Снимаю с себя всю ответственность за нули на коллоквиуме, полученные из-за прочтения фактов с этого конспекта. По всем неточностям и предложениям: @helloclock.

Содержание

1 Лекция 1 (введение) **3**

2 Лекция 2 (модели, ДНФ) **4**

2.1 Модели . . . 4

2.2 Виды формул . . . 4

2.3 ДНФ . . . 5

2.4 Алгоритмическая сложность . . . 5

2.4.1 Задача о нахождении ДНФ по таблице истинности . . . 5

2.4.2 Задача о проверке тавтологичности . . . 5

3 Лекция 3 (полнота и максимальность) **7**

4 Лекция 4 (теорема Поста) **10**

4.1 Продолжение про классы функций . . . 10

4.2 Замены . . . 12

5 Лекция 5 (выводы) **13**

5.1 Правила вывода . . . 13

5.2 Конкретные правила . . . 14

6 Лекция 6 (продолжение про выводы) **15**

6.1 Примеры допустимых правил . . . 15

6.2 Противоречивость и непротиворечивость . . . 17

7 Лекция 7 **19**

7.1 Основное множество правил . . . 19

8 Лекция 8 **23**

8.1 Доказательства аксиом . . . 24

9 Лекция 9 (логика предикатов) **27**

10 Лекция 10 **29**

10.1 Выразимые предикаты 30

10.2 Изоморфизмы 31

11 Лекция 11 **33**

12 Лекция 12 TODO **36**

13 Лекция 13 **37**

13.1 Выводы 37

13.2 Ограничения на подстановки 37

13.3 Схемы аксиом 38

1 Лекция 1 (введение)

Определение 1.1. *Алфавит* $\Sigma = \{\,(,),\wedge,\vee,\neg,\to\,\} \cup \mathrm{Prop} \cup \{\,\mathrm{True},\mathrm{False}\,\}$, где Prop — множество пропозициональных переменных. В курсе $\mathrm{Prop} = \{\,p,\ldots,z,p_1,\ldots,z_1,\ldots\,\}$.

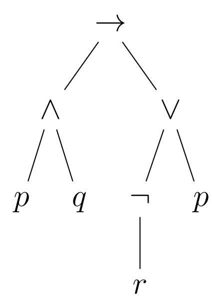
Определение 1.2. *Формула* — последовательность символов из алфавита, определяемая по индукции:

1. T и F — формулы;
2. $p \in \mathrm{Prop}$ — формула;
3. A — формула $\implies$ $\neg A$ — формула;
4. A, B — формулы $\implies$ $(A \wedge B), (A \vee B), (A \to B)$ — формулы.

Формулы удобно представлять в виде дерева, например для формулы

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

дерево выглядит следующим образом:



Определение 1.3. Пусть A — последовательность символов в алфавите Σ:

$$A = a_1 \ldots a_n \ (a_j \in \Sigma).$$

Тогда B — *префикс* ($B \sqsubseteq A$), если $B = a_1 \ldots a_k$ ($k \leqslant n$).

Лемма 1.1. *Если A — корректная формула и A' — её префикс, то A' — не корректная формула.*

Лемма 1.2 (Об однозначности разбора)**.** *Если A — корректно построена, то верно ровно одно из следующего:*

1. $A \in \mathrm{Prop}$
2. $A \in \{\,\top,\bot\,\}$
3. $\exists!\, B\colon A = \neg B$
4. $\exists!\, B, C\colon A = (B * C)$, *где* $* \in \{\,\wedge,\vee,\to\,\}$

2 Лекция 2 (модели, ДНФ)

2.1 Модели

Определение 2.1. *Модель* — функция $\mathrm{Var} \to \mathbb{B} = \{0, 1\}$. Но т.к. Var бесконечно, в программах будем считать моделью любую функцию из конечного множества переменных. В таком случае некоторым переменным значение не приписывается.

Модель задаёт интерпретацию истинности всех формул.

