} = R_2^{-1} \circ R_1^{-1}$
   (c) $(R_1 \cup R_2) \circ R_3 = (R_1 \circ R_3) \cup (R_2 \circ R_3)$
   (d) $R_1 \circ (R_2 \cup R_3) = (R_1 \circ R_2) \cup (R_1 \circ R_3)$
   (e) $(R_1 \cap R_2) \circ R_3 \subseteq (R_1 \circ R_3) \cap (R_2 \circ R_3)$
   (f) $R_1 \circ (R_2 \cap R_3) \subseteq (R_1 \circ R_2) \cap (R_1 \circ R_3)$
3. Построить пример бинарных отношений R_1, R_2, R_3, таких что
$$(R_1 \cap R_2) \circ R_3 \neq (R_1 \circ R_3) \cap (R_2 \circ R_3)$$
4. Доказать, что если $R_1 \subseteq R_2$, то
   (a) $R \circ R_1 \subseteq R \circ R_2$
   (b) $R_1 \circ R \subseteq R_2 \circ R$
   (c) $R_1^{-1} \subseteq R_2^{-1}$
5. Пусть символы R_1 и R_2 обозначают бинарные отношения на множестве $\mathbf{N} = \{0, 1, 2, 3, \ldots\}$ всех натуральных чисел, определяемые следующим образом:
$$R_1 \stackrel{\text{def}}{=} \{(a, b) \mid a, b \in \mathbf{N}, \quad a < b\}$$
$$R_2 \stackrel{\text{def}}{=} \{(a, b) \mid a, b \in \mathbf{N}, \quad a \leq b\}$$
   Доказать, что

(a) $R_1 \circ R_1 \neq R_1$

(b) $R_2 \circ R_1 = R_1$

(c) $R_2 \circ R_2^{-1} = \mathbf{N}^2$

6. Доказать, что если отношения R_1 и R_2 рефлексивны, то рефлексивны отношения

$$R_1 \cup R_2, \quad R_1 \cap R_2, \quad R_1^{-1}, \quad R_1 \circ R_2$$

7. Доказать, что если отношения R_1 и R_2 иррефлексивны, то иррефлексивны отношения

$$R_1 \cup R_2, \quad R_1 \cap R_2, \quad R_1^{-1}$$

Показать, что произведение $R_1 \circ R_2$ иррефлексивных отношений может не быть иррефлексивным.

8. Доказать, что если отношения R_1 и R_2 симметричны, то симметричны отношения

$$R_1 \cup R_2, \quad R_1 \cap R_2, \quad R_1^{-1}, \quad R_1 \circ R_1^{-1}$$

9. Доказать, что произведение $R_1 \circ R_2$ симметричных отношений R_1 и R_2 является симметричным тогда и только тогда когда

$$R_1 \circ R_2 = R_2 \circ R_1$$

10. Пусть R_1 и R_2 – антисимметричные отношения на множестве A.

Доказать, что

(a) отношения $R_1 \cap R_2$ и R_1^{-1} антисимметричны

(b) отношение $R_1 \cup R_2$ является антисимметричным тогда и только тогда когда

$$R_1 \circ R_2^{-1} \subseteq id_A$$

11. Построить бинарное отношение, которое

(a) рефлексивно, симметрично, не транзитивно

(b) рефлексивно, антисимметрично, не транзитивно

(c) рефлексивно, не симметрично, транзитивно

(d) не рефлексивно, антисимметрично, транзитивно

(e) не рефлексивно, симметрично, транзитивно

12. Доказать, что если отношение R одновременно симметрично и антисимметрично, то оно транзитивно.

6.5.3 Эквивалентности

1. Пусть n – некоторое положительное целое число, и R – бинарное отношение на множестве $\mathbf{Z}$ всех целых чисел, определяемое следующим образом:

$$R \stackrel{\text{def}}{=} \{(a,b) \mid a-b \ \text{ делится на } \ n\}$$

Доказать, что R – эквивалентность.

2. Пусть R – бинарное отношение на множестве $\mathbf{Z}^2$ всех пар целых чисел, определяемое следующим образом:

$$R \stackrel{\text{def}}{=} \{((a,b),(c,d)) \mid a+d = b+c\}$$

Доказать, что R – эквивалентность.

3. Пусть R – бинарное отношение на множестве $\mathbf{Z}^2$ всех пар целых чисел, определяемое следующим образом:

$$R \stackrel{\text{def}}{=} \left\{ ((a,b),(c,d)) \;\middle|\; \begin{array}{l} ad = bc, \ b \neq 0, \ d \neq 0 \\ \text{или} \\ a = c, \ b = 0, \ d = 0 \end{array} \right\}$$

Доказать, что R – эквивалентность.

4. Пусть A – множество всех прямых на плоскости. Являются ли эквивалентностями следующие отношения R_1 и R_2 на A:

(a) $(a,b) \in R_1 \quad \Leftrightarrow \quad a$ и b параллельны

(b) $(a,b) \in R_2 \quad \Leftrightarrow \quad a$ и b перпендикулярны

5. Пусть R – бинарное отношение на множестве $\mathbf{R}$ всех действительных чисел, определяемое следующим образом:

$$R \stackrel{\text{def}}{=} \{(a,b) \mid a-b \ \text{ – рациональное число}\}$$

Доказать, что R – эквивалентность.

6. Доказать, что если R – эквивалентность, то R^{-1} – тоже эквивалентность.

7. Пусть R – некоторое бинарное отношение на множестве A.

Доказать, что R является эквивалентностью тогда и только тогда, когда

$$(R \circ R^{-1}) \cup id_A = R$$

8. Пусть R_1 и R_2 – эквивалентности на некотором множестве A. Доказать, что

(a) $R_1 \circ R_1 = A^2 \quad \Leftrightarrow \quad R_1 = A^2$

(b) $R_1 \circ R_2 = A^2 \quad \Leftrightarrow \quad R_2 \circ R_1 = A^2$

9. Пусть $f : A \to B$ – произвольная функция. Определим отношение R на множестве A следующим образом:

$$R \stackrel{\text{def}}{=} \{(a_1, a_2) \mid f(a_1) = f(a_2)\}$$

Доказать, что R – эквивалентность.

10. Пусть R_1 и R_2 – эквивалентность на некотором множестве A.

Доказать, что

(a) $R_1 \cap R_2$ тоже является эквивалентностью

(b) $R_1 \cup R_2$ является эквивалентностью тогда и только тогда, когда

$$R_1 \cup R_2 = R_1 \circ R_2$$

(c) $R_1 \circ R_2$ является эквивалентностью тогда и только тогда, когда

$$R_1 \circ R_2 = R_2 \circ R_1$$

(d) если $R_1 \circ R_2 = R_2 \circ R_1$, то

$$R_1 + R_2 = R_1 \circ R_2$$

где $R_1 + R_2$ – это наименьшая эквивалентность, содержащая R_1 и R_2.

11. Пусть $p_0, p_1, p_2, \ldots$ – последовательность натуральных чисел, определяемая индуктивно следующим образом:

(a) $p_0 \stackrel{\text{def}}{=} 1$

(b) $p_{n+1} \stackrel{\text{def}}{=} \sum\limits_{i=0}^{n} C_n^i p_i$

Доказать, что для каждого $n \geq 1$ число p_n равно числу отношений эквивалентности на множестве из n элементов.

6.5.4 Частичные порядки

1. Доказать, что если R – частичный порядок, то R^{-1} тоже частичный порядок.

2. Доказать, что если R_1 и R_2 – частичные порядки на множестве A, то $R_1 \cap R_2$ тоже частичный порядок на множестве A.

3. Доказать, что отношения включения $\subseteq$ на множестве всех подмножеств некоторого множества является частичным порядком.

4. Пусть R – бинарное отношение на множестве $\mathbf{N} = \{0, 1, 2, 3, \ldots\}$ всех натуральных чисел, определяемые следующим образом:

$$R \stackrel{\text{def}}{=} \{(a, b) \mid a, b \in \mathbf{N}, \quad a \text{ делится на } b\}$$

(мы считаем, что 0 делится на 0).

Доказать, что R – частичный порядок.

5. Доказать, что всякое частично упорядоченное множество содержит

(a) не более одного наибольшего элемента и

(b) не более одного наименьшего элемента.

6. Доказать, что

(a) наибольший элемент частично упорядоченного множества (если он существует) является единственным максимальным элементом этого множества, и

(b) наименьший элемент частично упорядоченного множества (если он существует) является единственным минимальным элементом этого множества.

7. Построить пример частично упорядоченного множества, имеющего ровно один минимальный элемент, но не имеющего наименьшего элемента.

8. Доказать, что отношение R на множестве A является квазипорядком тогда и только тогда, когда

$$R = (R \circ R) \cup id_A$$

9. Пусть R – квазипорядок на A.

- Определим отношение Q на A следующим образом:
$$Q \stackrel{\text{def}}{=} R \cap R^{-1}$$
Доказать, что Q – эквивалентность на A.

- Определим отношение S на фактор-множестве A/Q (где $Q = R \cap R^{-1}$) следующим образом:
$$S \stackrel{\text{def}}{=} \{([a_1], [a_2]) \mid (a_1, a_2) \in R\}$$
Доказать, что S – частичный порядок.

10. Доказать, что если R – частичный (линейный, полный) порядок на множестве A, и $B \subseteq A$, то $R \cap B^2$ есть частичный (линейный, полный) порядок на множестве B.

11. Пусть $\leq$ – частичный порядок на A. Доказать, что отношение

$$< \quad \stackrel{\text{def}}{=} \{(a_1, a_2) \in A^2 \mid a_1 \leq a_2 \text{ и } a_1 \neq a_2\}$$

иррефлексивно и транзитивно.

12. Доказать, что если некоторое отношение $<$ на A иррефлексивно и транзитивно, то отношение

$$\leq \quad \stackrel{\text{def}}{=} \{(a_1, a_2) \in A^2 \mid a_1 < a_2 \text{ или } a_1 = a_2\}$$

есть частичный порядок на A.

13. Показать, что если A и B – частично упорядоченные множества, и $f : A \to B$ – монотонная функция, являющаяся биекцией, то f^{-1} может не быть монотонной.

14. Доказать, что для каждого частичного порядка R на конечном множестве A существует линейный порядок Q на множестве A, такой что $R \subseteq Q$.

6.5.5 Функции

1. Если функция gf – инъективная, то функция f – инъективная.

2. Если функция gf – сюръективная, то функция g – сюръективная.

3. Доказать, что существует биективная функция

   (a) из $A \times B$ в $B \times A$

   (b) из $A \times (B \times C)$ в $(A \times B) \times C$

   (c) из $(A \times B)^C$ в $(A^C) \times (B^C)$

   (d) из $(A^B)^C$ в $A^{(B\times C)}$

   (e) из $A^{B\cup C}$ в $(A^B) \times (A^C)$, если $B \cap C = \emptyset$.

4. Пусть задана функция $f : A \to B$. Обозначим символом R_f следующее бинарное отношение:

$$R_f \stackrel{\text{def}}{=} \{(a, f(a)) \mid a \in A\} \ \subseteq A \times B.$$

   Доказать, что функция f является

   - инъективной тогда и только тогда, когда

$$R_f \circ R_f^{-1} = id_A$$

   - сюръективной тогда и только тогда, когда

$$R_f^{-1} \circ R_f = id_B$$

5. Доказать, что для любой функции $f : A \to B$ и любой пары подмножеств $A_1, A_2 \subseteq A$

   (a) если $A_1 \subseteq A_2$, то $f(A_1) \subseteq f(A_2)$

   (b) $f(A_1 \cup A_2) = f(A_1) \cup f(A_2)$

   (c) $f(A_1 \cap A_2) \subseteq f(A_1) \cap f(A_2)$

   (d) $f(A_1) \setminus f(A_2) \subseteq f(A_1 \setminus A_2)$

   (e) если f – инъективна, то

      - $f(A_1 \cap A_2) = f(A_1) \cap f(A_2)$
      - $f(A_1) \setminus f(A_2) = f(A_1 \setminus A_2)$

6. Построить пример функции $f : A \to B$ и подмножеств $A_1, A_2 \subseteq A$, таких, что

$$f(A_1 \cap A_2) \neq f(A_1) \cap f(A_2)$$

7. Доказать, что для любой функции $f : A \to B$ и любой пары подмножеств $B_1, B_2 \subseteq B$

   (a) если $B_1 \subseteq B_2$, то $f^{-1}(B_1) \subseteq f^{-1}(B_2)$

   (b) $f^{-1}(B_1 \cup B_2) = f^{-1}(B_1) \cup f^{-1}(B_2)$

   (c) $f^{-1}(B_1 \cap B_2) = f^{-1}(B_1) \cap f^{-1}(B_2)$

   (d) $f^{-1}(B_1 \setminus B_2) = f^{-1}(B_1) \setminus f^{-1}(B_2)$

8. Доказать, что для любой функции $f : A \to B$ и любого подмножества $B' \subseteq B$

$$f^{-1}(B') = \emptyset \quad \Leftrightarrow \quad B' \cap Im(f) = \emptyset$$

9. Доказать, что для каждой функции $f : A \to B$ и каждой пары подмножеств $A' \subseteq A$, $B' \subseteq Im(f)$,

   (a) $A' \subseteq f^{-1}(f(A'))$

   (b) $f(f^{-1}(B')) = B'$

   (c) $f(A') \cap B' = f(A' \cap f^{-1}(B'))$

   (d) $f(A') \cap B' = \emptyset \quad \Leftrightarrow \quad A' \cap f^{-1}(B') = \emptyset$

   (e) $f(A') \subseteq B' \quad \Leftrightarrow \quad A' \subseteq f^{-1}(B')$

Лекция 7

Основные результаты теории множеств

7.1 Мощность множества

Для произвольного конечного множества A число $|A|$ его элементов называется **мощностью** множества A.

Пусть задана пара конечных множеств A, B.

Нетрудно доказать, что

1. $|A| \leq |B|$ тогда и только тогда, когда существует инъективное отображение $f : A \to B$
2. $|A| \geq |B|$ тогда и только тогда, когда существует сюръективное отображение $f : A \to B$.

Отсюда в частности следует, что $|A| = |B|$ тогда и только тогда, когда существует биективное отображение $f : A \to B$.

Понятие мощности можно обобщить на все множества. Для произвольного множества A его мощность обозначается символом $|A|$.

Отношение сравнения мощностей определяется следующим образом: для произвольной пары A, B множеств

1. $|A| \leq |B|$ тогда и только тогда, когда существует инъективное отображение $f : A \to B$
2. $|A| \geq |B|$ тогда и только тогда, когда существует сюръективное отображение $f : A \to B$
3. $|A| = |B|$ тогда и только тогда, когда существует биективное отображение $f : A \to B$

Знакосочетание

$$|A| < |B| \tag{7.1}$$

означает, что

$$|A| \leq |B| \quad \text{и} \quad |A| \neq |B|$$

Можно доказать, что для каждой пары множеств A, B верно одно и только одно из соотношений:

$$|A| < |B|, \quad |A| = |B|, \quad |B| < |A|.$$

7.2 Теорема Кантора

Теорема Кантора утверждает, что для каждого множества A имеет место соотношение

$$|A| < |\mathbf{2}^A| \tag{7.2}$$

Доказательство.

Поскольку существует инъективное отображение f вида

$$A \xrightarrow{f} \mathbf{2}^A \tag{7.3}$$

которое сопоставляет каждому $a \in A$ одноэлементное подмножество

$$\{a\} \in \mathbf{2}^A$$

то, следовательно, имеет место соотношение

$$|A| \leq |\mathbf{2}^A|$$

Следовательно, для доказательства неравенства (7.2) достаточно доказать, что

$$|A| \neq |\mathbf{2}^A| \tag{7.4}$$

Предположим, что (11.7) неверно, т.е.

$$|A| = |\mathbf{2}^A| \tag{7.5}$$

Согласно определению равенства мощностей, соотношение (7.5) эквивалентно существованию биективного отображения f вида (7.3).

Для каждого элемента $a \in A$ верно одно и только одно из следующих двух соотношений

$$a \in f(a) \tag{7.6}$$

$$a \notin f(a) \tag{7.7}$$

Обозначим символом B совокупность всех элементов множества A, для которых имеет место соотношение (7.7).

B является подмножеством множества A, т.е.

$$B \in \mathbf{2}^A$$

Поскольку отображение f является биективным, то оно в частности сюръективно, т.е. существует элемент b множества A, такой, что

$$f(b) = B$$

Элемент b и подмножество $B \subseteq A$ удовлетворяют одному и только одному из следующих соотношений:

$$b \in B \tag{7.8}$$

$$b \notin B \tag{7.9}$$

1. Если верно (7.8), то из определения подмножества B следует, что
$$b \notin f(b)$$
т.е.
$$b \notin B$$

2. Если верно (7.9), то из определения подмножества B следует, что
$$b \in f(b)$$
т.е.
$$b \in B$$

В обоих случаях получаем противоречие.

Таким образом, наше предположение о том, что существует биективное отображение f вида (7.3), является ошибочным.

Следовательно, имеет место соотношение (11.7).

7.3 Теорема Кантора-Бернштейна

Теорема Кантора–Бернштейна утверждает, что для каждой пары A, B множеств, такой, что

- существует инъективное отображение из A в B и
- существует инъективное отображение из B в A

имеет место соотношение

$$|A| = |B| \tag{7.10}$$

Доказательство: ...

Данную теорему можно применить для доказательства того, что мощность множества точек единичного отрезка
$$[0, 1]$$
равна мощности множества точек единичного квадрата

$$[0, 1] \times [0, 1]$$

Действительно,

- существует инъективное отображение f вида
$$[0, 1] \xrightarrow{f} [0, 1] \times [0, 1] \tag{7.11}$$
которое можно определить так:
$$\text{для каждого } a \in [0, 1] \quad f(a) \stackrel{\text{def}}{=} (a, 0)$$

- существует инъективное отображение g вида
$$[0, 1] \times [0, 1] \xrightarrow{g} [0, 1] \tag{7.12}$$
которое можно определить так: поскольку каждое действительное число a из отрезка $[0, 1]$ можно представить в виде бесконечной десятичной дроби
$$a \;=\; a_0 \,.\, a_1\, a_2\, a_3\, \ldots$$
где
  - $a_0 = 0$ или 1, и
  - для каждого $i \geq 1$
$$a_i \in \{0, \ldots, 9\}$$

то каждую точку квадрата $[0, 1] \times [0, 1]$, т.е. пару
$$(a, b) \in [0, 1] \times [0, 1]$$
можно представить парой десятичных дробей
$$(a_0 \,.\, a_1\, a_2\, a_3\, \ldots, \quad b_0 \,.\, b_1\, b_2\, b_3\, \ldots) \tag{7.13}$$

Определим отображение g следующим образом: для каждой пары (7.13) её образ относительно g равен дроби
$$0 \,.\, a_0\, b_0\, a_1\, b_1\, a_2\, b_2\, a_3\, b_3\, \ldots$$

Нетрудно доказать, что отображение g инъективно.

7.4 Аксиома выбора и лемма Цорна

7.5 Теорема Цермело

7.6 Трихотомия кардинальных чисел

7.7 Трансфинитная индукция

Лекция 8

Логика предикатов

8.1 Выражения

8.1.1 Типы

Мы предполагаем, что задано множество Types **типов**. С каждым типом $\tau \in$ Types может быть связано некоторое множество $\mathcal{D}_\tau$ **значений** данного типа, но эта связь нефиксирована, т.е. в разных ситуациях с одним и тем же типом могут быть связаны разные множества значений.

Например, Types может содержать тип `int`, и

- в одной ситуации с данным типом связывается множество всех целых чисел,
- а в другой ситуации - множество целых чисел в диапазоне от -32767 до $+32767$.

8.1.2 Переменные, константы, функциональные символы, предикаты

Предполагается, что заданы

- множество Var **переменных**, причём каждой переменной $x \in Var$ сопоставлен тип $\tau(x) \in$ Types,
- множество Con **констант**, и каждой константе $c \in Con$ сопоставлен тип $\tau(c) \in$ Types,
- множество Fun, элементы которого называются **функциональными символами**, причём каждому $f \in Fun$ сопоставлен тип
$$\tau(f) \;=\; (\tau_1, \ldots, \tau_n) \to \tau \qquad (8.1)$$
где $\tau_1, \ldots, \tau_n, \tau \in$ Types.
- множество Rel, элементы которого называются **предикатами**, причём каждому $R \in Rel$ сопоставлен тип
$$\tau(R) \;=\; (\tau_1, \ldots, \tau_n) \qquad (8.2)$$
где $\tau_1, \ldots, \tau_n \in$ Types.

8.1.3 Интерпретации

Интерпретацией называется соответствие I, сопоставляющее

- каждому типу $\tau \in$ Types – множество $\mathcal{D}^I_\tau$ **значений** типа τ
(совокупность всех значений всех типов обозначается символом $\mathcal{D}^I$ и называется **областью** интерпретации I)
- каждой константе $c \in Con$ – некоторое значение $c^I \in \mathcal{D}^I$ типа $\tau(c)$
- каждому функциональному символу f типа (8.1) – некоторую функцию f^I вида
$$f^I: \;\mathcal{D}^I_{\tau_1} \times \ldots \times \mathcal{D}^I_{\tau_n} \to \mathcal{D}^I_\tau$$
- каждому предикату R типа (8.2) – некоторую функцию R^I вида
$$R^I: \;\mathcal{D}^I_{\tau_1} \times \ldots \times \mathcal{D}^I_{\tau_n} \to \{0, 1\}$$

Ниже в этой главе символ I обозначает некоторую фиксированную интерпретацию.

8.1.4 Выражения

Выражения строятся из переменных, констант и функциональных символов. Каждому выражению e сопоставляется некоторый тип $\tau(e)$. Множество выражений обозначается символом $Expr$ и определяется следующим образом.

1. Каждая переменная $x \in Var$ является выражением типа $\tau(x)$.
2. Каждая константа $c \in Con$ является выражением типа $\tau(c)$.
3. Для каждого функционального символа f типа (8.1), и каждого списка выражений $e_1, \ldots, e_n$, такого, что $\tau(e_1) = \tau_1, \ldots, \tau(e_n) = \tau_n$, знакосочетание $f(e_1, \ldots, e_n)$ является выражением типа τ.

   Выражения вида $f(e_1, e_2)$ часто записывают в виде $e_1 f e_2$.

Совокупность всех переменных, входящих в выражение e, обозначается символом $Var(e)$.

8.1.5 Подстановки

Подстановкой называется знакосочетание θ вида

$$\theta \;=\; [x_1 := e_1, \dots, x_k := e_k] \tag{8.3}$$

где

- $x_1, \dots, x_k$ – список различных переменных, и
- $e_1, \dots, e_k$ – список выражений, причём для каждого $i = 1, \dots, k \quad \tau(x_i) = \tau(e_i)$.

Подстановка (8.3) индуцирует функцию вида

$$\theta : Expr \to Expr \tag{8.4}$$

обозначаемую тем же символом θ, и определяемую следующим образом: для каждого выражения $e \in Expr$ выражение $\theta(e)$ получается из e заменой для каждого $i \in \{1, \dots, k\}$ каждого вхождения переменной x_i в e на выражение e_i. Мы будем отождествлять подстановку (8.3) с соответствующей ей функцией (8.4).

Композицией подстановок θ_1 и θ_2 называется подстановка $\theta_1\theta_2$, которая действует на каждое выражение $e \in Expr$ следующим образом:

$$(\theta_1\theta_2)(e) \stackrel{\text{def}}{=} \theta_1(\theta_2(e))$$

8.1.6 Означивания

Пусть X – некоторое множество переменных из Var.

Означиванием переменных из X называется функция $\xi : X \to \mathcal{D}^I$, которая сопоставляет каждой переменной $x \in X$ некоторое значение $\xi(x) \in \mathcal{D}^I$ типа $\tau(x)$.

Для каждого выражения e, такого, что $Var(e) \subseteq X$, **значение** $\xi(e)$ выражения e на означивании ξ определяется рекурсивно следующим образом:

- если $e = x \in X$, то $\xi(e)$ уже определено
- если $e = c \in Con$, то $\xi(e) \stackrel{\text{def}}{=} c^I$
- если $e = f(e_1, \dots, e_k)$ то

$$\xi(e) \stackrel{\text{def}}{=} f^I(\xi(e_1), \dots, \xi(e_k))$$

Выражения e_1 и e_2 называются **эквивалентными**, если для каждого означивания ξ входящих в них переменных имеет место равенство

$$\xi(e_1) = \xi(e_2)$$

Знакосочетание $e_1 = e_2$ выражает тот факт, что e_1 и e_2 эквивалентны.

Для каждого означивания $\xi : X \to \mathcal{D}^I$, каждой переменной $x \in X$ и каждого значения $d \in \mathcal{D}^I_{\tau(x)}$ знакосочетание $\xi[x := d]$ обозначает означивание переменных из X, которое отличается от ξ только значением на x:

$$\forall y \in X \qquad \xi[x := d](y) \stackrel{\text{def}}{=} \begin{cases} \xi(y), & \text{если } y \neq x \\ d, & \text{если } y = x \end{cases}$$

8.2 Формулы логики предикатов

8.2.1 Понятие формулы

Формулы логики предикатов (ЛП) (называемые ниже просто **формулами**) – это знакосочетания, определяемые следующим образом.

1. Для
   - каждого предиката R типа (8.2), и
   - каждого списка выражений $e_1, \dots, e_n$, такого, что $\tau(e_1) = \tau_1, \dots, \tau(e_n) = \tau_n$

   знакосочетание $R(e_1, \dots, e_n)$ является формулой. Формулы такого вида называются **атомарными**.

   Формулы вида $R(e_1, e_2)$ часто записывают в виде $e_1 R e_2$.

2. Если A и B – формулы, то знакосочетания

   $$\overline{A}, \quad A \wedge B, \quad A \vee B, \quad A \to B, \quad A \leftrightarrow B$$

   являются формулами.

3. Если A – формула, и x – переменная, то знакосочетания $\forall x\ A$ и $\exists x\ A$ являются формулами.

   Знакосочетание $\forall x$ называется **квантором всеобщности**, а $\exists x$ – **квантором существования**.

   Формула A, входящая в формулы $\exists x A$ и $\forall x A$, называется **областью действия** кванторов, находящихся в начале данных формул.

Совокупность всех переменных, входящих в формулу A, обозначается символом $Var(A)$.

Для каждой формулы A формула $\neg A$ может также обозначаться символом $\overline{A}$.

Для произвольного списка $A_1, \dots, A_k$ формул знакосочетания

$$A_1 \wedge A_2 \wedge \ldots \wedge A_k \;\text{ и }\; A_1 \vee A_2 \vee \ldots \vee A_k$$

являются сокращённой записью формул

$$A_1 \wedge (A_2 \wedge (\ldots \wedge A_n)\ldots) \;\text{ и }\; A_1 \vee (A_2 \vee (\ldots \vee A_n)\ldots)$$

соответственно. Данные формулы также будут обозначаться знакосочетаниями

$$\left\{ \begin{array}{c} A_1 \\ \ldots \\ A_k \end{array} \right\} \quad \text{и} \quad \left[\begin{array}{c} A_1 \\ \ldots \\ A_k \end{array} \right]$$

соответственно.

В формулах ЛП можно опускать скобки, аналогично тому, как это делалось в формулах ЛВ. При восстановлении скобок используются те же правила, что и в пункте 2.1.4, и кроме того, предполагается что кванторы связывают сильнее отрицаний, т.е. при восстановлении скобок в первую очередь рассматриваются все вхождения кванторов, и для каждого квантора ищется минимальное знакосочетание справа от него, являющееся формулой.

8.2.2 Значения формул ЛП

Пусть задано некоторое означивание $\xi : X \to \mathcal{D}^I$.

Для каждой формулы A, такой, что $Var(A) \subseteq X$, **значение** $\xi(A) \in \{0,1\}$ формулы A на означивании ξ определяется рекурсивно следующим образом.

1. Если $A = R(e_1, \ldots, e_n)$ – атомарная формула, то
$$\xi(A) \stackrel{\text{def}}{=} R^I(\xi(e_1), \ldots, \xi(e_n))$$
2. $\xi(\overline{A}) \stackrel{\text{def}}{=} \overline{\xi(A)}$
3. $\xi(A \wedge B) \stackrel{\text{def}}{=} \xi(A) \wedge \xi(B)$
4. $\xi(A \vee B) \stackrel{\text{def}}{=} \xi(A) \vee \xi(B)$
5. $\xi(A \to B) = 1$, если $\xi(A) \leq \xi(B)$
6. $\xi(A \leftrightarrow B) = 1$, если $\xi(A) = \xi(B)$
7. $\xi(\forall x\ A) = 1$, если для любого $d \in \mathcal{D}^I_{\tau(x)}$ имеет место равенство $(\xi[x := d])(A) = 1$
8. $\xi(\exists x\ A) = 1$, если существует значение $d \in \mathcal{D}^I_{\tau(x)}$, для которого $(\xi[x := d])(A) = 1$

Если $\xi(A) = 1$, то A называется **истинной** на означивании ξ, иначе A называется **ложной** на ξ.

Если для каждого означивания $\xi : X \to \mathcal{D}^I$ имеет место равенство $\xi(A) = 1$, то A называется **истинной в интерпретации** I.

Формула A называется

- **тавтологией**, если она истинна в любой интерпретации
- **выполнимой**, если она истинна в некоторой интерпретации на некотором означивании.

8.2.3 Примеры формул

Формулы могут выражать суждения, например:

1. ассоциативность сложения:
$$\forall x\ \forall y\ \forall z\ (x + (y + z) = (x + y) + z)$$
2. дистрибутивность умножения относительно сложения:
$$\forall x\ \forall y\ \forall z\ (x \cdot (y + z) = (x \cdot y) + (x \cdot z))$$
3. рефлексивность равенства: $\forall x\ (x = x)$
4. симметричность равенства:
$$\forall x\ \forall y\ ((x = y) \to (y = x))$$
5. транзитивность равенства:
$$\forall x\ \forall y\ \forall z\ ((x = y) \wedge (y = z) \to (x = z))$$

В этих формулах используется предикат $=$ и функциональные символы $+$ и $\cdot$.

8.2.4 Свободные и связанные вхождения переменных в формулы

Пусть A – некоторая формула, и x – некоторая переменная, входящая в A.

Переменная x может входить в A несколько раз. Например, если A имеет вид
$$\forall y\ (R(x, y) \to \forall x\ Q(x))$$
то x имеет три вхождения в A.

Каждое вхождение переменной x в A является либо **свободным**, либо **связанным**.

Вхождение переменной x в A называется

- **связанным**, если это вхождение содержится в некоторой подформуле вида $\forall x\ B$ или $\exists x\ B$, и
- **свободным** – если данное вхождение не является связанным.

Например, рассмотрим следующие формулы:

$$R(x, y) \tag{8.5}$$
$$R(x, y) \to \forall x\ S(x) \tag{8.6}$$
$$\forall x\ (R(x, y) \to \forall x\ R(x)) \tag{8.7}$$

1. Вхождение переменной x в (8.5) свободно.
2. Первое вхождение переменной x в (8.6) свободно, а второе и третье – связанные.
3. Все вхождения x в (8.7) являются связанными.
4. Каждое вхождение переменной y во всех трёх формулах свободно.

Одна и та же переменная может иметь как свободные, так и связанные вхождения в одну и ту же формулу, как это имеет место например в (8.6).

Вхождение переменной в формуле A может быть

- связанным в A, и в то же время
- свободным в некоторой подформуле формулы A.

Так, например, первое вхождение x в формулу (8.6) свободно, но (8.6) является подформулой формулы (8.7), в которой то же вхождение x оказывается связанным.

Совокупность переменных, имеющих хотя бы одно свободное вхождение в формуле A, обозначается символом $FV(A)$. Формула A называется **замкнутой**, если $FV(A) = \emptyset$.

Нетрудно видеть, что значение $\xi(A)$ формулы A на означивании ξ зависит только от значений ξ на переменных из множества $FV(A)$. В частности, если A замкнута, то её значение в интерпретации I является одним и тем же для всех означиваний, т.е. A представляет собой высказывание, которое является истинным или ложным (в интерпретации I). Мы будем обозначать значение этого высказывания символом A^I.

8.3 Отношения, определяемые формулами

Для каждой интерпретации I и каждой формулы A, такой, что множество $FV(A)$ непусто и имеет вид

$$FV(A) = \{x_1, \ldots, x_n\}$$

формула A выражает некоторое свойство n–элементных кортежей значений соответствующих типов, т.е. определяет некоторое подмножество

$$A^I \subseteq \mathcal{D}^I_{\tau(x_1)} \times \ldots \times \mathcal{D}^I_{\tau(x_n)}$$

называемое **отношением**, которое состоит из всех списков $(d_1, \ldots, d_n)$, таких, что A истинна на означивании

$$[x_1 := d_1, \ldots, x_n := d_n]$$

Рассмотрим несколько примеров отношений, определяемых формулами.

1. Пусть в формулах

$$R(x,y) \tag{8.8}$$

$$\forall y\ R(x,y) \tag{8.9}$$

$$\exists x\ \forall y\ R(x,y) \tag{8.10}$$

предикат R имеет тип $(\mathtt{nat}, \mathtt{nat})$, где множество $\mathcal{D}^I_{\mathtt{nat}}$ состоит из всех натуральных чисел, и

$$R^I(d_1, d_2) = 1 \quad \Leftrightarrow \quad d_1 \leq d_2$$

В данном случае

- (8.8) определяет отношение, которое состоит из всех пар (d_1, d_2) натуральных чисел, таких, что $d_1 \leq d_2$
- (8.9) определяет отношение, которое состоит из всех натуральных чисел d_1, обладающих свойством

  для каждого натурального d' $\qquad d_1 \leq d'$

  нетрудно видеть, что данное отношение состоит лишь из числа 1
- (8.10) является истинным высказыванием, утверждающим существование наименьшего натурального числа.

2. Пусть τ обозначает тип, значениями которого являются все люди, а $R(x,y)$ и $S(x,y)$ (где предикаты R и S имеют тип (τ,τ)) интерпретируются соответственно как "x есть брат y" и "x есть родитель y".

   Тогда формула $\exists z\ \ (R(x,z) \wedge S(z,y))$ определяет отношение родства, связывающее дядю и племянника (или племянницу).

3. Формула

$$\left\{ \begin{array}{l} \neg(x = c) \\ \forall y\ (\exists z\ (x = y \cdot z) \to \left[\begin{array}{c} y = x \\ y = c \end{array} \right]) \end{array} \right\} \tag{8.11}$$

   будет определять множество всех простых чисел, если

   - предикат "$=$" типа $(\mathtt{nat}, \mathtt{nat})$, и
   - функциональный символ "$\cdot$" типа

$$(\mathtt{nat}, \mathtt{nat}) \to \mathtt{nat}$$

   интерпретируются как равенство и обычное умножение чисел, а константа c интерпретируется как натуральное число 1.

8.4 Эквивалентность формул

Формулы A_1 и A_2 называются **эквивалентными**, если в произвольной интерпретации I их значения совпадают на каждом означивании входящих в них переменных. Знакосочетание $A_1 \sim A_2$ выражает тот факт, что A_1 и A_2 эквивалентны.

Нетрудно доказать, что $\sim$ – отношение эквивалентности и конгруэнция относительно всех операций на формулах, т.е. если $A_1 \sim A_2$, то

- $\overline{A}_1 \sim \overline{A}_2$
- $A_1 \wedge B \sim A_2 \wedge B, \quad B \wedge A_1 \sim B \wedge A_2$
- $A_1 \vee B \sim A_2 \vee B, \quad B \vee A_1 \sim B \vee A_2$
- $A_1 \to B \sim A_2 \to B, \quad B \to A_1 \sim B \to A_2$
- $A_1 \leftrightarrow B \sim A_2 \leftrightarrow B, \quad B \leftrightarrow A_1 \sim B \leftrightarrow A_2$
- $\forall x\ A_1 \sim \forall x\ A_2, \quad \exists x\ A_1 \sim \exists x\ A_2$

Эти соотношения позволяют доказать **теорему об эквивалентной замене**, которая утверждает, что если

- формула A содержит некоторую подформулу B,
- B эквивалентна некоторой формуле C, и
- формула A' получается из A заменой B на C

то A эквивалентна A'.

Действительно, A и A' можно рассматривать как результат нескольких приписываний слева или справа к B и C одних и тех же знакосочетаний (каждое из которых является либо знаком отрицания, либо формулой со связкой, либо квантором). Согласно приведённым выше соотношениям, каждое приписывание сохраняет отношение эквивалентности между получающимися формулами.

8.5 Задачи

Во всех задачах этой главы предполагается, что типы всех выражений во всех формулах одинаковы.

8.5.1 Формализация предложений естественного языка

Перевести следующие предложения на язык формул.

1. Не все птицы могут летать.
2. Ты можешь обманывать кое-кого всё время, ты можешь обманывать всех некоторое время, но ты не можешь обманывать всех всё время.
3. Ни один политик не честен.
4. Если кто-нибудь может сделать это, то и Петя может.
5. Всякий, в ком есть упорство, может изучить логику.

8.5.2 Свободные и связанные вхождения переменных

Указать свободные и связанные вхождения переменных в следующие формулы

1. $\forall z\ (\forall x\ R(x,y) \to R(z,x))$
2. $\forall y\ R(z,y) \to \forall z\ R(z,y)$
3. $(\forall y\ \exists x\ R(x,y,f(x,y))) \vee \overline{\forall x\ S(y,g(x))}$
4. $\forall x\ (R(x,y) \to \forall y\ Q(y))$
5. $\forall x\ R(x,y) \to \forall y\ Q(x,y)$
6. $\overline{\exists y\ Q(y,y)} \wedge R(f(x,y))$

8.5.3 Выполнимость

1. Выполнимы ли формулы
   (a) $\exists x\ P(x)$
   (b) $\forall x\ P(x)$
   (c) $\exists x\ \forall y\ (Q(x,x) \wedge \overline{Q(x,y)})$
   (d) $\exists x\ \exists y\ (P(x) \wedge \overline{P(y)})$
   (e) $\exists x\ \forall y\ (Q(x,y) \to \forall z\ R(x,y,z))$
   (f) $P(x) \to \forall y\ P(y)$
   (g) $\forall x\ \exists y\ (P(x) \leftrightarrow \overline{P(y)})$
   (h) $\exists y\ \forall x\ (P(x) \leftrightarrow \overline{P(y)})$
   (i) $\exists x\ \forall y\ \exists z\ (R(x) \leftrightarrow\ (S(y) \vee T(z)))$
   (j) $\overline{\forall x\ \left(P(x) \to \forall y\ \left(P(y) \to \begin{bmatrix} Q(x) \to \overline{Q(y)} \\ \forall z\ P(z) \end{bmatrix}\right)\right)}$
   (k) $\forall x\ \exists y\ \overline{\left\{\begin{array}{l} P(y) \\ P(x) \to Q(x) \\ Q(x) \to R(x) \end{array}\right\} \to R(y)}$
   (l) $\forall x\ \exists z\ \forall y\ ((\left\{\begin{array}{l} P(y) \\ Q(z) \end{array}\right\} \to \begin{bmatrix} P(x) \\ R(z) \end{bmatrix}) \to (Q(x) \leftrightarrow \overline{Q(y)}))$
2. Доказать, что формула A выполнима тогда и только тогда, когда выполнима формула $\exists x A$, где x – произвольная переменная.

8.5.4 Тавтологии

1. Являются ли следующие формулы тавтологиями?
   (a) $\exists x\ P(x) \to \forall x\ P(x)$
   (b) $\overline{\exists x\ P(x) \to \forall x\ P(x)}$
   (c) $\exists x\ \forall y\ R(x,y) \to \forall y\ \exists x\ R(x,y)$
   (d) $\forall x\ \exists y\ R(x,y) \to \exists y\ \forall x\ R(x,y)$
   (e) $\exists x\ \forall y\ R(x,y) \to \exists y\ \forall x\ R(x,y)$
   (f) $\forall x\ \forall y\ R(x,y) \to \forall x\ R(x,x)$
   (g) $\exists x\ R(x,x) \to \exists x\ \exists y\ R(x,y)$
   (h) $(\forall x\ A \to \exists x\ B) \leftrightarrow (\exists x\ (A \to B))$
2. Доказать, что следующие формулы являются тавтологиями:
   (a) $\overline{\forall x\ A} \leftrightarrow \exists x\ \overline{A}$
   (b) $\overline{\exists x\ A} \leftrightarrow \forall x\ \overline{A}$
   (c) $\forall x\ (A\ \wedge\ B) \leftrightarrow (\forall x\ A\ \wedge\ \forall x\ B)$
   (d) $\exists x\ (A \vee B) \leftrightarrow (\exists x\ A \vee \exists x\ B)$
   (e) $(\forall x\ A \vee \forall x\ B) \to \forall x\ (A \vee B)$
   (f) $\exists x\ (A\ \wedge\ B) \to (\exists x\ A\ \wedge\ \exists x\ B)$
   (g) $\forall x\ (A \to B) \to (\forall x\ A \to \forall x\ B)$
   (h) $\forall x\ (A \to B) \to (\exists x\ A \to \exists x\ B)$
   (i) $(\forall x\ A \to \forall x\ B) \to \exists x\ (A \to B)$
   (j) $(\exists x\ A \to \exists x\ B) \to \exists x\ (A \to B)$
   (k) $(\exists x\ A \to \forall x\ B) \to \forall x\ (A \to B)$
   (l) $\forall x\ (A \vee B) \to (\exists x\ A \vee \forall x\ B)$
   (m) $\forall x\ (A\ \wedge\ B) \to (\forall x\ A\ \wedge\ \exists x\ B)$
   (n) $\forall x\ \forall y\ A \to \forall y\ \forall x\ A$
   (o) $\exists x\ \exists y\ A \to \exists y\ \exists x\ A$
   (p) $\exists x\ \forall y\ A \to \forall y\ \exists x\ A$
   (q) $(\forall x\ (A \leftrightarrow B)) \to ((\forall x\ A) \leftrightarrow (\forall x\ B))$
   (r) $(\forall x\ (A \leftrightarrow B)) \to ((\exists x\ A) \leftrightarrow (\exists x\ B))$
   (s) $(\exists x\ \left\{\begin{array}{l} A \\ B \to C \end{array}\right\}) \to (\forall x\ (A \to \overline{C}) \to \overline{B})$
   где x не входит в формулу B
   (t) $(\forall x\ (A \to \overline{B})) \to \overline{\exists x\ A\ \wedge\ \forall x\ B}$
   (u) $(\forall x\ (A \to \overline{B})) \to \overline{\forall x\ A\ \wedge\ \exists x\ B}$

3. Доказать, что следующие формулы не являются тавтологиями.

   (a) $(\exists x\ A\ \wedge\ \exists x\ B) \to \exists x\ (A \wedge B)$

   (b) $\forall x\ (A \vee B) \to (\forall x\ A \vee \forall x\ B)$

   (c) $(\forall x\ A \to \forall x\ B) \to \forall x\ (A \to B)$

   (d) $\forall y\ \exists x\ R(x,y) \to \exists x\ \forall y\ R(x,y)$

   (e) $\exists x\ \forall y\ (\left\{ \dfrac{R(x,y)}{R(y,x)} \right\} \to (R(x,x) \leftrightarrow R(y,y)))$

   (f) $\left\{ \begin{array}{l} \forall x\ \forall y\ \forall z\ (\left\{ \begin{array}{l} R(x,y) \\ R(y,z) \end{array} \right\} \to R(x,z)) \\ \forall x\ \overline{R(x,x)} \end{array} \right\} \to$
   $\to \exists x\ \forall y\ \overline{R(x,y)}$

   (g) $\forall x\ \forall y\ \forall z \left\{ \begin{array}{l} R(x,x) \\ R(x,z) \to \left[\begin{array}{l} R(x,y) \\ R(y,z) \end{array} \right] \end{array} \right\} \to$
   $\to \exists y\ \forall z\ R(y,z)$

4. Доказать, что A – тавтология тогда и только тогда, когда $\forall x A$ – тавтология.

5. Пусть каждая переменная выражения e не имеет связанных вхождений в формулу A. Доказать, что следующие формулы являются тавтологиями:

   (a) $\forall x\ A \to [x := e]A$

   (b) $[x := e]A \to \exists x\ A$

6. Пусть формула A не содержит кванторов.

   Доказать, что A является тавтологией тогда и только тогда, когда A имеет вид $\theta(B)$, где B – некоторая тавтология ЛВ, и θ – некоторая подстановка.

8.5.5 Истинность формул в интерпретациях

1. Рассмотрим следующие формулы

   - $R(f(x,y),a)$
   - $R(x,y) \to R(y,x)$
   - $\forall x\ \forall y\ \forall z\ (R(x,y) \to (R(y,z) \to R(x,z)))$

   Для следующих интерпретаций и для каждой из этих формул указать, при каких означиваниях свободных переменных эти формулы истинны.

   (a) В качестве области берётся множество всех натуральных чисел, $R(y,z)$, $f(y,z)$ и a интерпретируются соответственно как

   $$y \geq z, \quad y \cdot z, \quad 1$$

   (b) В качестве области берётся множество $\mathbf{2}^A$, где A – некоторое множество, $R(y,z)$, $f(y,z)$ и a интерпретируются соответственно как

   $$y \supseteq z, \quad y \cup z, \quad \emptyset$$

2. Написать формулу с одноаргументными предикатами, истинную лишь в таких интерпретациях, область которых содержит не менее 5 элементов.

3. Доказать, что формула

   $$\exists x\ \forall y\ (\left\{ \dfrac{R(x,y)}{R(y,x)} \right\} \to (R(x,x) \leftrightarrow R(y,y)))$$

   истинна в любой интерпретации, область которой состоит не более чем из трёх элементов

4. Доказать, что следующая формула истинна во всякой интерпретации с конечной областью, но ложна в некоторой интерпретации с бесконечной областью:

   $$\forall x\ \forall y\ \forall z\ \left\{ \begin{array}{l} R(x,x) \\ (R(x,y) \wedge R(y,z)) \to R(x,z) \\ R(x,y) \vee R(y,x) \end{array} \right\} \to$$
   $$\to\ \exists y\ \forall x\ R(y,x)$$

5. Доказать, что формула

   $$\left\{ \begin{array}{l} \forall x\ \exists y\ P(x,y) \\ \forall x\ \forall y\ (P(x,y) \to \overline{P(y,x)}) \\ \forall x\ \forall y\ \forall z\ \big((P(x,y) \wedge P(y,z)) \to P(x,z)\big) \end{array} \right\}$$

   истинна в некоторой интерпретации с бесконечной областью и ложна во всех интерпретациях с конечной областью.

6. Доказать, что следующие формулы истинны во всякой интерпретации с конечной областью, но не являются тавтологиями:

   (a) $\exists x\ \forall y\ \exists z\ \Big(\left\{ \begin{array}{l} R(y,z) \to R(x,z) \\ R(x,x) \end{array} \right\} \to R(y,x) \Big)$

   (b) $\forall x\ \forall y\ \forall z \left\{ \begin{array}{l} R(x,x) \\ R(x,z) \to \left[\begin{array}{l} R(x,y) \\ R(y,z) \end{array} \right] \end{array} \right\} \to$
   $\to \exists y\ \forall z\ R(y,z)$

7. Найти интерпретацию, в которой истинна формула $\exists x\ \exists y\ R(x,y)$ и ложна формула $\forall x\ \exists y\ R(x,y)$.

8.5.6 Свойства, выражаемые формулами

1. Пусть I – интерпретация, областью которой является множество натуральных чисел, и предикаты R и S интерпретируются следующим образом:

   - $R(x,y,z) = 1 \quad \Leftrightarrow \quad x + y = z$
   - $S(x,y,z) = 1 \quad \Leftrightarrow \quad x \cdot y = z$

   (a) Написать формулу с одной свободной переменной x, которая будет истинна в I тогда и только тогда когда

i. $x = 0$
ii. $x = 1$
iii. $x = 2$
iv. x – чётно
v. x – нечётно
vi. x – простое число

(b) Написать формулу с двумя свободными переменными x и y, истинную в I тогда и только тогда когда

i. $x = y$
ii. $x \leq y$
iii. $x < y$
iv. x делит y
v. x и y являются простыми числами-близнецами

(c) Написать формулу с тремя свободными переменными x, y и z, истинную в I тогда и только тогда когда

i. z – наименьшее общее кратное x и y
ii. z – наибольший общий делитель x и y

(d) Написать формулы, выражающие в интерпретации I следующие свойства:

i. коммутативность сложения
ii. ассоциативность сложения
iii. коммутативность умножения
iv. ассоциативность умножения
v. дистрибутивность сложения относительно умножения
vi. бесконечность множества простых чисел
vii. утверждение о том, что каждое число есть сумма четырёх квадратов
viii. утверждение о том, что для каждой пары отличных от нуля чисел существуют наибольший общий делитель и наименьшее общее кратное

(e) Наисать формулу, выражающую в интерпретации I

i. утверждение о том, что простых чисел-близнецов - бесконечно много
ii. всякое чётное число, большее 2, есть сумма двух простых

(f) Написать формулу, выражающую в интерпретации I утверждение о том, что уравнение $3x^2 + 2x + 1 = 0$ имеет в точности два различных корня.

(g) Написать формулу, выражающую в интерпретации I утверждение о том, что система уравнений

$$\begin{cases} 3x - y = 0 \\ x + y = 1 \end{cases}$$

не имеет решения.

2. Пусть I – интерпретация, областью которой является множество всех точек, прямых и плоскостей 3-мерного евклидова пространства, и предикаты `Точка`, `Прямая`, `Плоскость` и `Лежит` интерпретируются следующим образом:

$$\begin{array}{lcl} \texttt{Точка}(x) = 1 & \Leftrightarrow & x \text{ – точка} \\ \texttt{Прямая}(x) = 1 & \Leftrightarrow & x \text{ – прямая} \\ \texttt{Плоскость}(x) = 1 & \Leftrightarrow & x \text{ – плоскость} \\ \texttt{Лежит}(x, y) = 1 & \Leftrightarrow & x \text{ лежит на } y \end{array}$$

Написать формулы, выражающие следующие утверждения:

(a) через каждые две точки можно провести прямую, и если эти точки различны, то такая прямая единственна
(b) через каждые три точки, не лежащие на одной прямой, можно провести единственную плоскость
(c) аксиому Евклида о параллельных прямых

Написать формулы, выражающие следующие свойства:

(a) свойство параллельности прямых
(b) свойство параллельности плоскостей

3. Пусть I – некоторая интерпретация, в которой интерпретирован двухаргументный предикат R.

Написать формулу, выражающую следующие свойства R:

(a) R рефлексивен
(b) R симметричен
(c) R транзитивен
(d) R является эквивалентностью

4. Пусть I – некоторая интерпретация, в которой интерпретированы двухаргументные предикаты "$\leq$" и "$=$".

Написать с использованием данных предикатов формулы, выражающие аксиомы

(a) частично упорядоченного множества
(b) линейно упорядоченного множества

5. Пусть I – некоторая интерпретация с областью, являющейся частично упорядоченным множеством, и в I интерпретирован двухаргументный предикат R следующим образом:

$$R(x, y) = 1 \quad \Leftrightarrow \quad x \leq y$$

Написать формулы, выражающие следующие свойства:

(a) x есть наименьший элемент

(b) x есть минимальный элемент

6. Пусть

   - I – некоторая интерпретация с областью $\mathbf{2}^A$ где A – некоторое множество, и
   - в I интерпретирован двухаргументный предикат R следующим образом:

   $$R^I(x,y)=1 \quad \Leftrightarrow \quad x \subseteq y$$

   Написать формулы, выражающие следующие свойства:

   (a) x есть пересечение y и z

   (b) x есть объединение y и z

   (c) $x=\emptyset$

   (d) $x=A$

   (e) x есть дополнение y

7. Пусть

   - I – интерпретация с областью $\mathbf{2}^A$, где A – некоторое множество,
   - в I интерпретирован двухаргументный предикат R следующим образом:

   $$R^I(x,y)=1 \quad \Leftrightarrow \quad x=y$$

   - в I интерпретированы двухаргументные функциональные символы f и g следующим образом:

   $$f^I(x,y) \stackrel{\text{def}}{=} x \cap y$$
   $$g^I(x,y) \stackrel{\text{def}}{=} x \cup y$$

   Написать формулы, выражающие следующие свойства:

   (a) $x \subseteq y$

   (b) x – одноэлементное множество

8. Пусть

   - I – интерпретация с областью $\mathbf{N}$,
   - в I интерпретирована константа $c : c^I \stackrel{\text{def}}{=} 1$
   - в I интерпретирован одноаргументный функциональный символ $s : s^I(x) \stackrel{\text{def}}{=} x+1$
   - в I интерпретирован некоторый одноаргументный предикат P

   Написать аксиому индукции для P.

8.5.7 Эквивалентность формул

1. Пусть переменная y не входит в формулу A. Доказать, что

   (a) $\forall x\ A \sim \forall y\ [x:=y]A$

   (b) $\exists x\ A \sim \exists y\ [x:=y]A$

   (c) $\forall y\ A \sim A$

   (d) $\exists y\ A \sim A$

2. Пусть переменная y не входит в формулу A. Доказать, что в этом случае для произвольной формулы B имеют место соотношения

   (a) $A \wedge (\forall y\ B) \sim \forall y\ (A \wedge B)$

   (b) $A \vee (\forall y\ B) \sim \forall y\ (A \vee B)$

   (c) $A \wedge (\exists y\ B) \sim \exists y\ (A \wedge B)$

   (d) $A \vee (\exists y\ B) \sim \exists y\ (A \vee B)$

   (e) $A \to (\forall y\ B) \sim \forall y\ (A \to B)$

   (f) $A \to (\exists y\ B) \sim \exists y\ (A \to B)$

   (g) $(\forall y\ B) \to A \sim \exists y\ (B \to A)$

   (h) $(\exists y\ B) \to A \sim \forall y\ (B \to A)$

3. Доказать, что для любых формул A, B имеют место соотношения:

   (a) $\forall x\ \forall y\ A \sim \forall y\ \forall x\ A$

   (b) $\exists x\ \exists y\ A \sim \exists y\ \exists x\ A$

   (c) $\overline{\forall x\ A} \sim \exists x\ \overline{A}$

   (d) $\overline{\exists x\ A} \sim \forall x\ \overline{A}$

   (e) $(\forall x\ A) \wedge (\forall x\ B) \sim \forall x\ (A \wedge B)$

   (f) $(\exists x\ A) \vee (\exists x\ B) \sim \exists x\ (A \vee B)$

   (g) $\exists x\ (A \to B) \sim (\forall x\ A) \to (\exists x\ B)$

Лекция 9

Теорема Эрбрана

9.1 Сколемовская нормальная форма

Литералом называется формула ЛП вида A или $\overline{A}$, где A – атомарная формула.

Дизъюнктом называется дизъюнкция некоторого множества литералов. Если это множество пусто, то соответствующий ему дизъюнкт называется **пустым**.

Формула ЛП называется **сколемовской нормальной формой (СНФ)**, если она замкнута и имеет вид

$$\forall X\ (D_1\ \wedge\ \ldots\ \wedge\ D_k) \tag{9.1}$$

где $D_1, \ldots, D_k$ – дизъюнкты, и $\forall X$ является сокращением знакосочетания $\forall x_1\ \ldots \forall x_n$, где $X = \{x_1 \ldots x_n\}$.

Для каждой формулы Φ существует СНФ Ψ, обладающая следующим свойством:

$$\Phi \text{ выполнима} \quad \Leftrightarrow \quad \Psi \text{ выполнима}$$

СНФ Ψ может быть построена при помощи алгоритма, состоящего из перечисленных ниже этапов. Каждый этап заключается в циклическом выполнении связанных с ним действий, которые выполняются до тех пор, пока их будет возможно выполнять. Когда выполнение ни одного из действий текущего этапа невозможно, происходит переход к следующему этапу.

1. **Замыкание.**
   Если множество $FV(\Phi)$ непусто, то к Φ спереди приписывается знакосочетание $\exists x_1 \ldots \exists x_n$, где $\{x_1 \ldots x_n\} = FV(\Phi)$.

2. **Удаление стрелок.**
   (a) Каждая подформула вида $A \leftrightarrow B$ заменяется на $(A \wedge B) \vee (\overline{A} \wedge \overline{B})$.
   (b) Каждая подформула вида $A \to B$ заменяется на $\overline{A} \vee B$.

3. **Пронесение отрицаний вниз.**
   (a) Каждая подформула вида $\overline{\overline{A}}$ заменяется на A.
   (b) Каждая подформула вида $\overline{A \wedge B}$ заменяется на $\overline{A} \vee \overline{B}$.
   (c) Каждая подформула вида $\overline{A \vee B}$ заменяется на $\overline{A} \wedge \overline{B}$.
   (d) Каждая подформула вида $\overline{\forall X\ B}$ заменяется на $\exists X \overline{B}$.
   (e) Каждая подформула вида $\overline{\exists X B}$ заменяется на $\forall X\ \overline{B}$.