Для формулы A *истинность* формулы в модели M задаётся по индукции и обозначается $M(A)$:

- $M(\top) = 1$, $M(\bot) = 0$;
- На переменных уже задано;
- $M(\neg B) = 1 - M(B)$, если $A = \neg B$;
- $M(B_1 \odot B_2) = M(B_1) \odot M(B_2)$, если $A = (B_1 \odot B_2)$, $\odot \in \{\vee, \wedge, \to\}$.

Определение 2.2. *Булевая функция* — отображение $\mathbb{B}^k \to \mathbb{B}$, задаёт булеву функцию данной формулу для фиксированного порядка переменных.

2.2 Виды формул

Определение 2.3. *Тавтология* — формула, истинная во всех моделях

Пример: $p \to p$, $p \vee \neg p$

Определение 2.4. *Тождественно ложная/противоречивая* формула — формула, ложная во всех моделях.

Пример: $p \wedge \neg p$

Определение 2.5. *Выполнимая* формула — формула, истинная хотя бы в одной модели.

Пример: $p \wedge q$

Пример:

Если в пробах с Европы (спутник Юпитера) обнаружены бактерии, то на Европе есть жизнь или бактерии были занесены с Земли. Если бактерии были занесены с Земли, то на Земле есть похожие бактерии. В пробах с Европы обнаружены бактерии, похожие на Земные, следовательно на Европе нет жизни.

- p — "В пробах с Европы обнаружены бактерии"
- q — "На Европе есть жизнь"
- r — "Бактерии с Земли"
- s — "Бактерии похожи не Земные"

Утверждение можно записать следующей формулой:

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

Если она тавтологична, то утверждение верно, иначе — нет.

Чтобы проверить на тавтологичность, надо проверить, есть ли набор переменных, для которого формула ложна, тогда она будет не тавтологична. Для этого первая скобка должна быть истинной, а вторая — ложной. Отсюда $q = \top$, $(p \to q \vee r) = \top$, $(r \to s) = \top$, $s = \top$. Из имеющегося получаем $p = q = r = s = \top$. Для этого набора переменных утверждение ложно, т.е. оно не тавтологично, а значит — не истинно во всех моделях. □

2.3 ДНФ

Определение 2.6. *Литерал* — переменная или её отрицание.

Определение 2.7. *Элементарная конъюнкция/конъюнкт* — конъюнкция литералов.

Определение 2.8. *Дизъюнктивная нормальная форма (ДНФ)* — дизъюнкция конъюнктов.

Определение 2.9. *Совершенная дизъюнктивная нормальная форма (СДНФ)*:

- Определена для фиксированного множества переменных;
- ДНФ, в которой в каждом конъюнкте участвуют все переменные из множества и только один раз.

Построение СДНФ:

- Можно построить по таблице истинности при условии, что в ней есть хотя бы одна 1;
- Каждая строка преобразуется в элементарную конъюнкцию, которая истинна только на данном наборе переменных и ложна на всех остальных;
- Итоговая формула — дизъюнкция построенных конъюнктов.

Теорема 2.1 (Теорема о функциональной полноте)**.** *Для любой булевой функции существует булева формула, задающая эту функцию.*

2.4 Алгоритмическая сложность

2.4.1 Задача о нахождении ДНФ по таблице истинности

- Прямой алгоритм перебирает строки таблицы истинности;
- Полиномиальная сложность по размеру таблицы истинности.

2.4.2 Задача о проверке тавтологичности

- Проверяет, истинна ли формула во всех моделях;
- Связана с проблемой SAT (проблема выполнимости);

- NP-полнота: нахождение эффективного алгоритма неизвестно;
- Есть очень хорошие SAT-решатели, которые применяют различные эвристики и быстро работают на формулах, которые появляются в реальных задачах.

3 Лекция 3 (полнота и максимальность)

Определение 3.1. *Арность* операции (функции) — количество аргументов.

Арность может быть равной 0 — это константы.

Арность:

- 0 — операций всего 2 $(\top, \bot)$
- 1 —

x	$\bot$	x	$\neg x$	$\top$
0	0	0	1	1
1	0	1	0	1

- 2 —

x	y	f_1	f_2	f_3	f_4
0	0	0	0	0	...
0	1	0	0	0	...
1	0	0	0	1	...
1	1	0	1	0	...