4. **Передвижение кванторов направо.**
   (a) Подформулы вида $\forall x(A \wedge B)$ или $\exists x(A \vee B)$, где $x \in FV(A) \cap FV(B)$, заменяются соответственно на $\forall x A\ \wedge\ \forall x B$ и $\exists x A\ \vee\ \exists x B$
   (b) Подформулы вида $\forall x(A * B)$ или $\exists x(A * B)$ (вместо $A * B$ может быть $B * A$), где $x \notin FV(B)$, и "$*$" обозначает "$\wedge$" или "$\vee$", заменяются соответственно на $\forall x A * B$ и $\exists x A * B$

5. **Удаление кванторов существования.**
   Если в формулу входит хотя бы один квантор вида $\exists x$, и за самым левым вхождением этого квантора следует подформула A, то это вхождение квантора удаляется, и
   (a) если $FV(A) = \{x\}$, то A заменяется на формулу $[x := c]A$, где c – новая константа
   (b) если $FV(A) = \{x, x_1, \ldots, x_n\}$ $(n \geq 1)$, то A заменяется на формулу $[x := f(x_1, \ldots, x_n)]A$, где f – новый функциональный символ

6. **Переименование связанных переменных.**
   Если есть две подформулы с одинаковыми кванторами: $\forall x\ A$ и $\forall x\ B$, то подформула $\forall x\ B$ заменяется на $\forall y\ [x := y]B$, где y – новая переменная

7. **Перемещение кванторов налево.**
   Все кванторы перемещаются в начало формулы.

8. **Вынесение конъюнкций наружу.**
   Подформулы вида $(A \wedge B) \vee C$ или $C \vee (A \wedge B)$ заменяются на $(A \vee C) \wedge (B \vee C)$.

9. **Удаление лишних скобок.**
   Подформулы вида $(A \wedge B) \wedge C$ или $A \wedge (B \wedge C)$ переписываются в виде $A \wedge B \wedge C$, а подформулы вида $(A \vee B) \vee C$ или $A \vee (B \vee C)$ – в виде $A \vee B \vee C$.

9.2 Эрбрановские интерпретации

9.2.1 Понятие эрбрановской интерпретации

Пусть Γ – некоторое множество формул.

Мы будем использовать следующие обозначения:

- $Con(\Gamma)$ обозначает множество
  - в которое входят все константы, входящие в формулы из Γ, и, кроме того,
  - для каждого типа τ, такого, что в Γ есть выражение типа τ, но отсутствуют константы типа τ, $Con(\Gamma)$ содержит какую-либо константу типа τ
- $Fun(\Gamma)$ обозначает множество всех функциональных символов, входящих в формулы из Γ
- $Rel(\Gamma)$ обозначает множество всех предикатов, входящих в формулы из Γ
- $Expr(\Gamma)$ обозначает множество выражений, в которые входят только такие константы и функциональные символы, которые принадлежат соответственно $Con(\Gamma)$ и $Fun(\Gamma)$
- $H(\Gamma)$ обозначает множество всех выражений из $Expr(\Gamma)$, не содержащих переменных.

Эрбрановской интерпретацией (ЭИ) для Γ называется интерпретация с областью $H(\Gamma)$, в которой

- каждая константа $c \in Con(\Gamma)$ интерпретируется равным ей выражением из $H(\Gamma)$, и
- каждый функциональный символ $f \in Fun(\Gamma)$ интерпретируется функцией, сопоставляющей каждому списку выражений $(h_1, \ldots, h_n)$ соответствующих типов выражение $f(h_1, \ldots, h_n)$.

Ниже в этой главе предполагается, что список Γ состоит из одной СНФ S вида (9.1)

9.2.2 Связь произвольных интерпретаций с ЭИ

Пусть I – некоторая интерпретация, в которой истинна СНФ S вида (9.1). Построим ЭИ $H(I)$ для S, в которой S также будет истинна.

Для каждого выражения $h \in H(S)$ можно вычислить его значение в интерпретации I, которое мы будем обозначать символом h^I:

- если $h = c \in Con(S)$, то h^I является интерпретацией c^I константы c в I
- если $h = f(h_1, \ldots, h_n)$, то $h^I \stackrel{\text{def}}{=} f^I(h_1^I, \ldots, h_n^I)$

Для каждого означивания $\xi : X \to H(S)$ обозначим символом ξ^I означивание

$$X \xrightarrow{\xi^I} \mathcal{D}^I$$

которое сопоставляет каждому $x \in X$ значение $(\xi(x))^I$.

Каждое означивание $\xi : X \to H(S)$ можно рассматривать и как подстановку, которая действует на каждое выражение путём замены каждой входящей в него переменной x из X на выражение $\xi(x)$.

Для каждого выражения e из $Expr(S)$ с переменными из X имеет место соотношение

$$(\xi^I)(e) = (\xi(e))^I \tag{9.2}$$

в правой части которого ξ рассматривается как подстановка. Данное соотношение доказывается индукцией по структуре e.

В искомой ЭИ $H(I)$ каждый предикат $R \in Rel(S)$ интерпретируется отображением $R^{H(I)}$, которое сопоставляет каждому списку выражений $(h_1, \ldots, h_n)$ соответствующих типов значение

$$R^I(h_1^I, \ldots, h_n^I)$$

Если бы S была ложна в $H(I)$, то, поскольку S эквивалентна формуле

$$(\forall X D_1) \ \wedge \ \ldots \ \wedge \ (\forall X D_k)$$

то для некоторого $i \in \{1, \ldots, k\}$ формула $\forall X D_i$ была бы ложна в $H(I)$, т.е. для некоторого означивания $\xi : X \to H(S)$ было бы верно равенство $\xi(D_i) = 0$, т.е. для каждого литерала L, входящего в D_i, было бы верно равенство $\xi(L) = 0$.

Рассмотрим случай, когда литерал L положительный, т.е. имеет вид $R(e_1, \ldots, e_n)$. Согласно определениям и соотношению (9.2), имеет место цепочка равенств

$$\begin{aligned}
0 = \xi(L) = \xi(R(e_1, \ldots e_n)) = \\
= R^{H(I)}(\xi(e_1), \ldots, \xi(e_n)) = \\
= R^I((\xi(e_1))^I, \ldots, (\xi(e_n))^I) = \\
= R^I(\xi^I(e_1), \ldots, \xi^I(e_n)) = \\
= \xi^I(R(e_1, \ldots, e_n)) = \xi^I(L)
\end{aligned}$$

Аналогичным образом доказывается равенство

$$\xi^I(L) = 0$$

для отрицательных (т.е. содержащих отрицание) литералов из D_i.

Таким образом, имеет место соотношение

$$\xi^I(D_i) = 0$$

которое противоречит предположению о том, что S истинна в I.

9.3 Семантические деревья

9.3.1 Лемма Кёнига

Напомним, что **деревом** называется граф T

- в котором выделена вершина $Root(T)$, называемая **корнем**, и
- для каждой вершины n которого существует единственный путь из $Root(T)$ в n (который является пустым, если $n = Root(T)$).

Для каждой вершины $n \in T$ её **глубиной** называется количество рёбер на пути из $Root(T)$ в n.

Вершина $n \in T$ называется **терминальной**, если не существует рёбер, выходящих из n.

Путь π в дереве T называется **максимальным**, если он выходит из $Root(T)$, и либо бесконечен, либо заканчивается в некоторой терминальной вершине.

Для каждой вершины $n \in T$ символ $T(n)$ обозначает поддерево дерева T, вершинами которого являются концы путей, начинающихся в n.

При рассуждениях о деревьях важную роль играет **лемма Кёнига**, которая утверждает, что если

- дерево T бесконечно, и
- из каждой вершины $n \in T$ выходит конечное число рёбер

то в T существует бесконечный путь.

Действительно, обозначим символами $n_1^1, \ldots, n_k^1$ концы рёбер с началом в $Root(T)$. Если бы все деревья $T(n_1^1), \ldots, T(n_k^1)$ были конечными, то $T(n)$ тоже было бы конечным, поэтому для некоторого $i \in \{1, \ldots, k\}$ дерево $T(n_i^1)$ бесконечно. Дерево $T(n_i^1)$ тоже удовлетворяет условиям леммы Кёнига, и, следовательно, среди концов рёбер, выходящих из его корня n_i^1, существует такая вершина n_j^2, что дерево $T(n_j^2)$ бесконечно. Дерево $T(n_j^2)$ тоже удовлетворяет условиям леммы Кёнига, и т.д. Продолжая этот процесс неограниченно, мы построим искомый путь

$$Root(T) \to n_i^1 \to n_j^2 \to \ldots$$

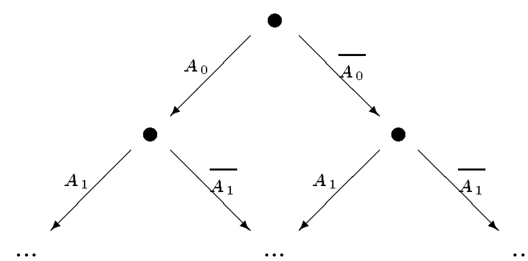
9.3.2 Семантические деревья

Обозначим символом $A(S)$ список $\{A_0, A_1, A_2, \ldots\}$ всех положительных литералов, в которые входят только предикаты из $Rel(S)$ и выражения из $H(S)$.

Семантическим деревом для S называется дерево T, в котором для каждого $i \geq 0$

- если $A(S)$ содержит литерал с номером i, то из каждой вершины дерева T глубины i выходят два ребра, одно из которых помечено литералом A_i, а другое – литералом $\overline{A_i}$
- если $A(S)$ не содержит литерал с номером i, то в дереве T нет вершин глубины $> i$.

Таким образом, T имеет вид



Для каждого максимального пути π в T, и каждого литерала A_i из $A(S)$, либо A_i либо $\overline{A_i}$ является меткой некоторого ребра на пути π. В первом случае мы будем писать $A_i \in \pi$, а во втором – $\overline{A_i} \in \pi$.

По каждой ЭИ I для S можно построить максимальный путь $\pi(I)$ в T, такой, что

$$\text{для каждого } A_i \in A(S) \quad A_i^I = 1 \quad \Leftrightarrow \quad A_i \in \pi(I) \tag{9.3}$$

Согласно определению значения формулы в интерпретации, соотношение $S^I = 0$ эквивалентно условию

$$\left.\begin{array}{l} \text{существуют означивание } \xi : X \to H(S) \\ \text{и дизъюнкт } D_i \text{ из } S\text{, такие, что} \\ \text{для каждого литерала } L \text{ из } D_i \quad \xi(L) = 0 \end{array}\right\} \tag{9.4}$$

Согласно выбору пути $\pi(I)$, соотношение $\xi(L) = 0$ эквивалентно соотношению $\overline{\xi(L)} \in \pi(I)$, в котором

- ξ рассматривается как подстановка, и
- если литерал L – отрицательный, то $\overline{\xi(L)}$ – положительный литерал, получаемый из $\xi(L)$ удалением отрицания.

Действительно, пусть, например, L – положительный литерал вида $R(e_1, \ldots, e_n)$. Соотношение $\xi(L) = 0$ означает, что

$$R^I(\xi(e_1), \ldots, \xi(e_n)) = 0$$

т.е. в ЭИ I литерал $R(\xi(e_1), \ldots, \xi(e_n))$ имеет значение 0, поэтому литерал

$$\overline{\xi(L)} \;=\; \overline{R(\xi(e_1), \ldots, \xi(e_n))}$$

имеет в I значение 1, и следовательно, по определению пути $\pi(I)$, $\overline{\xi(L)} \in \pi(I)$.

Аналогично рассматривается случай, когда L – отрицательный литерал.

Обозначим символом $n(I)$ вершину на пути $\pi(I)$, такую, что все литералы вида $\overline{\xi(L)}$, где $L \in D_i$, содержатся на участке пути $\pi(I)$ от корня до $n(I)$.

С использованием введённых понятий, условие (9.4) можно переформулировать так:

$$\left.\begin{array}{l} \text{существуют подстановка } \xi : X \to H(S) \\ \text{и дизъюнкт } D_i \text{ из } S\text{, такие, что} \\ \text{для каждого литерала } L \text{ из } D_i \\ \overline{\xi(L)} \text{ принадлежит пути из корня в } n(I) \end{array}\right\} \tag{9.5}$$

9.4 Теорема Эрбрана

Теорема Эрбрана утверждает, что невыполнимость СНФ S вида (9.1) эквивалентна следующему условию: существуют подстановки $\xi_1, \ldots, \xi_p : X \to H(S)$, и соответствующие им дизъюнкты $D_{j_1}, \ldots, D_{j_p}$ из S, такие, что формула

$$\xi_1(D_{j_1}) \wedge \ldots \wedge \xi_p(D_{j_p}) \tag{9.6}$$

имеет вид $\theta(F)$, где

- F – некоторая невыполнимая формула ЛВ, и
- θ – подстановка литералов из $A(S)$ вместо булевых переменных, входящих в F.

Для доказательства того, что из невыполнимости S следует данное условие, удалим из семантического дерева T для S все вершины (и входящие в них рёбра), в которые ведёт непустой путь из какой-либо вершины вида $n(I)$, где I – произвольная ЭИ для S. Нетрудно видеть, что получившийся граф T' будет деревом.

Дерево T' будет конечным, потому что в противном случае по лемме Кёнига в T' существует бесконечный путь π, который будет путём и в исходном дереве T. Для некоторой ЭИ I имеет место равенство $\pi = \pi(I)$, и, следовательно, на пути π расположена вершина $n(I)$. По построению дерева T', все вершины на пути π, расположенные ниже $n(I)$, должны отсутствовать в дереве T', что противоречит бесконечности пути π.

Пусть $(n_1, \ldots, n_p)$ – список терминальных вершин дерева T'. По построению, все они имеет вид $n(I_i)$ для некоторых ЭИ $I_1, \ldots, I_p$.

Так как S невыполнима, то для каждого $i = 1, \ldots, p$ имеет место соотношение $S^{I_i} = 0$, которое, согласно (9.5), эквивалентно условию

$$\left.\begin{array}{l}\text{существуют подстановка } \xi_i : X \to H(S)\\ \text{и дизъюнкт } D_{j_i} \text{ из } S\text{, такие, что}\\ \text{для каждого литерала } L \text{ из } D_{j_i}\\ \overline{\xi_i(L)} \text{ принадлежит пути из корня в } n(I_i)\end{array}\right\} \tag{9.7}$$

Искомая формула (9.6) строится из этих дизъюнктов и означиваний. Докажем, что она невыполнима.

Если бы она была выполнима, то она была бы истинна в некоторой ЭИ I. Путь $\pi(I)$ в дереве T проходит через некоторую вершину n_i из списка $(n_1, \ldots, n_p)$, и, следовательно, его участок от корня до n_i содержит все литералы вида $\overline{\xi_i(L)}$, где $L \in D_{j_i}$.

По определению пути $\pi(I)$, каждый литерал, принадлежащий $\pi(I)$, является истинным в I, и, следовательно, все литералы вида $\xi_i(L)$, где $L \in D_{j_i}$, ложны в I. Поэтому формула $\xi_i(D_{j_i})$ ложна в I, и, следовательно, вся формула (9.6) ложна в I.

Формула F, упомянутая в формулировке теоремы, получается из (9.6) заменой каждого входящего в неё литерала вида A_i из $A(S)$ на соответствующую ему булеву переменную p_i.

Для обратного доказательства (что из условия в формулировке теоремы следует невыполнимость S) предположим, что S выполнима. Тогда она истинна в некоторой ЭИ I. Следовательно, для каждого $i = 1, \ldots, p$ формула $\forall X D_{j_i}$ истинна в I, поэтому формула $\xi_i(D_{j_i})$ тоже истинна в I.

Таким образом, (9.6) истинна в I. Но, поскольку (9.6) имеет вид $\theta(F)$, где F – невыполнимая формула ЛВ, то она не может быть истинной ни в какой интерпретации. ■

Следствие.
Формула A является тавтологией тогда и только тогда, когда СНФ S для $\overline{A}$ удовлетворяет условию, изложенному в формулировке теоремы Эрбрана.

9.5 Задачи

1. Доказать, что исходная формула выполнима тогда и только тогда, когда построенная по ней СНФ выполнима.

2. Привести к СНФ

   (a) $(\exists x\ \forall y\ R(x,y)) \wedge (\exists x\ \forall y\ S(x,y))$

   (b) $(\exists x\ \forall y\ R(x,y)) \vee (\exists x\ \forall y\ S(x,y))$

   (c) $(\exists x\ \forall y\ R(x,y)) \to (\exists x\ \forall y\ S(x,y))$

   (d) $(\exists x\ \forall y\ R(x,y)) \to (\forall x\ \exists y\ R(x,y))$

   (e) $\forall x\ \exists y\ (R(x) \to Q(y,z)) \to$
   $\to \exists x\ \forall z\ (Q(x,z) \wedge R(y))$

   (f) $\forall x\ R(x) \to \forall y\ (\forall z\ Q(x,z) \to \forall u\ R(u))$

Лекция 10

Метод резолюций для ЛП

10.1 Описание метода резолюций

Как и в случае ЛВ, **метод резолюций** для ЛП предназначен для поиска ответа на вопрос, является ли анализируемая формула ЛП тавтологией.

Применение метода резолюций к формуле A заключается в том, что $\overline{A}$ приводится к СНФ S, и составляется набор дизъюнктов, который сначала состоит из всех дизъюнктов, входящих в S, а затем к нему добавляются

- резольвенты произвольных пар дизъюнктов, и
- склейки произвольных дизъюнктов

из текущего набора.

Если к текущему набору в некоторый момент добавился пустой дизъюнкт, то A является тавтологией.

Для определения понятия резольвенты и склейки дизъюнктов мы введём понятие **унификатора**.

10.1.1 Понятие унификатора

Пусть задано некоторое множество $\mathcal{L}$ литералов.

Для каждой подстановки θ символ $\theta(\mathcal{L})$ обозначает множество литералов вида $\theta(L)$, где $L \in \mathcal{L}$.

Множество $\mathcal{L}$ называется **унифицируемым**, если существует подстановка θ (называемая **унификатором** множества $\mathcal{L}$), такая, что множество $\theta(\mathcal{L})$ состоит из одного литерала.

Очевидно, что $\mathcal{L}$ унифицируемо тогда и только тогда, когда выполнены следующие условия:

- либо все литералы в $\mathcal{L}$ положительны, либо все они отрицательны
- предикаты во всех литералах из $\mathcal{L}$ совпадают
- пусть множество списков выражений в литералах из $\mathcal{L}$ имеет вид

  $$(e_1^1, \ldots, e_n^1), \ \ldots, \ (e_1^k, \ldots, e_n^k)$$

  тогда существует подстановка θ, такая, что

  $$\left\{ \begin{array}{l} \theta(e_1^1) = \ldots = \theta(e_1^k) \\ \ldots \\ \theta(e_n^1) = \ldots = \theta(e_n^k) \end{array} \right. \tag{10.1}$$

10.1.2 Системы формальных равенств

Рассмотрим систему формальных равенств вида

$$\left\{ \begin{array}{l} u_1 = v_1 \\ \ldots \\ u_m = v_m \end{array} \right. \tag{10.2}$$

где $u_1, v_1, \ldots, u_m, v_m$ – выражения.

Подстановка θ называется **решением** системы (10.2), если для каждого $i = 1, \ldots, m \quad \theta(u_i) = \theta(v_i)$.

Очевидно, что подстановка θ удовлетворяет условию (10.1) тогда и только тогда, когда она является решением системы, состоящей из формальных равенств вида $e_i^1 = e_i^j$, где $i = 1, \ldots, n$ и $j = 2, \ldots, k$. Таким образом, задача нахождения унификатора сводится к задаче нахождения решения системы формальных равенств.

Заметим, что если θ является решением системы (10.2), то для каждой подстановки θ' подстановка $\theta' \cdot \theta$ тоже является решением системы (10.2).

θ называется **наиболее общим решением (НОР)** системы (10.2), если каждое решение данной системы имеет вид $\theta' \cdot \theta$, где θ' – произвольная подстановка.

Мы будем говорить, что система (10.2) находится в **нормальной форме (НФ)**, если список $u_1, \ldots, u_m$ представляет собой список $x_1, \ldots, x_m$ различных переменных, каждая из которых не входит ни в одно из выражений $v_1, \ldots, v_m$. Нетрудно доказать, что в этом случае подстановка $\theta \stackrel{\text{def}}{=} [x_1 := v_1, \ldots, x_m := v_m]$ является решением системы (10.2).

Докажем, что данная подстановка является НОР системы (10.2). Пусть θ' – решение системы (10.2), т.е. для каждого $i = 1, \ldots, m \quad \theta'(x_i) = \theta'(v_i)$.

- Для каждой переменной x_i, входящей в список $(x_1, \ldots, x_m)$ имеет место равенство $\theta(x_i) = v_i$, поэтому $(\theta' \cdot \theta)(x_i) = \theta'(x_i)$.
- Для каждой переменной x, не входящей в список $(x_1, \ldots, x_m)$ имеет место равенство $\theta(x) = x$, поэтому для каждой такой переменной имеет место равенство $(\theta' \cdot \theta)(x) = \theta'(x)$.

Следовательно, равенство $(\theta' \cdot \theta)(x) = \theta'(x)$ имеет место для любой переменной x, т.е. подстановки θ' и $\theta' \cdot \theta$ совпадают.

Таким образом, θ является НОР системы (10.2). ■

Системы формальных равенств называются **эквивалентными**, если множества их решений совпадают.

Нахождение решения системы (10.2) производится путём её преобразования в эквивалентную ей систему в НФ. Алгоритм преобразования имеет итеративный вид, где каждый шаг итерации заключается в применении к текущей системе произвольного правила из излагаемого ниже списка, до тех пор, пока возможно применить какое-либо из этих правил.

1. Если система содержит равенство вида $u = u$, то оно удаляется.

2. Если система содержит равенство вида
$$f(u_1, \ldots, u_m) = f(v_1, \ldots, v_m)$$
то оно заменяется на совокупность равенств
$$u_1 = v_1, \ \ldots, \ u_m = v_m$$

3. Если система содержит равенство вида $x = v$ (или $v = x$), где x – переменная, не входящая в v, но входящая в какое-либо другое равенство, то во всех других равенствах x заменяется на v.

4. Если система содержит равенство вида $x = v$ (или $v = x$), где x – переменная, входящая в v, и $x \neq v$, то алгоритм заканчивается неудачей.

5. Если система содержит равенство $u = v$, где либо u и v – различные константы, либо одно из этих выражений имеет вид $f(u_1, \ldots, u_m)$ а другое - либо константа, либо имеет вид $g(v_1, \ldots, v_k)$, где $f \neq g$, то алгоритм заканчивается неудачей.

Очевидно, что действия 1,2,3 преобразуют систему в эквивалентную ей систему.

Заметим, что

- если данный алгоритм закончит свою работу успешно, то после замены в получившейся системе каждого формального равенства вида $v = x$ (где x – переменная) на $x = v$, данная система будет находиться в НФ, и, следовательно, имеет НОР, которое является также и НОР исходной системы
- если алгоритм заканчивается неудачей, то исходная система не имеет решений, потому что в этом случае она эквивалентна системе, которая
  - либо содержит равенство $x = v$ (или $v = x$), где x – переменная, входящая в v, $x \neq v$, и ясно, что никакая подстановка θ не может делать истинным равенство $\theta(x) = \theta(v)$, так как количество символов в левой части этого равенства всегда будет меньше, чем количество символов в его правой части
  - либо содержит равенство $u = v$, где первые символы в u и v различны и не являются переменными, поэтому для любой подстановки θ выражения $\theta(u)$ и $\theta(v)$ будут различны.

Докажем, что данный алгоритм всегда завершает свою работу. Предположим, что он допускает бесконечное вычисление, и последовательность систем, получающихся на каждом шаге этого вычисления, имеет вид $(S_i \mid i \geq 0)$. Для каждого $i \geq 0$ при переходе от S_i к S_{i+1} могут применяться только правила вида 1, 2, 3.

Количество применений правила 3 в этой последовательности не может быть бесконечным. Действительно, каждое применение правила 3 увеличивает количество равенств вида $x = v$ (или $v = x$), где x – переменная, имеющая только одно вхождение в текущую систему. Равенства такого вида не могут удалиться последующими применениями правил вида 1 и 2, хотя могут изменяться последующими применениями правила 3. Количество равенств такого вида не может быть больше, чем количество различных переменных в исходной системе.

Таким образом, начиная с некоторого момента, переходы от S_i к S_{i+1} происходят только по правилам 1 и 2, которые уменьшают количество символов в системе, и поэтому тоже не могут применяться бесконечно. ■

Унификатор θ для множества литералов $\mathcal{L}$ называется **наиболее общим** (и обозначается аббревиатурой **НОУ**), если θ является НОР системы формальных равенств, соответствующей условию (10.1).

10.1.3 Понятие резольвенты

Пусть D_1, D_2 – пара дизъюнктов, такая, что

- $FV(D_1) \cap FV(D_2) = \emptyset$, и
- D_1 содержит литерал L_1, D_2 – литерал $\overline{L_2}$, причём пара $\{L_1, L_2\}$ унифицируема, и θ – её НОУ.

Резольвентой D_1 и D_2 называется дизъюнкт, состоящий из литералов вида $\theta(L)$, где L – литерал из D_1, отличный от L_1, или литерал из D_2, отличный от $\overline{L_2}$.

В том случае, когда D_1 и D_2 содержат общие переменные, понятие резольвенты для них определяется почти так же, но с тем отличием, что вместо D_2 рассматривается дизъюнкт, получаемый из D_2 заменой каждой входящей в него переменной, входящей также и в D_1, на новую переменную, не входящую в D_1 и D_2 (при этом каждое вхождение одной и той же переменной заменяется на одну и ту же новую переменную).

Одна пара дизъюнктов может иметь несколько резольвент, в зависимости от выбора пары $L_1, \overline{L_2}$ удаляемых литералов.

10.1.4 Понятие склейки

Пусть D – дизъюнкт, содержащий унифицируемое подмножество литералов $\{L_1, \ldots, L_k\}$, и θ – НОУ этого подмножества.

Склейкой дизъюнкта D называется дизъюнкт, состоящий из литералов вида $\theta(L)$, где $L \in D$.

10.2 Корректность метода резолюций

Свойство **корректности** метода резолюций заключается в том, что если в некоторый момент к текущему набору добавился пустой дизъюнкт, то анализируемая формула A является тавтологией.

Для доказательства этого свойства предположим, что A – не тавтология, т.е. $\overline{A}$ выполнима. Следовательно, СНФ S истинна в некоторой интерпретации I, т.е. каждый дизъюнкт из S является истинным в I.

Если дизъюнкт D является истинным в I, то для каждой подстановки θ дизъюнкт $\theta(D)$ тоже является истинным в I, потому что для каждого означивания $\xi : Y \to \mathcal{D}^I$ (где Y – множество переменных, содержащее все переменные из D и θ) имеет место равенство $\xi(\theta(D)) = (\xi\theta)(D) = 1$, где означивание $\xi\theta : Y \to \mathcal{D}^I$ сопоставляет каждой переменной $y \in Y$ значение $\xi(\theta(y))$.

Отметим также, что операцию замены переменных, используемую при построении резольвенты (когда D_1 и D_2 содержат общие переменные) можно рассматривать как применение некоторой подстановки к D_2.

Таким образом, резольвенты и склейки дизъюнктов, которые истинны в I, тоже являются истинными в I. Следовательно, все дизъюнкты, которые были добавлены к исходному набору, являются истинными в I.

По предположению, в некоторый момент к текущему набору добавился пустой дизъюнкт. Пустой дизъюнкт может быть получен только как резольвента пары литералов вида $L_1, \overline{L_2}$, где множество $\{L_1, L_2\}$ унифицируемо. Обозначим его НОУ символом θ.

Если литералы L_1 и $\overline{L_2}$ истинны в I, то $\theta(L_1)$ и $\overline{\theta(L_2)}$ тоже истинны в I. Но данные литералы являются противоположными, и, следовательно, не могут быть одновременно истинными в I.

Следовательно, наше предположение о том, что A – не тавтология, является ошибочным. ■

10.3 Полнота метода резолюций

Докажем, что метод резолюций обладает свойством **полноты**, которая заключается в том, что если анализируемая формула A является тавтологией, то из набора дизъюнктов $D_1, \ldots, D_k$, входящих в СНФ S для $\overline{A}$, методом резолюций можно вывести пустой дизъюнкт.

Согласно следствию из теоремы Эрбрана, существуют подстановки $\xi_1, \ldots, \xi_p : X \to H(S)$, и соответствующие им дизъюнкты $D_{j_1}, \ldots, D_{j_p}$ из S, такие, что формула $\xi_1(D_{j_1}) \wedge \ldots \wedge \xi_p(D_{j_p})$ имеет вид $\theta(F)$, где F – невыполнимая формула ЛВ, и θ – подстановка, заменяющая каждую булеву переменную p_i в F на соответствующий ей литерал $A_i \in A(S)$.

Если $\theta(F)$ имеет вид конъюнкции дизъюнктов, то, значит, формула F имеет вид КНФ, и поскольку она невыполнима, то, по теореме о полноте метода резолюций для ЛВ, из дизъюнктов, входящих в F, можно вывести пустой дизъюнкт, т.е. существует последовательность дизъюнктов, каждый из которых

- либо является дизъюнктом, входящим в F,
- либо является резольвентой двух дизъюнктов, расположенных левее в этой последовательности

и последний дизъюнкт в ней является пустым. Нетрудно видеть, что, заменив в этой последовательности каждую булеву переменную p_i на соответствующую ей атомарную формулу $A_i \in A(S)$, мы получим вывод пустого дизъюнкта из набора $\xi_1(D_{j_1}), \ldots, \xi_p(D_{j_p})$.

Этот вывод можно "поднять" до вывода пустого дизъюнкта из набора дизъюнктов, входящих в S. Это возможно благодаря **лемме о подъёме**, которая утверждает, что если дизъюнкты D_1, D_2 не содержат общих переменных, и подстановки θ_1 и θ_2 таковы, что из $\theta_1(D_1)$ и $\theta_2(D_2)$ можно получить резольвенту D' то из дизъюнктов D_1 и D_2 можно получить при помощи построения резольвент и склеек такой дизъюнкт D, что $\theta(D) = D'$ для некоторой подстановки θ.

Действительно, при построении резольвенты D' выбираются литералы L_1 в $\theta_1(D_1)$ и L_2 в $\theta_2(D_2)$, такие, что множество $\{L_1, \overline{L_2}\}$ унифицируемо. Обозначим его НОУ символом θ'. Обозначим символами $\mathcal{L}_1$ и $\mathcal{L}_2$ множества литералов из D_1 и D_2 соответственно, состоящие из таких литералов L, что $\theta_1(L) = L_1$ и $\theta_2(L) = L_2$. Обозначим НОУ множеств $\mathcal{L}_1$ и $\mathcal{L}_2$ символами θ'_1 и θ'_2. По свойству НОУ, существуют подстановки θ''_1 и θ''_2, такие, что $\theta''_1 \cdot \theta'_1 = \theta_1$ и $\theta''_2 \cdot \theta'_2 = \theta_2$.

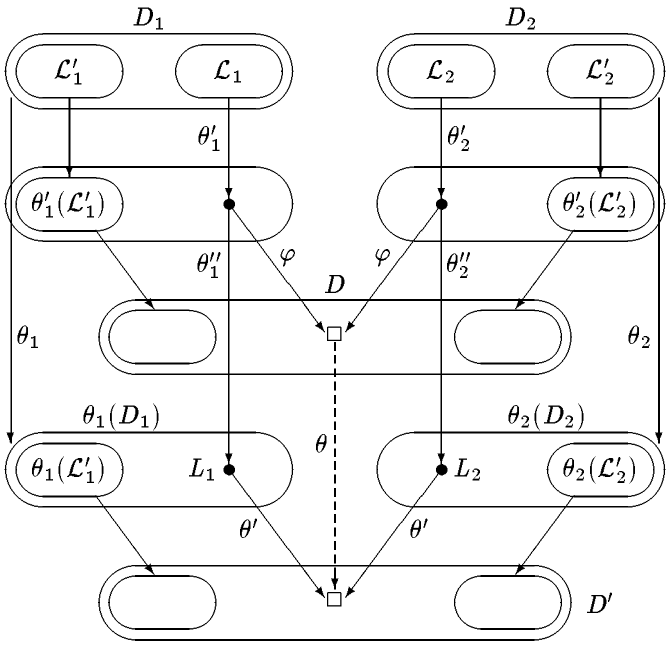
Поскольку D_1 и D_2 не имеют общих переменных, то $\theta'_1(D_1)$ и $\theta'_2(D_2)$ тоже не имеют общих переменных. Поэтому подстановки $\theta' \cdot \theta''_1$ и $\theta' \cdot \theta''_2$ можно рассматривать как составные части одной подстановки η. Поскольку η унифицирует пару литералов $\{\theta'_1(\mathcal{L}_1), \overline{\theta'_2(\mathcal{L}_2)}\}$, то существует подстановка θ, такая, что $\eta = \theta \cdot \varphi$, где φ – НОУ пары литералов $\{\theta'_1(\mathcal{L}_1), \overline{\theta'_2(\mathcal{L}_2)}\}$.

Искомый дизъюнкт D является резольвентой дизъюнктов $\theta'_1(D_1)$ и $\theta'_2(D_2)$ и состоит из всех литералов вида $(\varphi \cdot \theta'_i)(L)$, где L – произвольный литерал из D_i, не входящий в $\mathcal{L}_i \quad (i = 1, 2)$. Нетрудно видеть, что он удовлетворяет условию $\theta(D) = D'$. ■

Ниже данные рассуждения иллюстрируются диаграммой, в которой дизъюнкты изображаются в виде множеств входящих в них литералов. Символ «□» в дизъюнктах обозначает не включаемую в них пару противоположных литералов. Символ $\mathcal{L}'_i$ $(i = 1, 2)$ обозначает множество литералов из D_i, не входящих в $\mathcal{L}_i$.

10.4 Задачи

Решить методом резолюций все задачи из главы 8, в которых требуется проверить, является ли некоторая формула ЛП тавтологией или выполнимой формулой.


D_1
D_2
$\mathcal{L}'_1$
$\mathcal{L}_1$
$\mathcal{L}_2$
$\mathcal{L}'_2$
θ'_1
θ'_2
$\theta'_1(\mathcal{L}'_1)$
$\theta'_2(\mathcal{L}'_2)$
θ''_1
φ
φ
θ''_2
D
θ_1
θ_2
$\theta_1(D_1)$
$\theta_2(D_2)$
θ
$\theta_1(\mathcal{L}'_1)$
L_1
L_2
$\theta_2(\mathcal{L}'_2)$
θ'
θ'
D'

Лекция 11

Семантический вывод

11.1 Семантический вывод в ЛВ

11.1.1 Семантические таблицы

Все формулы в этом пункте являются формулами ЛВ.

Семантической таблицей (СТ) называется пара $(\Gamma \mid \Delta)$, где Γ и Δ – некоторые множества формул.

СТ $(\Gamma \mid \Delta)$ **противоречива**, если $\Gamma \cap \Delta \neq \emptyset$.

СТ $(\Gamma \mid \Delta)$ **выполнима**, если для некоторой оценки ξ переменных из Γ и Δ

$$\forall A \in \Gamma \quad \xi(A) = 1, \qquad \forall B \in \Delta \quad \xi(B) = 0 \qquad (11.1)$$

Правила вывода СТ позволяют получать из одних СТ другие СТ, и имеют следующий вид:

$$\frac{(A \wedge B,\ \Gamma \mid \Delta)}{(A,\ B,\ \Gamma \mid \Delta)} \qquad \frac{(\Gamma \mid A \wedge B,\ \Delta)}{(\Gamma \mid A,\ \Delta) \qquad (\Gamma \mid B,\ \Delta)}$$

$$\frac{(\Gamma \mid A \vee B,\ \Delta)}{(\Gamma \mid A,\ B,\ \Delta)} \qquad \frac{(A \vee B,\ \Gamma \mid \Delta)}{(A,\ \Gamma \mid \Delta) \qquad (B,\ \Gamma \mid \Delta)}$$

$$\frac{(\Gamma \mid A \to B,\ \Delta)}{(A,\ \Gamma \mid B,\ \Delta)} \qquad \frac{(A \to B,\ \Gamma \mid \Delta)}{(\Gamma \mid A,\ \Delta) \qquad (B,\ \Gamma \mid \Delta)}$$

$$\frac{(\overline{A},\ \Gamma \mid \Delta)}{(\Gamma \mid A,\ \Delta)} \qquad \frac{(\Gamma \mid \overline{A},\ \Delta)}{(A,\ \Gamma \mid \Delta)}$$

где A, B – формулы, Γ, Δ – множества формул, и для каждого множества формул M и каждой формулы Φ знакосочетание Φ, M обозначает множество $\{\Phi\} \cup M$. В каждом правиле над чертой изображена исходная СТ, а под ней - одна или две СТ, которые выводятся из исходной. Каждое правило вывода заключается в том, что в исходной СТ выделяется неатомарная формула, которая заменяется на одну или две подформулы этой формулы. Про выделенную формулу мы будем говорить, что она **раскрывается** в этом правиле вывода.

Нетрудно доказать, что каждое из правил вывода обладает следующим свойством:

$$\begin{array}{l}\text{исходная СТ}\\ \text{выполнима}\end{array} \Leftrightarrow \begin{array}{l}\text{хотя бы одна из выведенных}\\ \text{из неё СТ выполнима}\end{array} \qquad (11.2)$$

Отметим, что если СТ противоречива, то она не может быть выполнимой.

11.1.2 Дерево семантического вывода

Пусть Φ – некоторая формула.

Дерево семантического вывода (ДСВ) для Φ – это дерево $\mathcal{D}$, вершинами которого являются СТ, и

1. корневая вершина имеет вид $(\emptyset \mid \Phi)$,
2. каждая терминальная вершина противоречива, и
3. с каждой нетерминальной вершиной N связано некоторое правило вывода, исходной СТ которого является N, и концами рёбер, выходящих из вершины N, являются те СТ, которые выводятся из N на основании этого правила вывода.

Для каждой формулы Φ верна эквиваленция

$$\text{существует ДСВ для } \Phi \quad \Leftrightarrow \quad \Phi \text{ тавтология} \qquad (11.3)$$

Импликация "$\Rightarrow$" верна потому, что если существует ДСВ для Φ, но Φ – не тавтология, то СТ $(\emptyset \mid \Phi)$ выполнима, а следовательно, выполнимой будет некоторая терминальная вершина ДСВ, что невозможно.

Импликация "$\Leftarrow$" верна потому, что ДСВ для тавтологии Φ можно построить, начиная с дерева из одной вершины $(\emptyset \mid \Phi)$, путём итеративного выполнения следующей операции: если в дереве, построенном к текущему моменту, есть непротиворечивая терминальная вершина N с неатомарной формулой A, то существует правило вывода, исходной СТ которого является N, а раскрываемой формулой - A, и мы рисуем из N одно или два ребра, концами которых являются СТ, выводимые из N при помощи этого правила вывода.

Данный процесс не может продолжаться бесконечно (т.к. СТ в конце каждого из рисуемых рёбер содержит меньше связок, чем СТ в его начале), поэтому после некоторого количества шагов будет построено дерево $\mathcal{D}$, каждая терминальная вершина которого либо противоречива, либо состоит только из атомарных формул.

Если бы в $\mathcal{D}$ была хоть одна непротиворечивая терминальная вершина N, то, поскольку N состоит только из атомарных формул, можно определить оценку ξ так, чтобы было верно (11.1). Таким образом, N выполнима, поэтому все СТ на пути из корня в N выполнимы. В частности, $(\emptyset \mid \Phi)$ выполнима, что противоречит предположению о том, что Φ – тавтология.

11.2 Семантический вывод в ЛП

Все формулы в этом пункте, являются замкнутыми формулами ЛП.

СТ в ЛП тоже имеет вид $(\Gamma \mid \Delta)$, где Γ и Δ – множества формул, и тоже называется **противоречивой**, если $\Gamma \cap \Delta = \emptyset$.

СТ $(\Gamma \mid \Delta)$ называется **выполнимой**, если существует интерпретация I, такая, что

$$\forall A \in \Gamma \quad A^I = 1, \qquad \forall B \in \Delta \quad B^I = 0 \tag{11.4}$$

Список правил вывода СТ в ЛП состоит из всех правил из пункта (11.1), а также следующих правил:

$$\frac{(\exists x\ A,\ \Gamma \mid \Delta)}{([x := c]A,\ \Gamma \mid \Delta)} \qquad \frac{(\Gamma \mid \forall x\ A,\ \Delta)}{(\Gamma \mid [x := c]A,\ \Delta)}$$

где c – константа, не входящая в A, Γ и Δ, а также

$$\frac{(\forall x\ A,\ \Gamma \mid \Delta)}{([x := h_1]A, \ldots, [x := h_n]A,\ \forall x\ A,\ \Gamma \mid \Delta)} \tag{11.5}$$

$$\frac{(\Gamma \mid \exists x\ A,\ \Delta)}{(\Gamma \mid [x := h_1]A, \ldots, [x := h_n]A,\ \exists x\ A,\ \Delta)} \tag{11.6}$$

где $h_1, \ldots, h_n$ выражения типа $\tau(x)$ без переменных.

Нетрудно доказать, что каждое из правил вывода для СТ в ЛП обладает свойством (11.2).

Эквиваленция (14.8) тоже имеет место, и импликация "$\Rightarrow$" в ней обосновывается, так же, как в ЛВ.

Докажем импликацию "$\Leftarrow$" в (14.8). Пусть Φ – тавтология. Построим ДСВ $\mathcal{D}$ для Φ.

Построение $\mathcal{D}$ осуществляется так же, как в случае ЛВ, но мы будем руководствоваться при этом следующими дополнительными принципами:

- для каждой вершины N в том дереве, которое построено к текущему моменту, каждая неатомарная формула A из N должна раскрываться в N или ниже (т.е. через некоторое количество шагов построения должен возникнуть путь из N в СТ, раскрываемой формулой в которой будет A, причём в той же части (левой или правой) в которой A была в N)

- если раскрываемая формула в вершине N начинается с квантора, и применяется правило (11.5) или (11.6), то в качестве выражений $h_1, \ldots, h_n$ берутся все выражения из $H(N)$, длина которых не больше, чем расстояние от N до корня.

Пусть получившееся дерево $\mathcal{D}$ не является ДСВ для Φ.

Если $\mathcal{D}$ – конечное, то тогда в нём существует непротиворечивая терминальная вершина N. В этом случае все формулы в N, атомарны, поэтому СТ N выполнима в некоторой ЭИ. Согласно (11.2), все СТ на пути из корня в N выполнимы. В частности, корневая СТ $(\emptyset \mid \Phi)$ выполнима, что противоречит предположению о том, что Φ – тавтология.

Докажем, что $\mathcal{D}$ не может быть бесконечным. Предположим, что $\mathcal{D}$ бесконечно. Тогда, по лемме Кёнига, в $\mathcal{D}$ существует бесконечный путь $N_0 \to N_1 \to \ldots$ из корня. Обозначим для каждого $i \geq 0 \quad N_i = (\Gamma_i \mid \Delta_i)$.

Нетрудно заметить, что имеют место включения

$$\begin{array}{l} At(\Gamma_0) \subseteq At(\Gamma_1) \subseteq At(\Gamma_2) \subseteq \ldots \\ At(\Delta_0) \subseteq At(\Delta_1) \subseteq At(\Delta_2) \subseteq \ldots \end{array} \tag{11.7}$$

где $At(\Gamma_i)$ и $At(\Delta_i)$ – множества всех атомарных формул из Γ_i и Δ_i.

Обозначим $\Gamma \stackrel{\text{def}}{=} \bigcup\limits_{i \geq 0} At(\Gamma_i)$ и $\Delta \stackrel{\text{def}}{=} \bigcup\limits_{i \geq 0} At(\Delta_i)$. Имеет место равенство $\Gamma \cap \Delta = \emptyset$, так как иначе существует формула A, такая, что $A \in At(\Gamma_k)$ и $A \in At(\Delta_k)$ для некоторого $k \geq 0$, что невозможно по причине непротиворечивости каждой СТ N_i .

Из $\Gamma \cap \Delta = \emptyset$ следует, что СТ $(\Gamma \mid \Delta)$ выполнима в некоторой ЭИ I для $\Gamma \cup \Delta$.

Докажем, что для каждого $i \geq 0$ верны соотношения

$$\forall A \in \Gamma_i \quad A^I = 1, \qquad \forall B \in \Delta_i \quad B^I = 0 \tag{11.8}$$

Заметим, что, полагая в (11.8) $i = 0$ и $B = \Phi$, мы получаем соотношение $\Phi^I = 0$, которое противоречит предположению о том, что Φ – тавтология.

Соотношения (11.8) мы будем доказывать индукцией по количеству связок и кванторов в A и B.

1. Если A и B атомарны, то они принадлежат соответственно Γ и Δ, и соотношения (11.8) верны по определению интерпретации I.

2. A и B являются булевыми комбинациями. Рассмотрим, например, случай, когда $A = A_1 \wedge A_2$.

   Существует номер $j \geq i$, такой, что раскрываемой формулой в $(\Gamma_j \mid \Delta_j)$ является A, и, следовательно, $A_1 \in \Gamma_{j+1}$ и $A_2 \in \Gamma_{j+1}$.

   По индуктивному предположению, $A_1^I = A_2^I = 1$. Следовательно, $A^I = (A_1 \wedge A_2)^I = 1$.

   Другие возможные виды формул A и B для данного случая рассматриваются аналогично.

3. A и B начинаются с квантора.

   Рассмотрим, например, случай $A = \forall x\ A_1$.

   Нам необходимо доказать, что $(\forall x\ A_1)^I = 1$, т.е. для каждого выражения $h \in H(\Gamma \cup \Delta)$ имеет место равенство $([x := h]A_1)^I = 1$.

   Из (11.7) и из определений Γ и Δ следует, что существует индекс i_0, такой, что для каждого $j \geq i_0$

   $$h \in H(\Gamma_j \cup \Delta_j)$$

   Выбрав $j \geq \max(i_0, |h|)$ (где $|h|$ длина h) таким, что раскрываемой формулой в СТ $(\Gamma_j \mid \Delta_j)$ является $\forall x A_1$, получаем, что $[x := h]A_1 \in \Gamma_{j+1}$, и, следовательно, по предположению индукции, имеет место желаемое равенство $([x := h]A_1)^I = 1$.

Лекция 12

Теорема Гёделя

12.1 Аксиоматический метод

Согласно общепринятому мнению, наиболее правильный способ организации научных знаний заключается в представлении их в виде логических следствий, выведенных на основе формальных правил вывода из некоторых исходных утверждений, истинность которых не подвергается сомнению.

Данный способ организации знаний наиболее предпочтителен по следующим причинам.

1. Наличие у некоторой совокупности знаний хорошей логической структуры существенно упрощает овладение этими знаниями.

2. Формализация знаний облегчает их обработку и существенно повышает её объективность и надёжность, поскольку такая обработка может быть проведена только посредством формальных операций над символьными строками, без привлечения расплывчато–неформальной и субъективной интерпретации понятий, выражаемых этими символьными строками. Кроме того, сведение задачи обработки знаний к задаче выполнения операций над символьными строками обеспечивает возможность автоматизации обработки знаний.

3. Поскольку критерием истинности формализованных знаний является их соответствие некоторым синтаксическим правилам, то формальное представление знаний облегчает проверку ошибочности в рассуждениях, в которых используются эти знания, поскольку оно позволяет свести задачу нахождения ошибок в рассуждениях к задаче проверки правильности использования синтаксических правил при формальных операциях над символьными строками.

4. Представление совокупности знаний в виде логических следствий из некоторых исходных принципов является инструментом синтеза новых знаний, поскольку процесс получения новых знаний может иметь вид формальной комбинации уже установленных утверждений с использованием подходящих правил логического вывода.

Наиболее плодотворные результаты реализация данной точки зрения принесла в математике, в которой удалось представить все установленные математические утверждения в виде логических следствий некоторого небольшого числа исходных простых утверждений, называемых **аксиомами**. Метод организации математических знаний в виде логических следствий из аксиом получил название **аксиоматического метода**.

Аксиоматический метод стал источником бурного развития всех областей математики, и обогатил их глубокими и плодотворными результатами. Наиболее ярко это проявилось в абстрактной алгебре, которая, благодаря использованию в ней аксиоматического метода, заняла центральное положение в математике.

Некоторое время существовало убеждение, что на базе аксиоматического метода можно построить всю математику, то есть всю совокупность истинных математических утверждений можно представить в виде логических следствий некоторых аксиом, что позволит свести задачу получения новых математических знаний к выполнению формальных операций над символьными строками по заранее заданным правилам.

Однако, как было установлено в 1932 году Гёделем, никакая формальная система (т.е. совокупность аксиом и правил вывода) не может позволить получить таким механическим способом всю совокупность истинных математических утверждений. В частности, утверждение о том, что данная формальная система непротиворечива (т.е. в ней невозможно вывести двух взаимоисключающих предложений) невозможно обосновать методами данной формальной системы.

Теорема Гёделя является убедительным подтверждением тезиса о том, что главный источник развития математики лежит за её пределами. Истинный прогресс в математике, связанный с появлением новых концепций и формальных систем, невозможен в рамках фиксированной формальной системы, он может произойти только в результате взаимопроникновения и взаимовлияния самых разных областей научной, культурной и практической деятельности. Всякая принципиально новая и более сильная формальная система может быть только изобретением: согласно теореме Гёделя, никаким другим образом её получить невозможно.

12.2 Строки и функции на них

12.2.1 Символьные строки

Все объекты, рассматриваемые в математике, можно изобразить символьными строками (которые мы ниже будем называть просто **строками**), и операции на объектах можно представить в виде функций на строках, изображающих эти объекты.

Совокупность всех строк обозначается символом $\mathbf{S}$. Каждая строка представляет собой последовательность символов некоторого конечного алфавита, содержащего буквы, цифры, скобки, и т.д. Существует пустая строка, она не содержит ни одного символа, и обозначается символом ε.

Если строка u представляет собой последовательность символов $a_1 \ldots a_n$, то мы будем записывать этот факт знакосочетанием $u = \text{"}a_1 \ldots a_n\text{"}$.

Функции на строках мы будем изображать в виде функциональных программ. Функциональные программы позволяют определять новые функции на строках при помощи базовых функций и функций, уже определённых в виде функциональных программ.

12.2.2 Базовые функции

При построении функциональных программ мы будем использовать следующие функции на строках (называемые **базовыми функциями**).

1. $\mathbf{if\_then\_else} : \mathbf{S}^3 \to \mathbf{S}$
   Эта функция имеет 3 аргумента, и сопоставляет каждой тройке $(u, v, w) \in \mathbf{S}^3$
   - строку v, если $u = \text{"1"}$
   - строку w, в противном случае.

   Для каждой тройки $(u, v, w) \in \mathbf{S}^3$ знакосочетание $\mathbf{if\_then\_else}(u, v, w)$ будет сокращённо записываться в виде $u\ ?\ v : w$.

2. $\mathbf{head} : \mathbf{S} \to \mathbf{S}$
   Эта функция сопоставляет строке u
   - строку, состоящую из первого символа строки u, если $u \neq \varepsilon$,
   - строку ε, если $u = \varepsilon$.

   Для каждой строки u знакосочетание $\mathbf{head}(u)$ будет сокращённо записываться в виде $\hat{u}$.

3. $\mathbf{tail} : \mathbf{S} \to \mathbf{S}$
   Эта функция сопоставляет строке u
   - строку, получаемую из u удалением первого символа, если $u \neq \varepsilon$,
   - строку ε, если $u = \varepsilon$.

   Для каждой строки u знакосочетание $\mathbf{tail}(u)$ будет сокращённо записываться в виде u'.

4. $\mathbf{conc} : \mathbf{S}^2 \to \mathbf{S}$
   Эта функция имеет 2 аргумента, и сопоставляет каждой паре $(u, v) \in \mathbf{S}^2$ конкатенацию строк u и v, т.е.
   - строку $\text{"}a_1 \ldots a_n\, b_1 \ldots b_m\text{"}$, если $u = \text{"}a_1 \ldots a_n\text{"}$ и $v = \text{"}b_1 \ldots b_m\text{"}$,
   - строку v, если $u = \varepsilon$,
   - строку u, если $v = \varepsilon$.

   Знакосочетание $\mathbf{conc}(u, v)$ будет сокращённо записываться в виде $u \cdot v$.

5. $\mathbf{equal} : \mathbf{S}^2 \to \mathbf{S}$
   Эта функция имеет 2 аргумента, и сопоставляет каждой паре $(u, v) \in \mathbf{S}^2$
   - строку "1", если $u = v$,
   - строку "0", если $u \neq v$.

   Знакосочетание $\mathbf{equal}(u, v)$ будет сокращённо записываться в виде $u = v$.

6. $\mathbf{not} : \mathbf{S} \to \mathbf{S}$
   Эта функция сопоставляет каждой строке u
   - строку "1", если $u = \text{"0"}$,
   - строку "0", если $u \neq \text{"0"}$.

   Знакосочетание $\mathbf{not}(u)$ будет сокращённо записываться в виде $\neg u$ или $\overline{u}$.

7. $\mathbf{conj}$, $\mathbf{disj}$, $\mathbf{impl}$, $\mathbf{equiv} : \mathbf{S}^2 \to \mathbf{S}$
   Каждая из этих функций имеет 2 аргумента, и сопоставляет каждой паре $(u, v) \in \mathbf{S}^2$ строку "1" или "0", которая равна результату соответствующей булевской операции $(\wedge, \vee, \to, \leftrightarrow)$, если оба аргумента имеют вид "1" или "0".

   Знакосочетания $\mathbf{conj}(u, v)$, и т.д. будут сокращённо записываться в виде $u \wedge v$, и т.д.

12.2.3 Функциональные программы

Функциональная программа (ФП) представляет собой определение некоторого множества $f_1, \ldots, f_n$ новых функций на строках, и имеет вид системы уравнений

$$\left\{ \begin{array}{l} f_1(x_{11}, \ldots, x_{1k_1}) = F_1 \\ \ldots \\ f_n(x_{n1}, \ldots, x_{nk_n}) = F_n \end{array} \right. \tag{12.1}$$

где

- $f_1, \ldots, f_n$ – функциональные символы, являющиеся именами определяемых функций,
- x_{ij} – переменные, являющиеся формальными параметрами определяемых функций, и

- $F_1, \ldots, F_n$ – выражения, обладающие следующими свойствами: для каждого $i = 1, \ldots, n$ выражение F_i содержит
  - переменные $x_{i1}, \ldots, x_{ik_i}$,
  - константы (ими могут быть любые строки)
  - функциональные символы, являющиеся именами базовых или уже построенных функций
  - функциональные символы, являющиеся именами определяемых функций $(f_1, \ldots, f_n)$

Мы предполагаем, что все выражения в функциональных программах имеют один и тот же тип, значениями которого являются строки. Каждому функциональному символу f сопоставлено число $ar(f)$, равное количеству аргументов у f.

Функции, определяемые функциональными программами, вычисляются стандартной рекурсией: если требуется вычислить значение функции f_i, которая определяется системой уравнений (12.1), на списке аргументов $(u_1, \ldots, u_{k_i})$, то для этого вычисляется значение выражения

$$[x_{i1} := u_1, \ldots, x_{ik_i} := u_{k_i}]F_i \tag{12.2}$$

Вычисление значения выражения (12.2) происходит по следующей схеме:

- если данное выражение имеет вид
$$f(e_1, \ldots, e_n)$$
где f – функциональный символ, являющийся именем некоторой базовой или уже построенной функции, используемой в системе (12.1), то вычисляются значения выражений $e_1, \ldots, e_n$, после чего вычисляется значение функции f на списке значений $e_1, \ldots, e_n$
- если данное выражение имеет вид
$$f_j(e_1, \ldots, e_n)$$
где f_j – функциональный символ, являющийся именем одной из определяемых функций в системе (12.1), то его значение равно значению выражения
$$[x_{j1} := e_1, \ldots, x_{jk_j} := e_{k_j}]F_j \tag{12.3}$$
которое вычисляется по той же схеме, по которой вычисляется значение выражения (12.2).

Приведём два примера ФП.

1. Запись строки в обратном порядке (строка "$a_1 \ldots a_n$" преобразуется в строку "$a_n \ldots a_1$"):
$$\mathtt{reverse}(x) = (x = \varepsilon)\ ?\ \varepsilon : \mathtt{reverse}(x') \cdot \hat{x}$$
2. Сортировка вставкой:
$$\begin{cases} \mathtt{sort}(x) = (x = \varepsilon)\ ?\ \varepsilon : \mathtt{insert}(\hat{x}, \mathtt{sort}(x')) \\ \mathtt{insert}(a, y) = (y = \varepsilon)\ ?\ \varepsilon : \\ \quad \big((a < \hat{y})\ ?\ a \cdot y : \hat{y} \cdot \mathtt{insert}(a, y')\big) \end{cases}$$

12.2.4 Строковое представление формул

Для каждой формулы её представление в виде символьной строки строится следующим образом. Сначала в формуле восстанавливаются все опущенные скобки, и формула переписывается в стандартном виде, т.е.

- все символы бинарных операций пишутся перед своими аргументами,
- все символы отрицания, написанные в виде черты над подформулами, заменяются на символы отрицания вида "$\neg$" перед этими подформулами, и т.д.

Затем все входящие в формулу переменные, константы, и т.д., заменяются на строки вида

`var(имя)`, `con(имя)`, `fun(имя)`, `rel(имя)`

где **имя** – любая последовательность символов, не содержащая круглых скобок, причём одинаковые символы заменяются на одинаковые строки, а разные - на разные, и, кроме того, стандартные символы (константа ε, функциональные символы для базовых функций, предикат "$=$") заменяются на стандартные строки :

`con(empty)`, `fun(^)`, `rel(=)`, и т.д.

Булевы связки заменяются на строки вида `bool(имя)`, кванторы - на `quant(A)` и `quant(E)`.

Ниже мы будем отождествлять каждую формулу с её строковым представлением.

12.2.5 Некоторые ФП

Читателю предлагается самостоятельно написать ФП

`Check_var`, `Check_con`, `Check_fun`, `Check_rel`
`Check_expr`, `Check_fm`

определяющие функции с одним аргументом, которые выдают в качестве значения

- "1", если их аргумент является соответственно переменной, константой, функциональным символом, предикатом, выражением, формулой
- "0", в противном случае.

12.2.6 Строковая интерпретация

Ниже все рассматриваемые формулы будут интерпретироваться только в одной интерпретации (называемой **строковой интерпретацией**), областью которой является множество $\mathbf{S}$ всех строк, и

- каждая константа (которой может быть любая строка) интерпретируется равной ей строкой
- каждый функциональный символ, соответствующий некоторой базовой функции, или функции, определяемой при помощи ФП, интерпретируется той функцией, которой он соответствует,
- предикат "$=$" интерпретируется отношением $id_{\mathbf{S}}$

12.3 Формальные системы

Ниже под **формулами** понимаются формулы ЛП, в которых все переменные и константы имеют один и тот же тип, и значениями этого типа являются строки.

При записи формул мы будем использовать следующее соглашение. Если некоторая формула A имеет только одну свободную переменную x, то этот факт может выражаться добавлением справа к A знакосочетания (x), и, кроме того, в этом случае для каждого выражения e, в которое не входят переменные, отличные от x, знакосочетание $A(e)$ обозначает формулу $[x := e]A$.

12.3.1 Понятие формальной системы

Формальная система состоит из аксиом и правил вывода.

Аксиомы

Аксиомы - это формулы следующих видов:

1. логические аксиомы:
   - $A \to (B \to A)$
   - $(A \to B) \to ((A \to (B \to C)) \to (A \to C))$
   - $(A \wedge B) \to A$
   - $(A \wedge B) \to B$
   - $(A \to B) \to ((A \to C) \to (A \to (B \wedge C)))$
   - $A \to (A \vee B)$
   - $B \to (A \vee B)$
   - $(A \to C) \to ((B \to C) \to ((A \vee B) \to C))$
   - $(A \to B) \to ((A \to \overline{B}) \to \overline{A})$
   - $\overline{\overline{A}} \to A$
   - $\forall x A(x) \to A(e)$
   - $A(e) \to \exists x A(x)$
   - $\forall x (B \to A) \to (B \to \forall x A)$
   - $\forall x (A \to B) \to (\exists x A \to B)$

   где A, B, C – произвольные формулы, причём в двух последних аксиомах предполагается, что x не имеет свободных вхождений в B
2. аксиомы равенства
   - $x = x$
   - $(x = y) \to (y = x)$
   - $(x = y) \to ((y = z) \to (x = z))$
3. аксиомы индукции:
$$\left\{ \begin{array}{l} A(0) \\ \forall x \; (A(x') \to A(x)) \end{array} \right\} \to \forall x A(x)$$
   где A – произвольная формула с одной свободной переменной x
4. аксиомы для базовых функций на строках
   - $("1" \; ? \; x : y) = x$
   - $("0" \; ? \; x : y) = y$
   - $(x = y) \;\leftrightarrow\; (x \cdot z = y \cdot z)$
   - $(x = y) \;\leftrightarrow\; (z \cdot x = z \cdot y)$
   - $(x \cdot y = \varepsilon) \to (x = \varepsilon) \wedge (y = \varepsilon)$
   - $(\hat{x} = \varepsilon) \to (x = \varepsilon)$
   - $x = \hat{x} \cdot x'$
   - $(\hat{x})' = \varepsilon$
   - $(x \cdot y) \cdot z = x \cdot (y \cdot z)$
   - $\varepsilon \cdot x = x, \quad x \cdot \varepsilon = x$
5. все уравнения, входящие во все ФП
6. другие аксиомы, задаваемые как множество значений некоторой функции f, определяемой при помощи ФП: для каждого значения аргумента u строка $f(u)$ является аксиомой, причём предполагается, что для каждой строки u длина $f(u)$ не меньше длины u.

Очевидно, что все аксиомы из групп 1-5 истинны в строковой интерпретации. Мы будем предполагать, что аксиомы из шестой группы тоже истинны в строковой интерпретации.

Правила вывода

Правила вывода позволяют получать из одних формул другие формулы, и имеют следующий вид:
(в данных правилах символы A, B обозначают формулы, а символы e, e_1, e_2 – выражения)

1. modus ponens
$$\frac{A, \quad A \to B}{B}$$
2. generalization
$$\frac{A}{\forall x A}$$
3. $$\frac{e_1 = e_2}{[x := e_1]e \;=\; [x := e_2]e}$$
4. $$\frac{e_1 = e_2}{[x := e_1]A \;\leftrightarrow\; [x := e_2]A} \qquad (12.4)$$
   где e_1 и e_2 не содержат переменных, имеющих связанные вхождения в A

В каждом правиле вывода над чертой изображены одна или две формулы (называемые **посылками**), из которых выводится формула, расположенная под чертой (называемая **заключением**).

Нетрудно доказать, что каждое из правил вывода обладает следующим свойством: если посылки этого правила вывода истинны в строковой интерпретации, то заключение этого правила тоже истинно в строковой интерпретации

Понятие доказательства

Пусть A – некоторая формула.

Доказательством формулы A называется последовательность формул

$$A_1, \ldots, A_n$$

обладающая следующими свойствами:

1. $A_n = A$
2. для каждого $i = 1, \ldots, n$ формула A_i – либо аксиома, либо является заключением некоторого правила вывода, посылки которого содержатся в множестве $\{A_1, \ldots, A_{i-1}\}$.

Формула называется **доказуемой**, если существует доказательство этой формулы. Из вышесказанного следует, что все доказуемые формулы истинны в строковой интерпретации.

Каждое доказательство можно изобразить в виде строки, используя специальный символ (например, "$*$") для разделения входящих в него формул.

Читателю предлагается самостоятельно написать ФП

- `Check_axiom`, определяющую функцию с одним аргументом u, которая выдаёт в качестве значения "1", если u является аксиомой, и "0", в противном случае,
- `Prf`, определяющую функцию с двумя аргументами u, v, которая выдаёт в качестве значения "1", если u является доказательством v, и "0", в противном случае.

При написании данных ФП можно предполагать, что совокупность всех имеющихся ФП изображается одной строкой, в которой уравнения отделяются друг от друга разделителем "$*$".

12.3.2 Доказательства, связанные с вычислениями

Каждое выражение вида

$$f(u_1, \ldots, u_n) \tag{12.5}$$

в котором f – имя некоторой функции, определяемой при помощи ФП, и $(u_1, \ldots, u_n)$ – список значений её аргументов, порождает некоторую последовательность $e_1, e_2, \ldots$ выражений, называемую **вычислением** значения выражения (12.5), в которой

- e_1 совпадает с (12.5), и
- для каждого $i \geq 1$ выражение e_{i+1} получается из e_i путём применения какого-либо уравнения в некоторой ФП, т.е. существует уравнение $t = s$ в некоторой ФП, такое, что для некоторой подстановки θ и некоторого выражения e имеют место равенства $e_i = [x := \theta(t)]e, \quad e_{i+1} = [x := \theta(s)]e$.

Если вышеупомянутая последовательность $e_1, \ldots$ конечна и имеет вид $e_1, \ldots, e_k$, где e_k – выражение, не содержащее функциональных символов (т.е. константа), то, согласно определению значения функции, вычисляемой функциональной программой, данная константа является значением выражения (12.5). Поскольку для каждого уравнения $t = s$ в каждой ФП формула $t = s$ является аксиомой, то, следовательно, для каждой подстановки θ формула $\theta(s) = \theta(s)$ является доказуемой, поэтому доказуемыми являются равенства $e_1 = e_2$, $e_2 = e_3$, $\ldots$, $e_{k-1} = e_k$, откуда, ввиду наличия аксиомы транзитивности равенства, получаем, что равенство $e_1 = e_k$ является доказуемым.

Таким образом, если для строк $u_1, \ldots, u_n, v$ имеет место равенство

$$f(u_1, \ldots, u_n) = v \tag{12.6}$$

то формула (12.6) является доказуемой.

Очевидно, что процедура построения доказательства формулы (12.6) может производиться по одной и той же схеме, независимо от вида ФП, определяющей функцию f и значений $u_1, \ldots, u_n, v$.

Читателю предлагается самостоятельно написать ФП, которая определяет функцию `Proof` с тремя аргументами:

$$f, \quad (u_1, \ldots, u_n), \quad v$$

где f – имя некоторой функции, определяемой при помощи ФП, $(u_1, \ldots, u_n)$ – список значений аргументов функции f, и v – некоторая строка. Значением функции `Proof` на этой тройке является строка, представляющая собой доказательство формулы (12.6), если это равенство является верным.

12.3.3 Дополнительные аксиомы

Мы будем использовать следующее обозначение: для любых выражений p и A знакосочетание $\Box_p A$ является сокращённой записью формулы $\texttt{Prf}(p, A) = 1$.

Мы будем предполагать, что в число аксиом из группы 6 входят следующие группы формул:

$$\Box_x A \to (\Box_y (A \to B) \to \Box_{x*y*B} B) \tag{12.7}$$

где x, y – переменные и A, B – формулы, а также

$$\begin{aligned} &(f(x_1, \ldots, x_n) = y) \to \\ &\to \Box_{\texttt{Proof}(f,(x_1,\ldots,x_n),y)} \Big(f(x_1, \ldots, x_n) = y \Big) \end{aligned} \tag{12.8}$$

где f – имя произвольной функции, определяемой при помощи ФП. Из определения функций `Prf` и `Proof` следует, что эти формулы истинны в строковой интерпретации. Аксиомы вида (12.7) выражают тот факт, что если последовательность формул x является доказательством формулы A, и последовательность формул y является доказательством формулы $A \to B$, то, соединяя эти последовательности, и добавляя к получившейся последовательности справа формулу B (а также добавив разделители "$*$" между x, y и B), мы получим доказательство формулы B.

12.4 Оператор доказуемости

Для любого выражения A знакосочетание $\Box A$ является сокращённой записью формулы $\exists x\ \Box_x A$. Символ "$\Box$" в данном контексте называется **оператором доказуемости**. Ниже мы приводим три свойства оператора доказуемости.

Лемма 1. Если доказуема формула A, то доказуема формула $\Box A$.

Доказательство.

Если формула A доказуема, то существует строка u, такая, что формула $\Box_u A$ является истинной. Поскольку каждая истинная формула вида (12.6) является доказуемой, то формула $\Box_u A$ доказуема. Из данной формулы и аксиомы $\Box_u A \to \exists x \Box_x A$ по правилу modus ponens получаем формулу $\exists x \Box_x A$, которая равна $\Box A$. ■

Лемма 2. Для любых формул A и B доказуема формула

$$\Box A \to (\Box(A \to B) \to \Box B) \tag{12.9}$$

Доказательство.

Используя аксиомы (12.7) и $\Box_{x*y*B} B \to \exists z \Box_z B$, а также некоторые тавтологии и правило modus ponens, нетрудно вывести формулу

$$\Box_x A \to (\Box_y (A \to B) \to \Box B)$$

из которой, с использованием правил generalization и modus ponens, а также аксиом

$$\forall z(C \to D) \to (C \to \forall z D)$$
$$\forall z(D \to C) \to (\exists z D \to C)$$

(где z не входит свободно в C), и некоторых тавтологий, нетрудно вывести искомую формулу. ■

Лемма 3. Если доказуема формула $A \to B$, то доказуема формула $\Box A \to \Box B$.

Доказательство.

По лемме 1, из доказуемости $A \to B$ следует доказуемость $\Box(A \to B)$, откуда на основании доказуемости формулы (12.9), которая эквивалентна формуле

$$\Box(A \to B) \to (\Box A \to \Box B) \tag{12.10}$$

по правилу modus ponens получаем искомую формулу $\Box A \to \Box B$. ■

Лемма 4. Для любой формулы A доказуема формула

$$\Box A \to \Box\Box A$$

Доказательство.

К аксиомам вида (12.8) относится формула

$$\Box_x A \to \Box_{\mathtt{Proof}(\Box_x A)} \Box_x A \tag{12.11}$$

Частным случаем аксиом вида $A(e) \to \exists z A(z)$ является формула

$$\Box_{\mathtt{Proof}(\Box_x A)} \Box_x A \to \Box\Box_x A \tag{12.12}$$

Из доказуемости формул (12.11) и (12.12) следует доказуемость формулы

$$\Box_x A \to \Box\Box_x A \tag{12.13}$$

Частным случаем аксиом вида $A(e) \to \exists z A(z)$ является формула

$$\Box_x A \to \Box A \tag{12.14}$$

По лемме 3, из доказуемости (12.14) следует доказуемость формулы

$$\Box\Box_x A \to \Box\Box A \tag{12.15}$$

Из доказуемости формул (12.13) и (12.15) следует доказуемость формулы

$$\Box_x A \to \Box\Box A \tag{12.16}$$

Применяя к (12.16) правило generalization, и, затем, применяя к получившейся формуле и аксиоме вида

$$\forall x(C \to D) \to (\exists x C \to D) \quad (\text{где } x \notin D)$$

правило modus ponens, получаем формулу $\Box A \to \Box\Box A$.

12.5 Лемма о неподвижной точке

Лемма о неподвижной точке утверждает, что для каждой формулы A с одной свободной переменной x существует замкнутая формула φ, такая, что доказуема формула

$$\varphi \ \leftrightarrow\ [x := \varphi]A \tag{12.17}$$

Доказательство.

Мы можем предполагать, что все вхождения x в A являются свободными.

Пусть Subst – функциональный символ, которому соответствует функция

$$\mathtt{Subst}(u, v) = [x := v]u$$

Обозначим символом B формулу $[x := \mathtt{Subst}(x, x)]A$.

Искомая формула φ имеет вид $[x := B]B$. Поскольку единственной свободной переменной в B была x, все вхождения которой заменились на строку, равную формуле B, то φ не содержит свободных переменных.

Согласно определению функции Subst, доказуема формула $\mathtt{Subst}(B, B) = [x := B]B$, т.е. доказуема формула $\mathtt{Subst}(B, B) = \varphi$. По правилу вывода (12.4), получаем доказуемость формулы

$$[x := \mathtt{Subst}(B, B)]A \ \leftrightarrow\ [x := \varphi]A$$

Левая часть в последней формуле совпадает с φ. Таким образом, имеет место желаемое соотношение (12.17). ■

12.6 Теорема Гёделя

Пусть формула A имеет вид $\overline{\Box x}$. По лемме о неподвижной точке, существует замкнутая формула φ, такая, что доказуема формула

$$\varphi \leftrightarrow \overline{[x := \varphi]\Box x}$$

т.е. доказуема формула

$$\varphi \leftrightarrow \overline{\Box\varphi} \tag{12.18}$$

Обозначим знакосочетанием $Consis$ формулу $\overline{\Box\mathbf{0}}$, где $\mathbf{0}$ – всегда ложная формула (отрицание тавтологии).

Докажем, что если наша формальная система непротиворечива, то обе формулы φ и $\overline{\varphi}$ недоказуемы.

1. Если доказуема φ, то по лемме 1 доказуема $\Box\varphi$, что, в сочетании с (12.18), приводит к доказуемости $\overline{\varphi}$, что невозможно, если наша формальная система непротиворечива.

2. Если доказуема $\overline{\varphi}$, то из (12.18) следует, что доказуема $\Box\varphi$, т.е. доказуема формула $\exists x\ \Box_x\varphi$. Поскольку каждая доказуемая формула является истинной в строковой интерпретации, то, следовательно, существует строка u, удовлетворяющая соотношению $\Box_u\varphi$, т.е. существует строка u, являющаяся доказательством φ, т.е. доказуема формула φ, что невозможно, если наша формальная система непротиворечива.

Докажем, что доказуема эквиваленция $\varphi \leftrightarrow Consis$ (из чего следует, что формула $Consis$ недоказуема).

1. Формула $\mathbf{0} \to \varphi$ является тавтологией, т.е. она доказуема, поэтому, по лемме 3, доказуема формула $\Box\mathbf{0} \to \Box\varphi$. Следовательно, доказуема формула $\overline{\Box\varphi} \to \overline{\Box\mathbf{0}}$. Используя (12.18), получаем доказуемость $\varphi \to \overline{\Box\mathbf{0}}$.

2. Докажем доказуемость обратной импликации, т.е. формулы $\overline{\Box\mathbf{0}} \to \varphi$. Для этого достаточно доказать доказуемость формулы $\overline{\varphi} \to \Box\mathbf{0}$, что, ввиду (12.18), эквивалентно доказуемости формулы $\Box\varphi \to \Box\mathbf{0}$.

   Формула $\varphi \to (\overline{\varphi} \to \mathbf{0})$ является тавтологией, т.е. она доказуема, поэтому, применяя два раза лемму 3 и правило modus ponens, получаем доказуемость формулы

   $$\Box\varphi \to (\Box\overline{\varphi} \to \Box\mathbf{0}) \tag{12.19}$$

   Из (12.18) следует доказуемость формулы $\Box\varphi \to \overline{\varphi}$, откуда, по лемме 3, следует доказуемость формулы $\Box\Box\varphi \to \Box\overline{\varphi}$. По лемме 4 получаем доказуемость формулы

   $$\Box\varphi \to \Box\overline{\varphi} \tag{12.20}$$

   Из (12.19) и (12.20), используя самую первую аксиому и правило modus ponens, нетрудно вывести доказуемость формулы $\Box\varphi \to \Box\mathbf{0}$. ■

Замечание.

Пусть формула $A(x)$ имеет вид $\overline{\Box_x\mathbf{0}}$.

Имеем: для каждой строки u формула $A(u)$ доказуема, но формула $\forall x A(x)$ недоказуема, так как она совпадает с $Consis$.

Лекция 13

Модальная логика

13.1 Понятие о модальной логике

Модальная логика является основой для построения логических систем, предназначенных для формализации суждений, в которых присутствуют количественные или качественные параметры, выражающие некоторую оценку суждений. В качестве таких оценок могут выступать, например,

- мера правдоподобия суждения
- вероятность того, что суждение истинно
- стоимость обоснования данного суждения
- отношение говорящего к суждению (например мера его уверенности в истинности суждения)
- мера полезности факта, выражаемого суждением, для достижения заданной цели
- мера ущерба, могущего возникнуть из-за того, что данное суждение не будет всегда истинным
- мера доверия к факту, выражаемому суждением, или к лицу, высказавшему суждение
- контекст (или ситуация), в котором высказано суждение

Мы рассмотрим простейший вид суждений такого вида, в которых могут быть использованы одноаргументные операторы $\Box$ и $\Diamond$, называемые **модальными операторами**. Эти операторы могут быть интерпретированы как самые разнообразные характеристики утверждений, перед которыми они стоят, например: «доказуемо», «необходимо», «возможно», «общепринято», «желательно», «скорее всего», «требуется», «должно быть», «маловероятно», «правдоподобно», «сомнительно», «предположительно», «интересно», «актуально», «известно», «целесообразно», и т.д.

Модальные операторы могут быть снабжены индексами (т.е. иметь вид $\Box_a$ и $\Diamond_a$, где a – некоторый количественный или качественный параметр, выражающий, например, силу модального оператора), но в данной главе мы рассматриваем только модальные операторы без индексов.

13.2 Модальные формулы

В модальной логике суждения формализуются в виде **модальных формул**, которые мы будем называть в данной главе просто **формулами**.

Основными структурными элементами в формулах являются **утверждения**, которые имеют тот же смысл, что и булевы переменные в логике высказываний. Множество всех утверждений обозначается символом $\mathcal{P}$.

Совокупность всех формул обозначается символом Φ и определяется следующим образом.

1. Каждое утверждение $p \in \mathcal{P}$ является формулой.
2. Символы $\mathbf{1}$ и $\mathbf{0}$ являются формулами.
3. Если A и B – формулы, то знакосочетания
$$\neg A, \quad A \wedge B, \quad A \vee B, \quad A \to B, \quad A \leftrightarrow B \qquad (13.1)$$
тоже являются формулами.
4. Для каждой формулы A знакосочетания $\Box A$ и $\Diamond A$ являются формулами.

Формулы (13.1) называются **булевыми комбинациями** формул A и B.

Связки $\Box$ и $\Diamond$ называются **модальными операторами**. Оператор $\Box$ читается как «необходимо», а оператор $\Diamond$ - как «возможно». Если формула не содержит модальных операторов, то она представляет собой формулу ЛВ или имеет вид $\mathbf{1}$ или $\mathbf{0}$. Формула без модальных операторов называется **тавтологией**, если она является тавтологией как формула ЛВ или имеет вид $\mathbf{1}$.

Подстановкой называется знакосочетание θ вида

$$\theta \ = \ [p_1 := A_1, \ldots, p_k := A_k] \qquad (13.2)$$

где

- $p_1, \ldots, p_k$ – список различных утверждений из $\mathcal{P}$, и
- $A_1, \ldots, A_k$ – список модальных формул.

Как и в ЛВ, подстановка (13.2) действует на каждую формулу A путём замены для каждого $i \in \{1, \ldots, k\}$ каждого вхождения утверждения p_i в A на формулу A_i. Формула, которая получается после такой замены, обозначается знакосочетанием $\theta(A)$.

13.3 Модальные логики

При проведении рассуждений о модальных формулах иногда рассматриваются не всевозможные формулы, а только формулы из некоторого ограниченного класса. Классы модальных формул принято называть **модальными логиками**, или просто **логиками**, т.е. словосочетание "модальная логика" имеет два значения: в первом значении – это одна из областей математической логики, а во втором – некоторый класс модальных формул.

Каждая модальная логика L должна удовлетворять следующим условиям.

1. L содержит все тавтологии.
2. L содержит формулу $\Box(p \wedge q) \leftrightarrow (\Box p \wedge \Box q)$, где $p, q \in \mathcal{P}$.
3. L содержит формулу $\Box\mathbf{1}$.
4. Если $A \in L$ и $A \to B \in L$, то $B \in L$.
5. Если $A \in L$, и θ - подстановка, то $\theta(A) \in L$.
6. Если L содержит формулу $A \leftrightarrow B$, то L также содержит формулу $\Box A \leftrightarrow \Box B$.

Из данного определения следует, что каждая модальная логика L обладает следующими свойствами:

1. L содержит формулу $A_1 \wedge \ldots \wedge A_n$ тогда и только тогда, когда L содержит все формулы $A_1, \ldots, A_n$,
2. если L содержит формулу A, то для любой формулы B L содержит $A \vee B$ и $B \to A$

Формула A называется **частным случаем тавтологии**, если она имеет вид $\theta(B)$, где B – тавтология, и θ – некоторая подстановка. Нетрудно доказать, что если $A \leftrightarrow B$ – частный случай тавтологии, то для любой логики L $A \in L \Leftrightarrow B \in L$.

Каждая модальная логика L порождает отношение эквивалентности $\sim_L$ на Φ, которое состоит из всех пар (A, B), обладающих свойством $A \leftrightarrow B \in L$. Обозначим символом $\Phi/_L$ совокупность классов разбиения множества Φ, которое соответствует отношению эквивалентности $\sim_L$.

На множестве $\Phi/_L$ можно определить отношение частичного порядка: $[A] \leq [B]$, если $A \to B \in L$. Нетрудно доказать, что $\Phi/_L$ является булевой алгеброй относительно этого частичного порядка, и для любых формул A, B верны равенства $1 = [\mathbf{1}]$, $0 = [\mathbf{0}]$, $[A]*[B] = [A*B]$, где $*$ – любой из символов: $\wedge, \vee, \to, \leftrightarrow$.

Кроме того, имеет место импликация

$$A \sim_L B \quad \Rightarrow \quad \Box A \sim_L \Box B \tag{13.3}$$

поэтому на $\Phi/_L$ можно определить одноаргументную операцию $\Box$, сопоставляющую классу $[A]$ класс $[\Box A]$. Из (13.3) следует, что эта операция определена корректно, т.е. если $[A] = [B]$, то $[\Box A] = [\Box B]$.

13.4 Модальные алгебры

Модальной алгеброй называется булева алгебра $\mathcal{A}$, на которой задана одноаргументная операция $\Box$, удовлетворяющая условиям:

- для всех $a, b \in \mathcal{A}$ $\Box(a \wedge b) = \Box(a) \wedge \Box(b)$, и
- $\Box(1) = 1$.

Нетрудно доказать, что для каждой логики L множество $\Phi/_L$ является модальной алгеброй.

Оценкой в модальной алгебре $\mathcal{A}$ называется произвольная функция ξ из $\mathcal{P}$ в $\mathcal{A}$. Для каждой оценки ξ в $\mathcal{A}$ и каждой формулы $A \in \Phi$ **значение** $\xi(A)$ формулы A на оценке ξ определяется рекурсивно:

- если $A = p \in \mathcal{P}$, то $\xi(A)$ уже задано
- $\xi(\mathbf{1}) = 1$, $\xi(\mathbf{0}) = 0$
- $\xi(\overline{A}) = \overline{\xi(A)}$
- $\xi(A * B) = \xi(A) * \xi(B)$, где $*$ – любой из символов $\wedge, \vee, \to, \leftrightarrow$
- $\xi(\Box A) = \Box(\xi(A))$

Логикой модальной алгебры $\mathcal{A}$ называется множество $L(\mathcal{A})$ всех формул $A \in \Phi$, таких, что для каждой оценки $\xi : \mathcal{P} \to \mathcal{A}$ имеет место равенство $\xi(A) = 1$.

Докажем, что для каждой логики L верно равенство

$$L = L(\Phi/_L)$$

т.е. для каждой формулы $A \in L$ условие $A \in L$ эквивалентно тому, что для каждой оценки $\xi : \mathcal{P} \to \Phi/_L$ имеет место равенство $\xi(A) = 1$.

Для этого сначала докажем, что для каждой формулы A имеет место эквиваленция $A \in L \Leftrightarrow [A] = 1$.

- Если $A \in L$, то $\mathbf{1} \to A \in L$ (потому что формула $A \to (\mathbf{1} \to A)$ – частный случай тавтологии).

  Кроме того, формула $A \to \mathbf{1}$ - частный случай тавтологии, и, следовательно, принадлежит L.

  Таким образом, L содержит $\mathbf{1} \to A$ и $A \to \mathbf{1}$, т.е. L содержит формулу $\mathbf{1} \leftrightarrow A$, поэтому $[A] = [\mathbf{1}] = 1$.

- Если $[A] = 1 = [\mathbf{1}]$, то $\mathbf{1} \leftrightarrow A \in L$, поэтому, в частности, $\mathbf{1} \to A \in L$, и, следовательно, $A \in L$.

Пусть $A \in L$, и ξ – оценка вида $\mathcal{P} \to \Phi/_L$. Для каждого $p \in \mathcal{P}$ обозначим символом A_p какую-либо формулу из класса $\xi(p)$. Нетрудно доказать, что для любой формулы $B \in \Phi$ имеет место равенство $\xi(B) = [\theta(B)]$, где подстановка θ заменяет каждое утверждение p в B на формулу A_p (это доказывается индукцией по структуре формулы B). Так как $A \in L$, то $\theta(A) \in L$, откуда, по доказанному выше, следует, что $[\theta(A)] = 1$, т.е. $\xi(A) = 1$.

Если $A \notin L$, то $A \leftrightarrow \mathbf{1} \notin L$, поэтому $[A] \neq [\mathbf{1}] = 1$. В этом случае для оценки ξ, сопоставляющей каждому утверждению $p \in \mathcal{P}$ класс $[p]$, имеет место соотношение $\xi(A) = [\theta(A)] = [A] \neq 1$. ■

13.5 Модели Крипке

13.5.1 Понятие модели Крипке

Модель Крипке (МК) – это пара $S = (Q, \delta)$, где

- Q – множество, элементы которого называются **состояниями**, и
- $\delta \subseteq Q^2$ - бинарное отношение, называемое **отношением перехода**

причём каждой паре $(q, p) \in Q \times \mathcal{P}$ сопоставлен элемент $q(p) \in \{0, 1\}$, называемый **оценкой** утверждения p в состоянии q.

Для каждого $q \in Q$ знакосочетание $\delta(q)$ обозначает множество $\{q' \in Q \mid (q, q') \in \delta\}$.

Для каждой пары $(q, q') \in Q^2$ выражение $\delta(q, q')$ имеет значение

- 1, если $(q, q') \in \delta$, и
- 0 – в противном случае.

Для каждой формулы A и каждого состояния $q \in Q$ **значение** A в состоянии q обозначается символом $q(A)$ и определяется рекурсивно следующим образом:

- если $A = p \in \mathcal{P}$, то $q(A)$ совпадает с оценкой p в q
- $q(\mathbf{1}) = 1,\ q(\mathbf{0}) = 0$
- $q(\overline{A}) = \overline{q(A)}$
- $q(A * B) = q(A) * q(B)$, где $*$ – любой из символов $\wedge, \vee, \rightarrow, \leftrightarrow$
- $q(\Box A) = \bigwedge_{q' \in Q} \Big(\delta(q, q') \rightarrow q'(A)\Big)$, т.е. $q(\Box A) = 1$, если для каждого $q' \in \delta(q) \quad q'(A) = 1$
- $q(\Diamond A) = \bigvee_{q' \in Q} \Big(\delta(q, q') \wedge q'(A)\Big)$, т.е. $q(\Diamond A) = 1$, если существует $q' \in \delta(q) : q'(A) = 1$

Каждой МК S соответствует модальная алгебра S^+ с множеством элементов $\mathbf{2}^Q$, на которой

- булевские операции совпадают с соответствующими теоретико-множественными операциями, т.е. $\wedge = \cap,\ \ \vee = \cup,\ \ 1 = Q,\ \ 0 = \emptyset$, и
- модальная операция $\Box : \mathbf{2}^Q \rightarrow \mathbf{2}^Q$ сопоставляет каждому множеству $V \subseteq Q$ множество

$$\Box(V) = \{q \in Q \mid \delta(q) \subseteq V\}$$

Нетрудно доказать, что операция $\Box$ на модальной алгебре S^+ сильно дистрибутивна относительно операции $\wedge$, т.е. для произвольной совокупности $\{V_i \mid i \in \Im\}$ элементов алгебры S^+ имеет место соотношение

$$\Box(\bigwedge_{i \in \Im} V_i) = \bigwedge_{i \in \Im} \Box(V_i)$$

Для каждой формулы $A \in \Phi$ символ Q_A обозначает множество $\{q \in Q \mid q(A) = 1\}$.

Пусть L – некоторая модальная логика. Нетрудно доказать, что следующие соотношения эквивалентны:

1. для каждой формулы $A \in L \quad Q_A = 1$
2. для любых формул $A, B \in \Phi$ из $A \sim_L B$ следует, что $Q_A = Q_B$
3. существует функция θ пополняющая диаграмму

$$\begin{tikzcd} \Phi \arrow[r, "{[\,]}"] \arrow[dr, "ev"'] & \Phi/_L \arrow[d, dashed, "\theta"] \\ & S^+ \end{tikzcd}$$

где $[\,]$ и ev – функции, сопоставляющие каждой формуле $A \in \Phi$ класс эквивалентности $[A] \in \Phi/_L$ и множество $Q_A \in S^+$ соответственно.

13.5.2 Морфизмы моделей Крипке

Пусть заданы две МК: $S_i = (Q_i, \delta_i) \quad (i = 1, 2)$.

Морфизмом f из S_1 в S_2 называется функция

$$f : Q_1 \rightarrow Q_2$$

такая, что для каждого $q \in Q_1$

$$f(\delta_1(q)) = \delta_2(f(q)) \tag{13.4}$$

и для каждого $p \in \mathcal{P}$ и каждого $q \in Q_1$

$$q(p) = f(q)(p)$$

Нетрудно доказать, что если f - морфизм из S_1 в S_2, то для каждой формулы A и каждого $q \in Q_1$

$$q(A) = f(q)(A)$$

Морфизму f из S_1 в S_2 соответствует функция

$$f^{-1} : \mathbf{2}^{Q_2} \rightarrow \mathbf{2}^{Q_1}$$

которая сохраняет все булевы операции.

Истинность условия (13.4) для каждого $q \in Q_1$ эквивалентна тому, что f^{-1} сохраняет также и операцию $\Box$, потому что для каждого подмножества $V \subseteq Q_2$ соотношение

$$f^{-1}(\Box V) = \Box f^{-1}(V)$$

эквивалентно условию: для каждого $q \in Q_1$

$$f(q) \in \Box V \quad \Leftrightarrow \quad \delta_1(q) \subseteq f^{-1}(V)$$

которое можно переписать в виде

$$\delta_2(f(q)) \subseteq V \quad \Leftrightarrow \quad f(\delta_1(q)) \subseteq V \tag{13.5}$$

Истинность соотношения (13.5) для каждого $V \subseteq Q_2$ эквивалентна условию (13.4). ■

13.6 Характеризация отношений перехода формулами

13.6.1 Транзитивность

Если в МК (Q, δ) отношение δ транзитивно, то для любого $q \in Q$ имеет место равенство

$$q(\Box p \to \Box\Box p) = 1 \tag{13.6}$$

так как если (13.6) неверно, то $q(\Box p) = 1$ и $q(\Box\Box p) = 0$, т.е. для некоторого $q' \in \delta(q)$ имеет место равенство $q'(\Box p) = 0$, из которого следует, что существует состояние $q'' \in \delta(q')$, такое, что $q''(p) = 0$. Поскольку δ транзитивно, то $q'' \in \delta(q)$, поэтому из $q(\Box p) = 1$ следует $q''(p) = 1$, что противоречит соотношению $q''(p) = 0$.

Если δ нетранзитивно, т.е. существуют состояния $q' \in \delta(q)$ и $q'' \in \delta(q')$, такие, что $q'' \notin \delta(q)$, то (13.6) будет неверно при такой оценке, при которой p истинно только в состояниях из $\delta(q)$.

13.6.2 Нётеровость

Если в МК (Q, δ) отношение δ транзитивно и **нётерово**, т.е. не существует последовательности $(q_n \mid n \geq 0)$ состояний, такой, что для каждого $n \geq 0$ $q_{n+1} \in \delta(q_n)$, то для каждого $q \in Q$

$$q(\Box(\Box p \to p) \to \Box p) = 1 \tag{13.7}$$

так как если (13.7) неверно, т.е. $q(\Box(\Box p \to p)) = 1$ и $q(\Box p) = 0$, то для некоторого $q_1 \in \delta(q)$

$$q_1(\Box p \to p) = 1, \quad q_1(p) = 0$$

откуда следует, что $q_1(\Box p) = 0$, т.е. для некоторого $q_2 \in \delta(q_1)$ $q_2(p) = 0$. Так как δ транзитивно, то $q_2 \in \delta(q)$, и из $q(\Box(\Box p \to p)) = 1$ следует, что $q_2(\Box p \to p) = 1$, что в сочетании с $q_2(p) = 0$ даёт соотношение $q_2(\Box p) = 0$, из которого следует, что существует $q_3 \in \delta(q_2)$, такой, что $q_3(p) = 0$. Продолжая в том же духе, мы построим последовательность $(q_n \mid n \geq 0)$, в которой $q_0 = q$ и для каждого $n \geq 0$ $q_{n+1} \in \delta(q_n)$, что противоречит нётеровости отношения δ.

Если δ транзитивно и не нётерово, т.е. существует последовательность $(q_n \mid n \geq 0)$, в которой для каждого $n \geq 0$ $q_{n+1} \in \delta(q_n)$, то (13.7) будет неверно при $q = q_0$ и такой оценке, при которой p истинно только в состояниях из $Q \setminus \{q_n \mid n \geq 0\}$.

13.6.3 Конфлюентность

Если в МК (Q, δ) отношение δ **конфлюентно**, т.е. для каждого $q \in Q$ и каждой пары $q_1, q_2 \in \delta(q)$ имеет место соотношение $\delta(q_1) \cap \delta(q_2) \neq \emptyset$, то для каждого $q \in Q$ имеет место равенство

$$q(\Diamond\Box p \to \Box\Diamond p) = 1 \tag{13.8}$$

так как если (13.8) неверно, то $q(\Diamond\Box p) = 1$ и $q(\Box\Diamond p) = 0$, т.е. для некоторого $q_1 \in \delta(q)$

$$q_1(\Box p) = 1 \tag{13.9}$$

и некоторого $q_2 \in \delta(q)$

$$q_2(\Diamond p) = 0 \tag{13.10}$$

Выберем произвольное состояние $q_3 \in \delta(q_1) \cap \delta(q_2)$. Из (13.9) следует, что $q_3(p) = 1$, а из (13.10) – $q_3(p) = 0$, что невозможно.

Если δ неконфлюентно, т.е. существуют состояния $q_1, q_2 \in \delta(q)$, такие, что $\delta(q_1) \cap \delta(q_2) = \emptyset$, то (13.8) будет неверно при такой оценке, при которой p истинно только в состояниях из $\delta(q_1)$.

13.6.4 Рефлексивность

Если в МК (Q, δ) отношение δ рефлексивно, то для любого $q \in Q$ имеет место равенство $q(\Box p \to p) = 1$, а если δ нерефлексивно, т.е. существует состояние $q \notin \delta(q)$, то $q(\Box p \to p) = 1$ будет неверно при такой оценке, при которой p истинно только в состояниях из $\delta(q)$.

13.6.5 Симметричность

Если в МК (Q, δ) отношение δ симметрично, то для любого $q \in Q$ имеет место равенство

$$q(\Diamond\Box p \to p) = 1 \tag{13.11}$$

Если δ несимметрично, т.е. существуют состояния q, q', такие, что $q' \in \delta(q)$, но $q \notin \delta(q')$, то (13.11) будет неверно при такой оценке, при которой p истинно только в состояниях из $\delta(q')$.

13.6.6 Сериальность

Если в МК (Q, δ) отношение δ **сериально**, т.е. для любого $q \in Q$ $\delta(q) \neq \emptyset$, то для любого $q \in Q$ имеет место равенство $q(\Diamond\mathbf{1}) = 1$, а если δ несериально, т.е. существует состояние q, такое, что $\delta(q) = \emptyset$ то $q(\Diamond\mathbf{1}) = 1$ будет неверно при любой оценке.

13.6.7 Детерминированность

Если в МК (Q, δ) отношение δ **детерминировано**, т.е. для любого $q \in Q$ и любых $q_1, q_2 \in \delta(q)$

$$\text{либо } q_1 = q_2, \text{ либо } q_2 \in \delta(q_1), \text{ либо } q_1 \in \delta(q_2)$$

то для любого $q \in Q$ имеет место равенство

$$q\Big(\Box(\Box p \wedge p \to q) \vee \Box(\Box q \wedge q \to p)\Big) = 1 \tag{13.12}$$

Если δ недетерминировано, т.е. существуют состояния $q, q_1 \in \delta(q)$ и $q_2 \in \delta(q)$, такие, что

$$q_1 \neq q_2, \; q_2 \notin \delta(q_1) \text{ и } q_1 \notin \delta(q_2)$$

то (13.12) будет неверно при такой оценке, при которой p истинно только в состояниях из $\delta(q_1) \cup \{q_1\}$, и q истинно только в состояниях из $\delta(q_2) \cup \{q_2\}$.

13.7 Канонические модели

13.7.1 L–непротиворечивые и L–полные множества

Пусть L – непротиворечивая логика (т.е. $L \neq \Phi$).

Множество формул $U \subseteq \Phi$ называется

- L–**непротиворечивым**, если для каждого его конечного подмножества $\{A_1, \ldots, A_n\}$ имеет место соотношение $\overline{A_1 \wedge \ldots \wedge A_n} \notin L$
- L–**полным**, если оно L–непротиворечиво, и для каждой формулы A либо $A \in U$, либо $\overline{A} \in U$.

Отметим, что логика L является L–непротиворечивым множеством, потому что если $A_1, \ldots, A_n \in L$, то $A_1 \wedge \ldots \wedge A_n \in L$ поэтому $\overline{A_1 \wedge \ldots \wedge A_n} \notin L$.

Если множество U L–полное, то $L \subseteq U$, потому, что если некоторая формула A из L не содержится в U, то $\overline{A} \in U$, откуда, ввиду L–непротиворечивости U, получаем: $\overline{\overline{A}} \notin L$, и, следовательно, $A \notin L$, что противоречит выбору A как формулы из L.

Если множество U L–непротиворечиво, то для любой формулы A либо $U \cup \{A\}$, либо $U \cup \{\overline{A}\}$ L–непротиворечиво, потому что если оба этих множества L–противоречивы, то существуют множества

$$\{B_1, \ldots, B_n\} \subseteq U \cup \{A\}, \quad \{C_1, \ldots, C_m\} \subseteq U \cup \{\overline{A}\}$$

такие, что $\overline{B_1 \wedge \ldots \wedge B_n} \in L$, $\quad \overline{C_1 \wedge \ldots \wedge C_m} \in L$. Первое из этих множеств содержит A, а второе - $\overline{A}$, так как иначе U будет L–противоречиво. Обозначим символом B конъюнкцию множества тех формул из совокупности $\{B_1, \ldots, B_n\}$, которые не совпадают с A, и символом C – конъюнкцию множества тех формул из совокупности $\{C_1, \ldots, C_m\}$, которые не совпадают с $\overline{A}$ (если какое-либо из этих множеств пусто, то его конъюнкция по определению равна формуле $\mathbf{1}$). Из соотношений $\overline{A \wedge B} \in L$, $\overline{\overline{A} \wedge C} \in L$, $\overline{A \wedge B} \to (\overline{\overline{A} \wedge C} \to \overline{B \wedge C}) \in L$ (последняя формула принадлежит L потому, что она является тавтологией) следует, что $\overline{B \wedge C} \in L$, что противоречит L-непротиворечивости множества U.

Для каждого L–непротиворечивого множества U существует L–полное множество U', такое, что $U \subseteq U'$. Множество U' можно построить, например, следующим образом. Пусть $(A_1, A_2, \ldots)$ – список всех формул. Определим последовательность $U_1, U_2, \ldots$ подмножеств множества Φ следующим образом: $U_1 \overset{\text{def}}{=} U$, и для каждого $n \geq 1$ $\quad U_{n+1}$ полагаем равным множеству

- $U_n \cup \{A_n\}$, если оно L-непротиворечиво, и
- $U_n \cup \{\overline{A_n}\}$ – в противном случае (согласно доказанному выше, в этом случае множество $U_n \cup \{\overline{A_n}\}$ будет L-непротиворечиво).

Искомое множество U' имеет вид $\bigcup\limits_{n \geq 1} U_n$. Если бы оно было L-противоречиво, то для некоторого $n \geq 1$ множество U_n было бы L-противоречиво, что противоречит определению последовательности $(U_n \mid n \geq 1)$. ■

13.7.2 Понятие канонической модели

Для каждого L-полного множества U и каждой формулы A знакосочетание $U(A)$ обозначает элемент множества $\{0, 1\}$, который равен 1, если $A \in U$, и 0 - в противном случае. Нетрудно доказать, что

- $U(\mathbf{1}) = 1$, $U(\mathbf{0}) = 0$
- $U(A) \wedge U(A \to B) \leq U(B)$
- $U(\overline{A}) = \overline{U(A)}$
- $U(A * B) = U(A) * U(B)$, где $*$ – любой из символов $\wedge, \vee, \to, \leftrightarrow$

Канонической моделью непротиворечивой логики L является МК $S_L = (Q_L, \delta_L)$, где

- Q_L состоит из всех L-полных множеств,
- $\delta_L(U, U') \overset{\text{def}}{=} \bigwedge_{A \in \Phi} \Big(U(\Box A) \to U'(A)\Big)$.
- для любых $U \in Q_L$ и $p \in \mathcal{P}$ оценка p в U совпадает с $U(p)$.

Докажем, что для любого $U \in Q_L$ и любой формулы A значение A в U совпадает с $U(A)$. С учётом вышесказанного, для этого достаточно доказать, что для каждой формулы A имеет место равенство $U(\Box A) = \Box U(A)$, т.е. $U(\Box A) = \bigwedge_{U' \in Q_L} \Big(\delta_L(U, U') \to U'(A)\Big)$.

Истинность неравенства

$$U(\Box A) \leq \delta_L(U, U') \to U'(A)$$

для каждого $U' \in Q_L$ следует из определения δ_L.

Обратное неравенство

$$\bigwedge_{U' \in Q_L} \Big(\delta_L(U, U') \to U'(A)\Big) \leq U(\Box A)$$

следует из того, что если $U(\Box A) = 0$, то существует множество $U' \in Q_L$, такое, что $\delta_L(U, U') \to U'(A) = 0$, т.е. $\delta_L(U, U') = 1$ и $U'(A) = 0$. В качестве U' можно взять L–полное множество, содержащее множество

$$\{B \in \Phi \mid U(\Box B) = 1\} \ \cup \ \{\overline{A}\} \qquad (13.13)$$

Докажем, что множество (13.13) L–непротиворечиво. Если оно L–противоречиво, то для некоторого подмножества $\{B_1, \ldots, B_n\}$ множества (13.13), имеет место соотношение $\overline{B_1 \wedge \ldots \wedge B_n} \in L$, из которого следует соотношение $\overline{\overline{A} \wedge B_1 \wedge \ldots \wedge B_n} \in L$. Пусть все формулы $B_1, \ldots, B_n$ отличны от $\overline{A}$. Обозначим символом B конъюнкцию $B_1 \wedge \ldots \wedge B_n$. Из соотношения $\overline{\overline{A} \wedge B} \in L$ следует, что $B \to A \in L$, откуда следует $\Box B \to \Box A \in L$. Так как L содержит формулу $\Box B \leftrightarrow (\Box B_1 \wedge \ldots \wedge \Box B_n)$, и $U(\Box B_1) = \ldots = U(\Box B_n) = 1$, то $U(\Box B) = 1$, откуда следует, что $U(\Box A) = 1$, что противоречит предположению о том, что $U(\Box A) = 0$. (если множество $\{B_1, \ldots, B_n\}$ пусто, то $B = \mathbf{1}$, и мы используем факт $\Box \mathbf{1} \in L$). ■

Если $A \in L$, то для любого $U \in Q_L$ $\quad U(A) = 1$ (т.к. $L \subseteq U$), а если $A \notin L$, то множество $\{\overline{A}\}$ L-непротиворечиво, и поэтому для некоторого $U \in Q_L$ $\quad U(A) = 0$.

13.8 Фильтрации МК

Для каждой формулы A знакосочетание $\langle A\rangle$ обозначает совокупность всех подформул формулы A.

Пусть (Q,δ) – некоторая МК. Определим отношение эквивалентности $\sim$ на Q следующим образом:

$$q \sim q' \quad \Leftrightarrow \quad \forall B \in \langle A\rangle \quad q(B) = q'(B)$$

Отображение

$$q \mapsto (q(A_1), \ldots, q(A_n)) \quad (\text{где } \{A_1, \ldots, A_n\} = \langle A\rangle)$$

сопоставляет всем элементам каждого класса разбиения по отношению $\sim$ один и тот же вектор из $\{0,1\}^n$, поэтому классов разбиения по отношению $\sim$ не может быть больше, чем векторов из $\{0,1\}^n$, количество которых равно 2^n.

Фильтрацией МК (Q,δ) по множеству $\langle A\rangle$ называется МК $(Q/_{\sim},\delta')$,

- отношение перехода δ' в которой состоит из всех пар $([q],[q']) \in (Q/_{\sim})^2$, таких, что $\delta(q,q')=1$, и
- для всех $q \in Q$ и $p \in \langle A\rangle \cap \mathcal{P}$ $\quad [q](p) = q(p)$.

Докажем, что для всех $q \in Q$ и $B \in \langle A\rangle \cap \mathcal{P}$ имеет место равенство $[q](B) = q(B)$. Данное равенство доказывается индукцией по структуре B. Если $B \in \mathcal{P}$, то оно верно по определению. Случай, когда B является булевой комбинацией, разбирается без особого труда. Если $B = \Box C$, то

$$\begin{aligned} [q](B) &= \bigwedge_{[q'] \in Q/\sim} \Big(\delta'([q],[q']) \to [q'](C)\Big) = \\ &= \bigwedge_{q' \in Q} \Big(\delta'([q],[q']) \to q'(C)\Big) \end{aligned} \qquad (13.14)$$

Нам надо доказать, что (13.14) совпадает с $q(\Box C)$, т.е. с

$$\bigwedge_{q' \in Q} \Big(\delta(q,q') \to q'(C)\Big) \qquad (13.15)$$

1. для каждого $q' \in Q$ из неравенства
$$\delta(q,q') \le \delta'([q],[q'])$$
следует неравенство
$$\delta'([q],[q']) \to q'(C) \;\le\; \delta(q,q') \to q'(C)$$
поэтому $(13.14) \le (13.15)$.

2. $q(\Box C) \le (13.14)$, так как для каждого $q' \in Q$ имеет место неравенство $q(\Box C) \le \delta'([q],[q']) \to q'(C)$, потому, что если $\delta'([q],[q']) = 1$, то для некоторых $q_1 \sim q$ и $q_1' \sim q'$ $\;\delta(q_1,q_1') = 1$, и если, кроме того, $q(\Box C) = q_1(\Box C) = 1$, то $q'(C) = q_1'(C) = 1$. ■

Поскольку $A \in \langle A\rangle$, то из вышедоказанного следует, что для каждого $q \in Q$ имеет место равенство $[q](A) = q(A)$. Поэтому если решается задача проверки истинности заданной формулы A во всех состояниях заданной МК (Q,δ) (известная как задача Model Checking), то данная задача может быть сведена к аналогичной задаче меньшей сложности, в которой вместо МК (Q,δ) рассматривается её фильтрация по множеству $\langle A\rangle$.

13.9 Задачи

1. Доказать, что условия, которым должна удовлетворять модальная логика, можно эквивалентным образом сформулировать так:
   (a) L содержит все тавтологии.
   (b) L содержит формулу $\Box(p \to q) \to (\Box p \to \Box q)$, где $p, q \in \mathcal{P}$.
   (c) Если $A \in L$ и $A \to B \in L$, то $B \in L$.
   (d) Если $A \in L$, и θ - подстановка, то $\theta(A) \in L$.
   (e) Если $A \in L$, то $\Box A \in L$.
2. Доказать, что S^+ является модальной алгеброй.
3. Доказать, что в каждой модели Крипке (Q,δ) для каждой формулы A имеет место равенство
$$Q_{\Diamond A} = Q_{\overline{\Box \overline{A}}}$$

Лекция 14

Нечёткие логики

14.1 Введение

Математические методы анализа систем заключаются в построении математических моделей исследуемых систем и формальном анализе этих моделей.

Поскольку модели систем не тождественны самим системам, и являются лишь их аппроксимациями, то, следовательно, свойства исследуемых систем и свойства их моделей могут различаться. Данная ситуация приводит к существенным трудностям при предсказании свойств реальных систем на основе информации о свойствах их моделей.

Один способ нахождения точных свойств анализируемых систем заключается в построении как можно более точных и детальных их математических моделей. Во многих ситуациях данный путь приводит к большим трудностям, по причине того, что большая сложность детальных моделей может вызывать существенные вычислительные проблемы при их формальном анализе.

Другой путь исследования свойств реальных систем заключается в построении таких их приближённых математических моделей, которые, хотя и являются грубыми подобиями исследуемых систем, но имеют приемлемую вычислительную сложность. Основная возникающая здесь проблема заключается в оценке меры расхождения между свойствами реальной системы и свойствами её приближённой модели.

Для точного оценивания данного расхождения необходим точный учёт в математической модели анализируемой системы всех предположений о нечёткости, недостоверности и неопределённости при построении данной модели, меры точности измерения параметров анализируемой системы, и т.п.

Все нечёткие компоненты математической модели анализируемой системы можно условно сгруппировать в следующие две категории.

1. Нечёткие компоненты, возникающие по причине *эффекта случайности*. Данный эффект имеет место например тогда, когда нечёткость в процессе измерения значения некоторого параметра анализируемой системы носит вероятностный характер, и измеряемые значения данного параметра подчиняются некоторым статистическим закономерностям.

   Данный вид нечёткости исследуется методами теории вероятностей, математической статистики и теории случайных процессов.

2. Нечёткие компоненты, возникающие по причине *концептуальной нечёткости*. Данные компоненты могут быть связаны с неполным и недостоверным знанием об изучаемой системе.

В настоящей главе излагается аппарат для исследования нечётких компонентов, относящихся ко второй категории.

14.2 Нечёткие логики

14.2.1 Шкала оценок

Напомним, что **полной решёткой** называется частично упорядоченное множество $(\mathcal{B}, \leq)$, такое, что для каждого подмножества $Q \subseteq \mathcal{B}$ существуют его точная нижняя грань и точная верхняя грань, т.е. такие элементы $\inf(Q)$ и $\sup(Q)$ множества $\mathcal{B}$, что для каждого $b \in \mathcal{B}$ имеют место соотношения

$$(\forall q \in Q \quad b \leq q) \quad \Leftrightarrow \quad b \leq \inf(Q),$$

$$(\forall q \in Q \quad q \leq b) \quad \Leftrightarrow \quad \sup(Q) \leq b.$$

Ниже элементы $\inf(\mathcal{B})$ и $\sup(\mathcal{B})$ обозначаются символами 0 и 1 соответственно.

Для произвольного конечного подмножества

$$Q = \{a_1, \ldots, a_n\} \subseteq \mathcal{B}$$

элементы $\inf(Q)$ и $\sup(Q)$ будут обозначаться знакосочетаниями

$$a_1 \wedge \ldots \wedge a_n \quad \text{и} \quad a_1 \vee \ldots \vee a_n$$

соответственно. Для данных элементов также будут использоваться обозначения

$$\left\{ \begin{array}{c} a_1 \\ \ldots \\ a_n \end{array} \right\} \quad \text{и} \quad \left[\begin{array}{c} a_1 \\ \ldots \\ a_n \end{array} \right]$$

соответственно.

Шкалой оценок называется полная решётка $\mathcal{B}$, в которой для каждой пары $a, b \in \mathcal{B}$ определён элемент

$$a \to b \tag{14.1}$$

обладающий следующим свойством: для каждого $c \in \mathcal{B}$

$$c \leq (a \to b) \quad \Leftrightarrow \quad (c \wedge a) \leq b \tag{14.2}$$

Элемент (14.1) можно интерпретировать как меру истинности высказывания

$$\text{“}a \leq b\text{”}$$

В нижеследующем тексте символ $\mathcal{B}$ обозначает некоторую фиксированную шкалу оценок.

Для каждой пары $a, b \in \mathcal{B}$ символом $a \leftrightarrow b$ будет ниже обозначаться элемент $(a \to b) \wedge (b \to a)$.

14.2.2 Нечёткие модальные формулы

Мы предполагаем, что задано некоторое множество $\mathcal{P}$, элементы которого называются **утверждениями**.

Множество Fm **нечётких модальных формул** (называемых ниже просто **формулами**) определяется индуктивно следующим образом:

- Каждый элемент множества $\mathcal{P}$ является формулой.
- Каждый элемент шкалы $\mathcal{B}$ является формулой.
- Если A и B – формулы, то знакосочетания $A \wedge B$, $A \vee B$, и $A \to B$ являются формулами.
- Если A – формула, и $a \in \mathcal{B}$, то знакосочетание $\Box_a A$ является формулой.

Модальные связки вида $\Box_a$ называются **нечёткими модальными операторами**.

При некоторых интерпретациях формул и оценок формулу вида $\Box_a A$ можно интерпретировать как высказывание

мера убедительности факта,
выражаемого формулой A, равна a.

Для произвольного списка $A_1, \ldots, A_n$ формул из Fm знакосочетания

$$A_1 \wedge A_2 \wedge \ldots \wedge A_n \;\text{ и }\; A_1 \vee A_2 \vee \ldots \vee A_n$$

являются сокращённой записью формул

$$A_1 \wedge (A_2 \wedge (\ldots \wedge A_n) \ldots) \;\text{ и }\; A_1 \vee (A_2 \vee (\ldots \vee A_n) \ldots)$$

соответственно. Данные формулы также будут обозначаться знакосочетаниями

$$\left\{ \begin{array}{c} A_1 \\ \ldots \\ A_n \end{array} \right\} \quad \text{и} \quad \left[\begin{array}{c} A_1 \\ \ldots \\ A_n \end{array} \right]$$

соответственно.

Для каждой пары $A, B \in Fm$ знакосочетание $A \leftrightarrow B$ является сокращённым обозначением формулы

$$(A \to B) \wedge (B \to A).$$

14.2.3 Подстановки

Подстановкой называется знакосочетание θ вида

$$\theta \;=\; [p_1 := A_1, \ldots, p_k := A_k] \tag{14.3}$$

где

- $p_1, \ldots, p_k$ – список различных утверждений из $\mathcal{P}$, и
- $A_1, \ldots, A_k$ – список формул.

Подстановка (14.3) действует на каждую формулу A путём замены для каждого $i \in \{1, \ldots, k\}$ каждого вхождения утверждения p_i в A на формулу A_i. Формула, которая получается после такой замены, обозначается знакосочетанием $\theta(A)$.

14.2.4 Тавтологии

Пусть A и B – некоторые формулы из Fm. Мы будем говорить, что B **получена из A эквивалентным преобразованием**, если

- A содержит подформулу вида

  $$a \wedge b, \;\; a \vee b, \;\; \text{или} \;\; a \to b$$

  где $a, b \in \mathcal{B}$, и
- B получается из A путём замены данной подформулы на элемент шкалы $\mathcal{B}$, являющийся результатом применения соответствующей операции к паре a, b.

Две формулы из Fm называются **эквивалентными**, если одну из них можно получить из другой путём нескольких эквивалентных преобразований.

Пусть A – формула, не содержащая модальных операторов, и список всех утверждений, входящих в A, имеет вид

$$(p_1, \ldots, p_n).$$

Формула A называется **тавтологией**, если для каждой подстановки θ вида (14.3), такой, что

$$\forall i \in \{1, \ldots, n\} \quad A_i = a_i \in \mathcal{B}$$

формула $\theta(A)$ эквивалентна элементу $1 \in \mathcal{B}$.

14.2.5 Нечёткие логики

Нечёткой логикой называется произвольное подмножество L множества Fm, обладающее следующими свойствами:

- каждая тавтология принадлежит L
- для всех $A, B \in Fm$ и каждого $a \in \mathcal{B}$

  $$\Box_a \left\{ \begin{array}{c} A \\ B \end{array} \right\} \;\leftrightarrow\; \left\{ \begin{array}{c} \Box_a A \\ \Box_a B \end{array} \right\} \;\; \in L, \tag{14.4}$$

- для каждого $a \in \mathcal{B}$

$$a \to \Box_a 1 \quad \in L, \tag{14.5}$$

- для каждой формулы $A \in Fm$ и каждого $a \in \mathcal{B}$

$$\Box_a A \to a \quad \in L, \tag{14.6}$$

- для всех $A, B \in Fm$

$$\begin{array}{ll} \textbf{если} & A \ \in L \quad \textbf{и} \quad A \to B \ \in L \\ \textbf{то} & B \ \in L \end{array} \tag{14.7}$$

- для каждой формулы $A \in Fm$ и каждой подстановки θ

$$\begin{array}{ll} \textbf{если} & A \in L \\ \textbf{то} & \theta(A) \in L \end{array} \tag{14.8}$$

- для всех $A, B \in Fm$ и всех $a, b \in \mathcal{B}$

$$\begin{array}{ll} \textbf{если} & a \to (A \to B) \ \in L \\ \textbf{то} & a \to (\Box_b A \to \Box_b B) \ \in L \end{array} \tag{14.9}$$

- для каждой формулы $A \in Fm$ и каждого подмножества $\{a_i \mid i \in \Im\} \subseteq \mathcal{B}$

$$\begin{array}{ll} \textbf{если} & \forall i \in \Im \quad a_i \to A \ \in L \\ \textbf{то} & (\sup\limits_{i \in \Im} a_i) \to A \quad \in L. \end{array} \tag{14.10}$$

Из данного определения вытекает, что существует минимальная (относительно включения) нечёткая логика, которую мы будем обозначать знакосочетанием FK (которое является аббревиатурой словосочетания *Fuzzy Kripke*).

Нетрудно доказать, что для каждой нечёткой логики L имеет место следующее правило вывода:

$$\begin{array}{ll} \textbf{если} & a_1 \to A_1 \ \in L, \ \ldots, \ a_n \to A_n \ \in L \\ & \left(\begin{array}{ll} \text{где} & a_1, \ldots, a_n \in \mathcal{B}, \quad \text{и} \\ & A_1, \ldots, A_n \in Fm \end{array} \right) \\ \textbf{то} & \left\{ \begin{array}{c} a_1 \\ \ldots \\ a_n \end{array} \right\} \to \left\{ \begin{array}{c} A_1 \\ \ldots \\ A_n \end{array} \right\} \ \in L. \end{array} \tag{14.11}$$

Ниже вместо термина "нечёткая логика" будет использоваться эквивалентный ему в данной главе термин "логика".

Для каждой формулы A и каждой логики L символ

$$[\![A]\!]_L$$

обозначает точную верхнюю грань множества

$$\{a \in \mathcal{B} \mid a \to A \quad \in L\}. \tag{14.12}$$

Из данного определения и из свойства (14.10) следует соотношение

$$\forall a \in \mathcal{B} \qquad a \to A \ \in L \quad \Leftrightarrow \quad a \leq [\![A]\!]_L.$$

14.3 Нечёткие модели Крипке

14.3.1 Нечёткие множества

Нечётким множеством называется пара

$$W = (X, \mu) \tag{14.13}$$

где

- X – множество (называемое **носителем** W), и
- μ – отображение вида

$$\mu : X \times X \to \mathcal{B}$$

обладающее следующими свойствами:

$$\forall x, y \in X \qquad \mu(x, y) = \mu(y, x) \tag{14.14}$$

$$\forall x, y, z \in X \qquad \left\{ \begin{array}{c} \mu(x, y) \\ \mu(y, z) \end{array} \right\} \leq \mu(x, z) \tag{14.15}$$

Для каждой пары $x, y \in X$ элемент $\mu(x, y)$ называется **мерой близости** x **и** y. Для каждого $x \in X$ элемент $\mu(x, x)$ называется **мерой принадлежности** элемента x нечёткому множеству (14.13).

Бинарным отношением на (14.13) называется произвольное отображение R вида

$$R : X \times X \to \mathcal{B}$$

удовлетворяющее следующим условиям:

$$\forall x, y, x', y' \in X \qquad \left\{ \begin{array}{c} R(x, y) \\ \mu(x, x') \\ \mu(y, y') \end{array} \right\} \leq R(x', y'), \tag{14.16}$$

$$\forall x, y \in X \qquad R(x, y) \leq \left\{ \begin{array}{c} \mu(x, x) \\ \mu(y, y) \end{array} \right\}. \tag{14.17}$$

Для каждой пары $(x, y) \in X \times X$ элемент $R(x, y)$ можно интерпретировать как **меру принадлежности** данной пары бинарному отношению R.

Подмножеством нечёткого множества (14.13) называется произвольное отображение s вида

$$s : X \to \mathcal{B}$$

удовлетворяющее следующим условиям:

$$\forall x, x' \in X \qquad \left\{ \begin{array}{c} s(x) \\ \mu(x, x') \end{array} \right\} \leq s(x'), \tag{14.18}$$

$$\forall x \in X \qquad s(x) \leq \mu(x, x). \tag{14.19}$$

Для каждого $x \in X$ элемент $s(x)$ можно интерпретировать как **меру принадлежности** элемента x подмножеству s.

Совокупность всех подмножеств нечёткого множества (14.13) обозначается символом $Sub(W)$.

Ниже для каждого нечёткого множества W его носитель будет обозначаться тем же самым символом W, и для каждой пары x, y элементов носителя мера близости x и y будет обозначаться символом $W(x, y)$. Кроме того, для каждого $x \in W$ символ $W(x)$ по определению обозначает меру принадлежности элемента x нечёткому множеству W.

14.3.2 Определение нечёткой модели Крипке

Нечёткой моделью Крипке называется произвольная тройка M вида

$$M = (W, \{R_a \mid a \in \mathcal{B}\}, \xi) \qquad (14.20)$$

компоненты которой определяются следующим образом:

1. W – это некоторое нечёткое множество, элементы которого называются **состояниями**,
2. $\{R_a \mid a \in \mathcal{B}\}$ – это $\mathcal{B}$–индексированная совокупность бинарных отношений на W, называемых **отношениями перехода**,
3. ξ – это отображение вида
$$\xi : \mathcal{P} \to Sub(W) \qquad (14.21)$$
называемое **оценкой утверждений**.

Ниже вместо термина "нечёткая модель Крипке" будет использоваться эквивалентный ему в данной главе термин "модель".

14.3.3 Оценка формул в моделях

Для каждой формулы $A \in Fm$ и каждой модели (14.20) **оценкой A в M** называется отображение

$$[\![A]\!]_M : W \to \mathcal{B},$$

которое сопоставляет каждому $x \in W$ оценку $[\![A]\!]_x \in \mathcal{B}$, определяемую следующим образом:

- для всех $p \in \mathcal{P}$
$$[\![p]\!]_x \stackrel{\text{def}}{=} \xi(p)(x), \qquad (14.22)$$
- для всех $a \in \mathcal{B}$
$$[\![a]\!]_x \stackrel{\text{def}}{=} \left\{ \begin{array}{l} a \\ W(x) \end{array} \right\}, \qquad (14.23)$$
- $$[\![A \wedge B]\!]_x \stackrel{\text{def}}{=} [\![A]\!]_x \wedge [\![B]\!]_x, \qquad (14.24)$$
- $$[\![A \vee B]\!]_x \stackrel{\text{def}}{=} [\![A]\!]_x \vee [\![B]\!]_x, \qquad (14.25)$$
- $$[\![A \to B]\!]_x \stackrel{\text{def}}{=} \left\{ \begin{array}{l} [\![A]\!]_x \to [\![B]\!]_x \\ W(x) \end{array} \right\}, \qquad (14.26)$$
- $$[\![\Box_a A]\!]_x \stackrel{\text{def}}{=} \left\{ \begin{array}{l} a \\ \inf\limits_{y \in W} (R_a(x,y) \to [\![A]\!]_y) \\ W(x) \end{array} \right\}. \qquad (14.27)$$

Нетрудно доказать, что отображение $[\![A]\!]_M$ является подмножеством нечёткого множества W.

14.3.4 Истинность формул в моделях

Формула $A \in Fm$ называется **истинной в точке** x модели (14.20), если имеет место соотношение

$$[\![A]\!]_x = W(x). \qquad (14.28)$$

Формула $A \in Fm$ называется **истинной в модели** (14.20), если она истинна в каждой точке этой модели.

Нетрудно доказать, что каждая формула логики FK истинна в каждой модели. Это следует из того, что

- каждая тавтология истинна в любой модели,
- формулы из соотношений (14.4), (14.5) и (14.6) истинны в произвольной модели, и
- правила вывода (14.7), (14.8), (14.9) и (14.10) сохраняют свойство истинности в произвольной модели.

Оставшая часть главы посвящена доказательству обратного утверждения: если формула истинна в каждой модели, то она принадлежит логике FK.

14.4 L–совместимые множества

14.4.1 Непротиворечивые логики

Логика $L \subseteq Fm$ называется **непротиворечивой**, если

$$\forall a \in \mathcal{B} \qquad a \in L \quad \Rightarrow \quad a = 1. \qquad (14.29)$$

Докажем, что логика FK непротиворечива.

Как было отмечено в параграфе 14.3.4, для каждого $a \in \mathcal{B}$, из соотношения $a \in FK$ следует, что формула a истинна в каждой модели, в частности, в модели вида (14.20), где W состоит из одного элемента x, и

$$W(x) = 1. \qquad (14.30)$$

Соотношение (14.29) следует из (14.23), (14.28) и (14.30).

■

Ниже под логикой понимается непротиворечивая логика.

14.4.2 Определение L–совместимого множества

Пусть

- L – некоторая непротиворечивая логика, и
- u – некоторое подмножество Fm.

Множество u называется **L–совместимым**, если для

- каждого конечного подмножества множества u, имеющего вид

$$\{a_1 \to A_1, \dots, a_n \to A_n\}$$
$$(\text{где } \ a_1, \dots, a_n \in \mathcal{B}, \ \ A_1, \dots, A_n \in Fm) \tag{14.31}$$

  и

- каждого $b \in \mathcal{B}$

из соотношения

$$\left\{ \begin{array}{c} A_1 \\ \dots \\ A_n \end{array} \right\} \to b \quad \in L \tag{14.32}$$

следует соотношение

$$\left\{ \begin{array}{c} a_1 \\ \dots \\ a_n \end{array} \right\} \leq b. \tag{14.33}$$

14.4.3 Свойства L–совместимых множеств

Для каждой пары u_1, u_2 подмножеств Fm неравенство

$$u_1 \leq u_2$$

означает, что

$$\text{для каждой формулы вида } \ a \to A \ \in u_1$$
$$a = 0 \ \text{ или } \ \exists\, b \geq a : \ b \to A \ \in u_2.$$

Теорема 1.
Для каждой пары u_1, u_2 подмножеств Fm из неравенства

$$u_1 \leq u_2$$

следует, что если u_2 – L–совместимо, то u_1 тоже L–совместимо.

■

Теорема 2.
Каждая непротиворечивая логика L является L–совместимым множеством.

Доказательство.
Применяя правило вывода (14.11) к подмножеству (14.31) множества L, получаем соотношение

$$\left\{ \begin{array}{c} a_1 \\ \dots \\ a_n \end{array} \right\} \to \left\{ \begin{array}{c} A_1 \\ \dots \\ A_n \end{array} \right\} \quad \in L. \tag{14.34}$$

Из (14.32), (14.34) и (14.7) следует соотношение

$$\left\{ \begin{array}{c} a_1 \\ \dots \\ a_n \end{array} \right\} \to b \quad \in L \tag{14.35}$$

Из (14.35) и (14.29) следует (14.33).

■

Ниже символ L обозначает произвольную непротиворечивую логику.

Теорема 3.
Пусть

- u – некоторое L–совместимое множество,
- A – некоторая формула, и
- Q – множество всех элементов $a \in \mathcal{B}$, таких, что

$$u \cup \{a \to A\} \quad L\text{–совместимо.} \tag{14.36}$$

Тогда для каждого $a \in \mathcal{B}$ имеет место соотношение

$$a \leq \sup(Q) \quad \Leftrightarrow \quad a \in Q.$$

Доказательство.
Заметим, что $Q \neq \emptyset$, т.к. $0 \in Q$.
Импликация

$$a \in Q \quad \Rightarrow \quad a \leq \sup(Q)$$

очевидна.
Импликация

$$a \leq \sup(Q) \quad \Rightarrow \quad a \in Q$$

эквивалентна следующей паре утверждений:

1. множество
$$u \cup \{\sup(Q) \to A\} \tag{14.37}$$
   является L–совместимым
2. если множество
$$u \cup \{a \to A\}$$
   L–совместимо, то для каждого $a' \leq a$ множество
$$u \cup \{a' \to A\}$$
   тоже L–совместимо.

Утверждение 2 следует из теоремы 1.
Докажем утверждение 1: для

- каждого подмножества (14.31) множества (14.37), и
- каждого $b \in \mathcal{B}$

из (14.32) следует (14.33).
Так как u по предположению L–совместимо, то для доказательства импликации

$$(14.32) \quad \Rightarrow \quad (14.33)$$

достаточно рассмотреть лишь случай, когда множество (14.31) имеет следующий вид:

- $(a_1 \to A_1) = (\sup(Q) \to A)$
- $\forall\, i = 2, \ldots, n \quad (a_i \to A_i) \in u.$

В этом случае (14.33) имеет следующий вид:

$$\left\{ \begin{array}{l} \sup(Q) \\ a_2 \wedge \ldots \wedge a_n \end{array} \right\} \leq b \qquad (14.38)$$

(14.38) эквивалентно соотношению

$$\forall\, a \in Q \quad \left\{ \begin{array}{l} a \\ a_2 \wedge \ldots \wedge a_n \end{array} \right\} \leq b \qquad (14.39)$$

(14.39) следует из (14.36).
■

Элемент $\sup(Q)$, который однозначно определяется по A и u, обозначается ниже символом

$$[\![A]\!]_u \qquad (14.40)$$

Из определения элемента $[\![A]\!]_u$ вытекает, что для каждого $u \subseteq Fm$ имеет место импликация

$$\begin{array}{l} u \quad L\text{–совместимо} \quad \Rightarrow \quad \forall\, A \in Fm \\ u \cup \{[\![A]\!]_u \to A\} \quad L\text{–совместимо} \end{array} \qquad (14.41)$$

Теорема 4.
Пусть u_1 и u_2 – L–совместимые множества, такие, что

$$u_1 \leq u_2.$$

Тогда для каждой формулы A

$$[\![A]\!]_{u_2} \leq [\![A]\!]_{u_1}. \qquad (14.42)$$

Доказательство.
Так как

- множество
$$u_2 \cup \{[\![A]\!]_{u_2} \to A\}$$
L–совместимо, и
- $u_1 \cup \{[\![A]\!]_{u_2} \to A\} \leq u_2 \cup \{[\![A]\!]_{u_2} \to A\}$

то из теоремы 1 следует, что множество

$$u_1 \cup \{[\![A]\!]_{u_2} \to A\} \qquad (14.43)$$

L–совместимо.
Из L–совместимости (14.43) и из определения элемента $[\![A]\!]_{u_1}$ следует неравенство (14.42).
■

Теорема 5.
Пусть

- $u \subseteq Fm$ – некоторое L–совместимое множество, и
- A, B – пара формул, таких, что

$$A \to B \quad \in L \qquad (14.44)$$

Тогда имеет место неравенство

$$[\![A]\!]_u \leq [\![B]\!]_u \qquad (14.45)$$

Доказательство.
(14.45) эквивалентно L–совместимости множества

$$u \cup \{[\![A]\!]_u \to B\} \qquad (14.46)$$

т.е. утверждению о том, что для

- каждого подмножества (14.31) множества (14.46), и
- каждого $b \in \mathcal{B}$

из (14.32) следует (14.33).
Так как u по предположению L–совместимо, то для доказательства импликации

$$(14.32) \quad \Rightarrow \quad (14.33)$$

достаточно рассмотреть лишь тот случай, когда (14.31) имеет следующий вид:

- $(a_1 \to A_1) = ([\![A]\!]_u \to B)$
- для каждого $i = 2, \ldots, n$
$$a_i \to A_i \quad \in u \qquad (14.47)$$

В этом случае (14.32) эквивалентно соотношению

$$B \to (\left\{ \begin{array}{l} A_2 \\ \ldots \\ A_n \end{array} \right\} \to b) \quad \in L \qquad (14.48)$$

Из (14.44) и (14.48) следует соотношение

$$A \to (\left\{ \begin{array}{l} A_2 \\ \ldots \\ A_n \end{array} \right\} \to b) \quad \in L \qquad (14.49)$$

которое эквивалентно соотношению

$$\left\{ \begin{array}{l} A \\ A_2 \\ \ldots \\ A_n \end{array} \right\} \to b \quad \in L \qquad (14.50)$$

Так как множество

$$u \cup \{[\![A]\!]_u \to A\}$$

является L–совместимым, то из (14.47) и (14.50) следует неравенство

$$\left\{ \begin{array}{l} [\![A]\!]_u \\ a_2 \\ \ldots \\ a_n \end{array} \right\} \leq b \qquad (14.51)$$

которое эквивалентно (14.33) для данного случая.
■

Теорема 6.
Для

- каждого L–совместимого множества u, и
- каждой формулы $A \in Fm$

имеет место неравенство:

$$[\![A]\!]_L \leq [\![A]\!]_u \tag{14.52}$$

Доказательство.
(14.52) эквивалентно L–совместимости множества

$$u \cup \{[\![A]\!]_L \to A\} \tag{14.53}$$

т.е. утверждению о том, что для

- каждого подмножества (14.31) множества (14.53), и
- каждого $b \in \mathcal{B}$

из (14.32) следует (14.33).

Так как u по предположению L–совместимо, то для доказательства импликации

$$(14.32) \quad \Rightarrow \quad (14.33)$$

достаточно рассмотреть лишь тот случай, когда (14.31) имеет следующий вид:

- $(a_1 \to A_1) = ([\![A]\!]_L \to A)$
- для каждого $i = 2, \ldots, n$

$$a_i \to A_i \quad \in u \tag{14.54}$$

В этом случае (14.32) эквивалентно соотношению

$$A \to (\left\{\begin{array}{c} A_2 \\ \ldots \\ A_n \end{array}\right\} \to b) \quad \in L \tag{14.55}$$

Из соотношений

$$[\![A]\!]_L \to A \quad \in L$$

и (14.55) следует соотношение

$$[\![A]\!]_L \to (\left\{\begin{array}{c} A_2 \\ \ldots \\ A_n \end{array}\right\} \to b) \quad \in L \tag{14.56}$$

Из (14.56) следует соотношение

$$\left\{\begin{array}{c} A_2 \\ \ldots \\ A_n \end{array}\right\} \to ([\![A]\!]_L \to b) \quad \in L \tag{14.57}$$

Так как u по предположению L–совместимо, то из (14.54) и (14.57) следует неравенство

$$\left\{\begin{array}{c} a_2 \\ \ldots \\ a_n \end{array}\right\} \leq [\![A]\!]_L \to b \tag{14.58}$$

Из (14.58) следует (14.33).
■

14.5 L–полные множества

14.5.1 Определение L–полного множества

Пусть x – некоторое подмножество множества Fm.
Множество x называется L**–полным**, если

- x является L–совместимым,
- для каждой формулы $A \in Fm$

$$[\![A]\!]_x \to A \quad \in x. \tag{14.59}$$

14.5.2 Пополнение L–совместимых множеств

Пусть

- u – некоторое L–совместимое множество, и
- x – некоторое L–полное множество.

x называется **пополнением** u, если

$$u \leq x \tag{14.60}$$

Теорема 7.
Для каждого L–совместимого множества u существует пополнение x.
Доказательство.
Пусть последовательность

$$B_1, B_2, \ldots \tag{14.61}$$

есть некоторое перечисление всех формул из Fm.
Определим последовательность

$$u_1, u_2, \ldots$$

подмножеств множества Fm следующим образом:

- $u_1 \stackrel{\text{def}}{=} u$,
- для каждого $k \geq 1$

$$u_{k+1} \stackrel{\text{def}}{=} u_k \cup \{[\![B_k]\!]_{u_k} \to B_k\}$$

Из данного определения и из утверждения (14.41) следует, что для каждого $k \geq 1$ верно утверждение:

$$\begin{array}{l} \text{если } u_k \quad L\text{–совместимо,} \\ \text{то } u_{k+1} \text{ тоже } L\text{–совместимо.} \end{array} \tag{14.62}$$

Так как u_1 по предположению L–совместимо, то из (14.62) следует, что

$$\forall k \geq 1 \quad u_k \quad L\text{–совместимо}$$

Определим искомое множество x следующим образом:

$$x \stackrel{\text{def}}{=} \bigcup_{k \geq 1} u_k$$

Множество x является L–совместимым, поскольку для каждого его конечного подмножества вида (14.31) существует номер $k \geq 1$, такой, что данное подмножество содержится в множестве u_k (которое, как было отмечено выше, является L–совместимым).

Докажем, что для каждой формулы $A \in Fm$ верно свойство (14.59).

По определению последовательности (14.61), существует номер k, такой, что $A = B_k$.

Поскольку

$$[\![B_k]\!]_{u_k} \to B_k \quad \in x$$

то

$$[\![B_k]\!]_{u_k} \leq [\![B_k]\!]_x. \tag{14.63}$$

Поскольку $u_k \subseteq x$, то из теоремы 4 следует, что

$$[\![B_k]\!]_x \leq [\![B_k]\!]_{u_k}. \tag{14.64}$$

Объединяя (14.63) и (14.64), получаем равенство

$$[\![B_k]\!]_x = [\![B_k]\!]_{u_k}. \tag{14.65}$$

Следовательно,

$$[\![B_k]\!]_x \to B_k \quad = \quad [\![B_k]\!]_{u_k} \to B_k \quad \in u_{k+1} \subseteq x. \tag{14.66}$$

Из (14.66) вытекает (14.59) (при $A = B_k$).

Таким образом, множество x является L–полным.

Докажем, что x является пополнением множества u, т.е.

$$\forall\ (a \to A) \in u \qquad a \leq [\![A]\!]_x.$$

По определению x,

$$\exists k \geq 1: \quad A = B_k.$$

Так как

$$(a \to B_k) \in u \subseteq u_k$$

то

$$u_k \cup \{a \to B_k\} \quad L\text{–совместимо.} \tag{14.67}$$

Из (14.67) и (14.65) получаем:

$$a \leq [\![B_k]\!]_{u_k} = [\![B_k]\!]_x = A_x.$$

■

14.6 Свойства L–полных множеств

Теорема 8.

Пусть x – L–полное множество, и $a \in \mathcal{B}$. Тогда

$$[\![a]\!]_x = a \tag{14.68}$$

Доказательство.

Поскольку x является L–совместимым, то его одноэлементное подмножество $\{[\![a]\!]_x \to a\}$ обладает следующим свойством: для каждого $b \in \mathcal{B}$ из соотношения

$$a \to b \quad \in L \tag{14.69}$$

следует неравенство

$$[\![a]\!]_x \leq b \tag{14.70}$$

Поскольку (14.69) верно для $b = a$, то (14.70) тоже должно быть верно для $b = a$, т.е.

$$[\![a]\!]_x \leq a. \tag{14.71}$$

Для доказательства обратного неравенства докажем L–совместимость множества

$$x \cup \{a \to a\}. \tag{14.72}$$

Для этого необходимо доказать, что для

- каждого подмножества (14.31) множества (14.72), и
- каждого $b \in \mathcal{B}$

из (14.32) следует (14.33).

Так как x по предположению L–совместимо, то для доказательства импликации

$$(14.32) \quad \Rightarrow \quad (14.33)$$

достаточно рассмотреть лишь тот случай, когда (14.31) удовлетворяет следующим условиям:

$$(a_1 \to A_1) = (a \to a)$$

$$\forall i = 2, \ldots, n \qquad a_i \to A_i \quad \in x \tag{14.73}$$

В этом случае (14.32) эквивалентно соотношению

$$\left\{ \begin{array}{l} a \\ A_2 \\ \ldots \\ A_n \end{array} \right\} \to b \quad \in L \tag{14.74}$$

а (14.33) эквивалентно неравенству

$$\left\{ \begin{array}{l} a \\ a_2 \\ \ldots \\ a_n \end{array} \right\} \leq b \tag{14.75}$$

(14.74) эквивалентно соотношению

$$\left\{ \begin{array}{l} A_2 \\ \ldots \\ A_n \end{array} \right\} \to (a \to b) \quad \in L \tag{14.76}$$

Из (14.76) и из L–совместимости x следует неравенство

$$\left\{ \begin{array}{l} a_2 \\ \ldots \\ a_n \end{array} \right\} \leq a \to b \tag{14.77}$$

(14.75) следует из (14.77)

■

Во всех нижеследующих рассуждениях мы будем предполагать, что шкала $\mathcal{B}$ обладает следующим свойством:

$$\forall a \in \mathcal{B} \qquad (a \to 0) \to 0 = a. \tag{14.78}$$

Нетрудно доказать, что данное свойство эквивалентно тому, что $\mathcal{B}$ является булевой алгеброй, операции в которой определяются следующим образом: для всех $a, b \in \mathcal{B}$

$$a \wedge b \stackrel{\mathrm{def}}{=} \inf\{a, b\}, \quad a \vee b \stackrel{\mathrm{def}}{=} \sup\{a, b\}, \quad \neg a \stackrel{\mathrm{def}}{=} a \to 0.$$

Теорема 9.
Для

- каждого L–полного множества x, и
- каждой пары формул A, B

имеет место равенство

$$[\![A \to B]\!]_x = [\![A]\!]_x \to [\![B]\!]_x \tag{14.79}$$

Доказательство.
Для доказательства равенства (14.79) достаточно доказать неравенства

$$[\![A \to B]\!]_x \leq [\![A]\!]_x \to [\![B]\!]_x \tag{14.80}$$

и

$$[\![A]\!]_x \to [\![B]\!]_x \leq [\![A \to B]\!]_x \tag{14.81}$$

Докажем неравенство (14.80). Данное неравенство эквивалентно неравенству

$$\left\{ \begin{array}{l} [\![A \to B]\!]_x \\ [\![A]\!]_x \end{array} \right\} \leq [\![B]\!]_x \tag{14.82}$$

Неравенство (14.82) эквивалентно L–совместимости множества

$$x \cup \{\left\{ \begin{array}{l} [\![A \to B]\!]_x \\ [\![A]\!]_x \end{array} \right\} \to B\} \tag{14.83}$$

т.е. утверждению о том, что для

- каждого подмножества (14.31) множества (14.83), и
- каждого $b \in \mathcal{B}$

из (14.32) следует (14.33).

Так как x по предположению L–совместимо, то для доказательства импликации

$$(14.32) \quad \Rightarrow \quad (14.33)$$

достаточно рассмотреть лишь тот случай, когда (14.31) имеет следующий вид:

- $a_1 \to A_1 \quad = \quad \left\{ \begin{array}{l} [\![A \to B]\!]_x \\ [\![A]\!]_x \end{array} \right\} \to B$
- для каждого $i = 2, \ldots, n$

$$a_i \to A_i \quad \in x \tag{14.84}$$

В этом случае (14.32) эквивалентно соотношению

$$B \to (\left\{ \begin{array}{l} A_2 \\ \ldots \\ A_n \end{array} \right\} \to b) \quad \in L \tag{14.85}$$

а (14.33) эквивалентно неравенству

$$\left\{ \begin{array}{l} \left\{ \begin{array}{l} [\![A \to B]\!]_x \\ [\![A]\!]_x \end{array} \right\} \\ a_2 \\ \ldots \\ a_n \end{array} \right\} \leq b \tag{14.86}$$

Поскольку формула

$$\left\{ \begin{array}{l} A \\ A \to B \end{array} \right\} \to B$$

является тавтологией, то

$$\left\{ \begin{array}{l} A \\ A \to B \end{array} \right\} \to B \quad \in L \tag{14.87}$$

Из (14.85) и (14.87) следует, что

$$\left\{ \begin{array}{l} A \\ A \to B \end{array} \right\} \to (\left\{ \begin{array}{l} A_2 \\ \ldots \\ A_n \end{array} \right\} \to b) \quad \in L \tag{14.88}$$

Соотношение (14.88) эквивалентно соотношению

$$\left\{ \begin{array}{l} A \\ A \to B \\ A_2 \\ \ldots \\ A_n \end{array} \right\} \to b \quad \in L \tag{14.89}$$

Поскольку множество x по предположению является L–полным, то

$$[\![A]\!]_x \to A \quad \in x \tag{14.90}$$

и

$$[\![A \to B]\!]_x \to (A \to B) \quad \in x \tag{14.91}$$

Из (14.89), (14.90), (14.91), (14.84) и свойства L–совместимости множества x вытекает требуемое неравенство (14.86).

Теперь докажем неравенство (14.81). Данное неравенство эквивалентно L–совместимости множества

$$x \cup \{([\![A]\!]_x \to [\![B]\!]_x) \to (A \to B)\} \tag{14.92}$$

т.е. утверждению о том, что для

- каждого подмножества (14.31) множества (14.92), и

- каждого $b \in \mathcal{B}$

из (14.32) следует (14.33).

Так как x по предположению L–совместимо, то для доказательства импликации

$$(14.32) \quad \Rightarrow \quad (14.33)$$

достаточно рассмотреть лишь тот случай, когда (14.31) имеет следующий вид:

- $a_1 \to A_1 \quad = \quad ([\![A]\!]_x \to [\![B]\!]_x) \to (A \to B)$
- для каждого $i = 2, \ldots, n$

$$a_i \to A_i \quad \in x \tag{14.93}$$

В этом случае (14.32) эквивалентно соотношению

$$(A \to B) \to (\left\{ \begin{array}{l} A_2 \\ \ldots \\ A_n \end{array} \right\} \to b) \quad \in L \tag{14.94}$$

а (14.33) эквивалентно неравенству

$$\left\{ \begin{array}{l} [\![A]\!]_x \to [\![B]\!]_x \\ a_2 \\ \ldots \\ a_n \end{array} \right\} \leq b \tag{14.95}$$

Для доказательства неравенства (14.95) достаточно доказать эквивалентное ему неравенство

$$\left\{ \begin{array}{l} b \to 0 \\ a_2 \\ \ldots \\ a_n \end{array} \right\} \leq \left\{ \begin{array}{l} [\![A]\!]_x \\ [\![B]\!]_x \to 0 \end{array} \right\} \tag{14.96}$$

Для того, чтобы доказать неравенство (14.96), достаточно доказать пару неравенств:

$$\left\{ \begin{array}{l} b \to 0 \\ a_2 \\ \ldots \\ a_n \end{array} \right\} \leq [\![A]\!]_x \tag{14.97}$$

и

$$\left\{ \begin{array}{l} b \to 0 \\ a_2 \\ \ldots \\ a_n \end{array} \right\} \leq [\![B]\!]_x \to 0 \tag{14.98}$$

Докажем неравенство (14.97). Данное неравенство эквивалентно L–совместимости множества

$$x \cup \{\left\{ \begin{array}{l} b \to 0 \\ a_2 \\ \ldots \\ a_n \end{array} \right\} \to A\} \tag{14.99}$$

т.е. утверждению о том, что для

- каждого конечного подмножества множества (14.99) вида
$$\{c_1 \to C_1, \ldots, c_m \to C_m\}$$
такого, что
$$c_1 \to C_1 \quad = \quad \left\{ \begin{array}{l} b \to 0 \\ a_2 \\ \ldots \\ a_n \end{array} \right\} \to A$$
$$\forall i = 2, \ldots, m \qquad c_i \to C_i \quad \in x \tag{14.100}$$
и
- каждого $d \in \mathcal{B}$

из соотношения

$$\left\{ \begin{array}{l} A \\ C_2 \\ \ldots \\ C_m \end{array} \right\} \to d \quad \in L \tag{14.101}$$

следует неравенство

$$\left\{ \begin{array}{l} \left\{ \begin{array}{l} b \to 0 \\ a_2 \\ \ldots \\ a_n \end{array} \right\} \\ c_2 \\ \ldots \\ c_m \end{array} \right\} \leq d \tag{14.102}$$

Для доказательства неравенства (14.102) достаточно доказать эквивалентное ему неравенство

$$\left\{ \begin{array}{l} a_2 \wedge \ldots \wedge a_n \\ c_2 \wedge \ldots \wedge c_m \end{array} \right\} \leq (b \to 0) \to d \tag{14.103}$$

Из соотношения (14.101) вытекает соотношение

$$A \to (\left\{ \begin{array}{l} C_2 \\ \ldots \\ C_m \end{array} \right\} \to d) \quad \in L$$

из которого следует соотношению

$$((\left\{ \begin{array}{l} C_2 \\ \ldots \\ C_m \end{array} \right\} \to d) \to B) \to (A \to B) \quad \in L \tag{14.104}$$

Из (14.104) и (14.94) следует соотношение

$$((\left\{ \begin{array}{l} C_2 \\ \ldots \\ C_m \end{array} \right\} \to d) \to B) \to (\left\{ \begin{array}{l} A_2 \\ \ldots \\ A_n \end{array} \right\} \to b) \quad \in L \tag{14.105}$$

Поскольку формула

$$\left\{ \begin{array}{l} \left\{ \begin{array}{l} C_2 \\ \ldots \\ C_m \end{array} \right\} \\ d \to B \end{array} \right\} \to ((\left\{ \begin{array}{l} C_2 \\ \ldots \\ C_m \end{array} \right\} \to d) \to B)$$

является тавтологией, то она принадлежит L. Отсюда и из (14.105) следует соотношение

$$\left\{\begin{array}{l} d \to B \\ A_2 \wedge \ldots \wedge A_n \\ C_2 \wedge \ldots \wedge C_m \end{array}\right\} \to b \quad \in L \tag{14.106}$$

Из (14.106), (14.93), (14.100) и из L–совместимости множества x вытекает неравенство

$$\left\{\begin{array}{l} [\![d \to B]\!]_x \\ a_2 \wedge \ldots \wedge a_n \\ c_2 \wedge \ldots \wedge c_m \end{array}\right\} \leq b$$

которое эквивалентно неравенству

$$\left\{\begin{array}{l} a_2 \wedge \ldots \wedge a_n \\ c_2 \wedge \ldots \wedge c_m \end{array}\right\} \leq [\![d \to B]\!]_x \to b \tag{14.107}$$

Докажем, что имеет место неравенство

$$[\![d \to B]\!]_x \to b \leq (b \to 0) \to d \tag{14.108}$$

(14.108) эквивалентно неравенству

$$\left\{\begin{array}{l} [\![d \to B]\!]_x \to b \\ b \to 0 \end{array}\right\} \leq d \tag{14.109}$$

Так как имеет место неравенство

$$\left\{\begin{array}{l} [\![d \to B]\!]_x \to b \\ b \to 0 \end{array}\right\} \leq [\![d \to B]\!]_x \to 0$$

то для доказательства (14.109) достаточно доказать неравенство

$$[\![d \to B]\!]_x \to 0 \leq d \tag{14.110}$$

(14.110) эквивалентно неравенству

$$d \to 0 \leq [\![d \to B]\!]_x \tag{14.111}$$

Докажем неравенство (14.111). Поскольку формула

$$(d \to 0) \to (d \to B)$$

является тавтологией, то, следовательно,

$$(d \to 0) \to (d \to B) \quad \in L \tag{14.112}$$

Из (14.112) и из теоремы 5 следует неравенство

$$[\![d \to 0]\!]_x \leq [\![d \to B]\!]_x \tag{14.113}$$

Из (14.113) и из теоремы 8 следует неравенство (14.111).

Из истинности неравенства (14.111) следует истинность неравенства (14.108), а из истинности неравенств (14.107) и (14.108) следует истинность неравенства (14.103).

Таким образом, L–совместимость множества (14.99) установлена, и, следовательно, неравенство (14.97) доказано.

Теперь докажем неравенство (14.98). Данное неравенство эквивалентно неравенству

$$\left\{\begin{array}{l} [\![B]\!]_x \\ a_2 \\ \ldots \\ a_n \end{array}\right\} \leq b \tag{14.114}$$

(14.114) имеет место потому, что

1. из (14.94) и из соотношения

   $$B \to (A \to B) \quad \in L$$

   следует соотношение

   $$B \to (\left\{\begin{array}{c} A_2 \\ \ldots \\ A_n \end{array}\right\} \to b) \quad \in L,$$

   которое эквивалентно соотношению

   $$\left\{\begin{array}{l} B \\ A_2 \\ \ldots \\ A_n \end{array}\right\} \to b \quad \in L,$$

2. $\{([\![B]\!]_x \to B), (a_2 \to A_2), \ldots, (a_n \to A_n)\} \subseteq x$, и
3. x является L–совместимым.

■

Теорема 10.
Пусть

- x – некоторое L–полное множество, и
- A, B – пара формул.

Тогда имеет место равенство

$$[\![A \wedge B]\!]_x = [\![A]\!]_x \wedge [\![B]\!]_x \tag{14.115}$$

Доказательство.
Для доказательства равенства (14.115) достаточно доказать неравенства

$$[\![A \wedge B]\!]_x \leq [\![A]\!]_x, \qquad [\![A \wedge B]\!]_x \leq [\![B]\!]_x, \tag{14.116}$$

и

$$[\![A]\!]_x \wedge [\![B]\!]_x \leq [\![A \wedge B]\!]_x \tag{14.117}$$

Неравенства (14.116) следуют из соотношений

$$\begin{array}{ll} (A \wedge B) \to A & \in L \\ (A \wedge B) \to B & \in L \end{array}$$

и из теоремы 5.

Неравенство (14.117) следует из L–совместимости множества

$$x \cup \{(([\![A]\!]_x \wedge [\![B]\!]_x) \to (A \wedge B)\}$$

■

Теорема 11.
Пусть

- x – некоторое L–полное множество, и
- A, B – пара формул.

Тогда имеет место равенство

$$[\![A \vee B]\!]_x = [\![A]\!]_x \vee [\![B]\!]_x \tag{14.118}$$

Доказательство.
Равенство (14.118) эквивалентно равенству

$$([\![A]\!]_x \vee [\![B]\!]_x) \to 0 = [\![A \vee B]\!]_x \to 0 \tag{14.119}$$

(14.119) вытекает из следующих соотношений:

$$\begin{array}{lcll} ([\![A]\!]_x \vee [\![B]\!]_x) \to 0 & = & \left\{ \begin{array}{c} [\![A]\!]_x \to 0 \\ [\![B]\!]_x \to 0 \end{array} \right\} & = \\ = \left\{ \begin{array}{c} [\![A]\!]_x \to [\![0]\!]_x \\ [\![B]\!]_x \to [\![0]\!]_x \end{array} \right\} & = & \left\{ \begin{array}{c} [\![A \to 0]\!]_x \\ [\![B \to 0]\!]_x \end{array} \right\} & = \\ = [\![\left\{ \begin{array}{c} A \to 0 \\ B \to 0 \end{array} \right\}]\!]_x & = & [\![(A \vee B) \to 0]\!]_x & = \\ = [\![A \vee B]\!]_x \to [\![0]\!]_x & = & [\![A \vee B]\!]_x \to 0 & \end{array}$$

■

Теорема 12.
Пусть x – некоторое L–полное множество.
Для каждой формулы $A \in Fm$ и каждого элемента $a \in \mathcal{B}$ имеет место неравенство

$$[\![\Box_a A]\!]_x \leq a. \tag{14.120}$$

Доказательство.
Из (14.6) следует соотношение

$$(a \to 0) \to (\Box_a A \to 0) \quad \in L \tag{14.121}$$

из которого, согласно теоремам 5 и 8, следует неравенство

$$a \to 0 \ \leq \ [\![\Box_a A \to 0]\!]_x \tag{14.122}$$

Поскольку, согласно теоремам 9 и 8,

$$[\![\Box_a A \to 0]\!]_x = [\![\Box_a A]\!]_x \to [\![0]\!]_x = [\![\Box_a A]\!]_x \to 0 \tag{14.123}$$

то из (14.122) и (14.123) следует неравенство

$$a \to 0 \ \leq \ [\![\Box_a A]\!]_x \to 0, \tag{14.124}$$

которое эквивалентно (14.120).

■

14.7 Канонические модели

14.7.1 Определение канонической модели

Канонической моделью логики L называется модель

$$M_L \stackrel{\text{def}}{=} (W_L, \{(R_L)_a \mid a \in \mathcal{B}\}, \xi_L)$$

компоненты которой определяются следующим образом:

- W_L состоит из всех L–полных множеств.

  Для каждой пары $x, y \in W_L$

  $$W_L(x,y) \stackrel{\text{def}}{=} \inf_{A \in Fm} ([\![A]\!]_x \leftrightarrow [\![A]\!]_y) \tag{14.125}$$

  Заметим, что из данного определения вытекает соотношение

  $$\forall x \in W_L \qquad W_L(x) = 1. \tag{14.126}$$

  Нетрудно доказать, что определение W_L удовлетворяет условиям (14.14) и (14.15).

- Для каждого $a \in \mathcal{B}$ символ $(R_L)_a$ обозначает нечёткое бинарное отношение на W_L

  $$(R_L)_a : W_L \times W_L \to \mathcal{B}$$

  определяемое следующим образом:

  $$\begin{array}{c} \forall x, y \in W_L \\ (R_L)_a(x,y) \stackrel{\text{def}}{=} \inf\limits_{A \in Fm} ([\![\Box_a A]\!]_x \to [\![A]\!]_y) \end{array} \tag{14.127}$$

  Нетрудно доказать, что определение $(R_L)_a$ удовлетворяет условиям (14.16) и (14.17).

- ξ_L – это отображение вида

  $$\xi_L : \mathcal{P} \to Sub(W_L)$$

  где для каждого $p \in \mathcal{P}$ нечёткое подмножество

  $$\xi_L(p) : W_L \to \mathcal{B}$$

  определяется следующим образом:

  $$\forall x \in W_L \qquad \xi_L(p)(x) \stackrel{\text{def}}{=} [\![p]\!]_x. \tag{14.128}$$

  Нетрудно доказать, что для каждого $p \in \mathcal{P}$ отображение $\xi_L(p)$ удовлетворяет условиям (14.18) и (14.19).

14.7.2 Основное свойство канонических моделей

Теорема 13.
Для каждой формулы $A \in Fm$ и каждого $x \in W_L$

$$[\![A]\!](x) = [\![A]\!]_x \tag{14.129}$$

Доказательство.
Докажем данную теорему индукцией по структуре формулы A.

$A = p \in \mathcal{P}$

В этом случае равенство (14.129) следует из (14.128).

$A = a \in \mathcal{B}$

Из (14.23), (14.126) и (14.68) следуют соотношения

$$[\![a]\!](x) = \left\{ \begin{array}{l} a \\ W_L(x) \end{array} \right\} = \left\{ \begin{array}{l} a \\ 1 \end{array} \right\} = a = [\![a]\!]_x$$

$A = B \wedge C,\ A = B \vee C,\ A = B \to C$

По индуктивному предположению,

$$\forall x \in W_L \qquad [\![B]\!](x) = [\![B]\!]_x, \quad [\![C]\!](x) = [\![C]\!]_x.$$

Согласно теореме 10, из L–полноты множества x следует соотношение

$$[\![B]\!]_x \wedge [\![C]\!]_x = [\![B \wedge C]\!]_x$$

Следовательно,

$$[\![A]\!](x) = [\![B \wedge C]\!](x) \stackrel{\text{def}}{=}$$

$$\stackrel{\text{def}}{=} [\![B]\!](x) \wedge [\![C]\!](x) = [\![B]\!]_x \wedge [\![C]\!]_x =$$

$$= [\![B \wedge C]\!]_x = [\![A]\!]_x.$$

Случаи $A = B \vee C$ и $A = B \to C$ разбираются аналогично.

$A = \Box_a B$

По индуктивному предположению,

$$\forall y \in W_L \qquad [\![B]\!](y) = [\![B]\!]_y. \tag{14.130}$$

Докажем, что элемент

$$[\![\Box_a B]\!](x) \tag{14.131}$$

совпадает с элементом

$$[\![\Box_a B]\!]_x. \tag{14.132}$$

Из (14.130), (14.126), и (14.27) следует, что элемент (14.131) совпадает с элементом

$$\left\{ \begin{array}{l} a \\ \inf\limits_{y \in W_L} ((R_L)_a(x,y) \to [\![B]\!]_y) \end{array} \right\}. \tag{14.133}$$

Для доказательства равенства (14.132) = (14.133) мы докажем, что

- (14.132) $\leq$ (14.133), и
- (14.132) $\geq$ (14.133).

Неравенство (14.132) $\leq$ (14.133) следует из (14.120) и из неравенства

$$[\![\Box_a B]\!]_x \leq \inf_{y \in W_L} ((R_L)_a(x,y) \to [\![B]\!]_y) \tag{14.134}$$

Для доказательства неравенства (14.134) достаточно доказать, что для каждого $y \in W_L$

$$\left\{ \begin{array}{l} (R_L)_a(x,y) \\ [\![\Box_a B]\!]_x \end{array} \right\} \leq [\![B]\!]_y \tag{14.135}$$

Неравенство (14.135) следует из соотношения (14.127).

Теперь докажем неравенство (14.132) $\geq$ (14.133). Для доказательства данного неравенства будет достаточно построить элемент $y \in W_L$, такой, что

$$\left\{ \begin{array}{l} a \\ (R_L)_a(x,y) \to [\![B]\!]_y \end{array} \right\} \leq [\![\Box_a B]\!]_x \tag{14.136}$$

Обозначим символом u множество, состоящее из всех формул вида

$$\left\{ \begin{array}{l} [\![\Box_a A]\!]_x \\ [\![\Box_a B]\!]_x \to 0 \end{array} \right\} \to A \tag{14.137}$$

а также из формулы

$$([\![\Box_a B]\!]_x \to 0) \to (B \to 0) \tag{14.138}$$

Лемма.

Множество u является L–совместимым.

Доказательство.

Докажем, что для

- каждого конечного подмножества (14.31) множества u, и
- каждого $b \in \mathcal{B}$

из (14.32) следует (14.33).

Сначала рассмотрим случай, когда

$$(14.138) \in (14.31).$$

Пусть (14.31) имеет следующий вид:

- $a_1 \to A_1 \ = \ (14.138)$
- для каждого $i = 2, \ldots, n$

$$a_i = \left\{ \begin{array}{l} [\![\Box_a A_i]\!]_x \\ [\![\Box_a B]\!]_x \to 0 \end{array} \right\} \tag{14.139}$$

В этом случае (14.32) имеет вид

$$\left\{ \begin{array}{l} B \to 0 \\ A_2 \\ \ldots \\ A_n \end{array} \right\} \to b \quad \in L \tag{14.140}$$

Из (14.140) вытекают соотношения

$$(b\to 0)\to(\left\{\begin{array}{l} B\to 0\\ A_2\\ \dots\\ A_n\end{array}\right\}\to 0)\quad \in L \qquad \Rightarrow$$

$$(b\to 0)\to(\left\{\begin{array}{l} A_2\\ \dots\\ A_n\end{array}\right\}\to B)\quad \in L \qquad \Rightarrow$$

$$(b\to 0)\to(\left\{\begin{array}{l} \Box_a A_2\\ \dots\\ \Box_a A_n\end{array}\right\}\to \Box_a B)\quad \in L \qquad \Rightarrow$$

$$b\to 0\ \leq\ \left\{\begin{array}{l} [\![\Box_a A_2]\!]_x\\ \dots\\ [\![\Box_a A_n]\!]_x\end{array}\right\}\to [\![\Box_a B]\!]_x$$

Последнее неравенство эквивалентно неравенству

$$\left\{\begin{array}{l} b\to 0\\ [\![\Box_a A_2]\!]_x\\ \dots\\ [\![\Box_a A_n]\!]_x\end{array}\right\}\leq [\![\Box_a B]\!]_x. \qquad (14.141)$$

Из (14.141) следует неравенство

$$\left\{\begin{array}{l} [\![\Box_a B]\!]_x\to 0\\ [\![\Box_a A_2]\!]_x\\ \dots\\ [\![\Box_a A_n]\!]_x\end{array}\right\}\leq b. \qquad (14.142)$$

Неравенство (14.142) эквивалентно искомому неравенству (14.33) для данного случая.

Теперь рассмотрим случай, когда (14.138) $\notin$ (14.31).

Так как формула

$$\left\{\begin{array}{l} B\to 0\\ A_1\\ \dots\\ A_n\end{array}\right\}\to\left\{\begin{array}{l} A_1\\ \dots\\ A_n\end{array}\right\}$$

является тавтологией, то из (14.32) следует соотношение

$$\left\{\begin{array}{l} B\to 0\\ A_1\\ \dots\\ A_n\end{array}\right\}\to b\quad \in L \qquad (14.143)$$

Как уже было показано выше в данном доказательстве, из последнего соотношения вытекает неравенство

$$\left\{\begin{array}{l} [\![\Box_a B]\!]_x\to 0\\ [\![\Box_a A_1]\!]_x\\ \dots\\ [\![\Box_a A_n]\!]_x\end{array}\right\}\leq b. \qquad (14.144)$$

Неравенство (14.144) эквивалентно искомому неравенству (14.33) для данного случая.

■

Пусть символ y обозначает L–пополнение множества u.

Из определения множеств u и y следует, что

$$[\![\Box_a B]\!]_x\to 0\leq [\![B\to 0]\!]_y=[\![B]\!]_y\to 0 \qquad (14.145)$$

и для каждой формулы $A\in Fm$

$$\left\{\begin{array}{l} [\![\Box_a A]\!]_x\\ [\![\Box_a B]\!]_x\to 0\end{array}\right\}\leq [\![A]\!]_y. \qquad (14.146)$$

Из (14.145) следует неравенство

$$[\![B]\!]_y\leq [\![\Box_a B]\!]_x. \qquad (14.147)$$

Из (14.146) следует, что $\forall A\in Fm$

$$[\![\Box_a B]\!]_x\to 0\ \leq\ [\![\Box_a A]\!]_x\to [\![A]\!]_y \qquad (14.148)$$

Из (14.148) и (14.127) следует неравенство

$$\left\{\begin{array}{l} a\\ [\![\Box_a B]\!]_x\to 0\end{array}\right\}\leq (R_L)_a(x,y). \qquad (14.149)$$

Искомое неравенство (14.136) следует из (14.147), (14.149), и из неравенства

$$\left\{\begin{array}{l} a\\ \left\{\begin{array}{l} a\\ c\to 0\end{array}\right\}\to c\end{array}\right\}\leq c \qquad (14.150)$$

где $c\stackrel{\text{def}}{=}[\![\Box_a B]\!]_x$.

Докажем неравенство (14.150). Данное неравенство эквивалентно неравенству

$$c\to 0\ \leq\ \left\{\begin{array}{l} a\\ \left\{\begin{array}{l} a\\ c\to 0\end{array}\right\}\to c\end{array}\right\}\to 0, \qquad (14.151)$$

т.е.

$$\left\{\begin{array}{l} c\to 0\\ a\\ \left\{\begin{array}{l} a\\ c\to 0\end{array}\right\}\to c\end{array}\right\}\leq 0, \qquad (14.152)$$

которое, очевидно, истинно.

■

14.8 Полнота логики FK

Теорема 14.

Для каждой формулы $A\in Fm$ следующие условия эквивалентны:

$$A\in FK \qquad (14.153)$$

$$A \text{ истинна в каждой модели.} \qquad (14.154)$$

Доказательство.

Импликация

$$(14.153) \quad \Rightarrow \quad (14.154)$$

была обоснована в параграфе 14.3.4.

Докажем, что если $A \notin FK$, то A не является истинной в некоторой точке канонической модели логики FK.

Лемма.

Множество

$$\{([\![A]\!]_{FK} \to 0) \to (A \to 0)\} \qquad (14.155)$$

является FK–совместимым.

Доказательство.

Докажем, что для каждого $b \in \mathcal{B}$ из соотношения

$$(A \to 0) \to b \quad \in FK \qquad (14.156)$$

следует неравенство

$$[\![A]\!]_{FK} \to 0 \leq b \qquad (14.157)$$

Из (14.156) следуют соотношения

$$\begin{aligned} &(b \to 0) \to A \quad \in FK && \Rightarrow \\ &b \to 0 \ \leq \ [\![A]\!]_{FK} && \Rightarrow \\ &[\![A]\!]_{FK} \to 0 \ \leq \ b \end{aligned}$$

Таким образом, множество (14.155) FK–совместимо.

■

Согласно теореме 7, из FK–совместимости множества (14.155) следует, что

$$\exists x \in W_{FK} : \quad [\![A]\!]_{FK} \to 0 \ \leq \ [\![A \to 0]\!]_x \qquad (14.158)$$

Так как множество x является FK–полным, то согласно теореме 9 из (14.158) следует, что

$$[\![A \to 0]\!]_x = [\![A]\!]_x \to [\![0]\!]_x = [\![A]\!]_x \to 0 \qquad (14.159)$$

Из (14.129), (14.158) и (14.159) вытекает соотношение

$$[\![A]\!]_{FK} \to 0 \ \leq \ [\![A]\!](x) \to 0 \qquad (14.160)$$

которое эквивалентно соотношению

$$[\![A]\!](x) \ \leq \ [\![A]\!]_{FK} \qquad (14.161)$$

Докажем, что формула A не является истинной в точке x.

Если A истинна в x, то из (14.28) и (14.126) следует что

$$[\![A]\!](x) = 1 \qquad (14.162)$$

Из (14.161) и (14.162) следует равенство $[\![A]\!]_{FK} = 1$, из которого вытекает соотношение $A \in FK$, которое противоречит предположению о том, что $A \notin FK$.

■