Утверждение 3.1. Штрих Шеффера, имеющий следующую таблицу истинности:

x	y	$x \uparrow y$
0	0	1
0	1	1
1	0	1
1	1	0

— полная операция, для системы $\{\uparrow\}$ верна теорема о функциональной полноте:

- $x \uparrow x = \neg x$
- $x \uparrow y = \neg(x \land y)$
- $\neg(x \uparrow y) = \neg\neg(x \land y) = x \land y$
- $x \lor y = \neg(\neg x \land \neg y)$

Утверждение 3.2. Стрелка Пирса, имеющая следующую таблицу истинности:

x	y	$x \downarrow y$
0	0	1
0	1	0
1	0	0
1	1	0

— также полная операция и для неё выполнена теорема о функциональной полноте.

Определение 3.2. G — множество булевых функций, тогда $[G]$ — *замыкание* множества G, т.е. все булевы функции, которые можно выразить формулами, использующими операции из G.

Эквивалентно, $[G]$ — минимальное множество булевых функций, которое удовлетворяет следующим свойствам:

1. $G \subset [G]$;
2. 1. $[G]$ замкнуто относительно композиции;
   2. $\forall f_1, \ldots, f_n \in [G] \land g(x_1, \ldots, x_n) \in G \hookrightarrow g(f_1(x_1, \ldots, x_{m_1}), \ldots, f_n(x_1, \ldots, x_{m_n})) \in [G]$
3. $[G]$ содержит все тождественные проекции, т.е. $\forall n \in \mathbb{N}, i < n\colon p_i^n(x_1, \ldots, x_n) \equiv x_i$

Определение 3.3. Множество (класс) функций G называется *замкнутым*, если $[G] = G$.

Определение 3.4. Класс функций G называется *полным*, если $[G] = F_n$, где F_n — множество всех булевых функций n переменных.

Определение 3.5. Класс G называется *максимальным*, если это замкнутый собственный ($\neq F_n$) класс, такой, что $\forall f \in F_m \setminus G \hookrightarrow G \cup \{ f \}$ — полный класс. Эквивалентно, $[G \cup \{ f \}] = F_n$.

Определение 3.6. Класс функций H *неполный*, если $\exists\, G$ — замкнутый, такой, что $G \neq F_n \land H \subset G$.

Лемма 3.1. *Свойства замыкания:*

1. $G \subset [G]$
2. $G \subset H \implies [G] \subset [H]$
3. $[G] = [[G]]$

Доказательство. 1. Очевидно

2. Пусть $f \in [G]$, тогда она получена по 1 и 2 свойствам замыкания из функций в G. Тогда очевидно, что $f \in [H]$.
3. $\subset$ — следует из первых двух пунктов
   $\supset$ — докажем по индукции. Пусть $f \in [[G]]$. Тогда пункты 1 и 3 из определения тривиальны. Проверим 2.
   Факт: проекции позволяют увеличивать число переменных некоторыми мнимыми. Например, $g(p_1^3(x_1, x_2, x_3), p_2^3(x_1, x_2, x_3))$.
   Пусть $f(x_1, \ldots, x_n) = g(f_1(x_1, \ldots, x_n), \ldots, f_m(x_1, \ldots, x_n))$. По предположению индукции $f_i \in [G]\ \forall i$. Таким образом, $f \in [G]$ как композиция.

$\square$

Лемма 3.2. *H не является полной $\iff$ $\exists\, G$ — максимальная и $H \subseteq G$.*

Доказательство. $\Longleftarrow$ — очевидно ©

$\implies$ если H — неполная, тогда $[H]$ — замкнута и неполна.

1. Случай 1: $[H]$ — максимальна, тогда всё хорошо.
2. Случай 2: $[H]$ — не максимальна $\implies$ $\exists f \in F_m \setminus [H]\colon [[H] \cup \{ f \}] \neq F_m$. Тогда пусть $H := [H] \cup \{ f \}$ и вернёмся в начало. Теоретически, этот процесс может не сойтись. Сходимость доказывается леммой Цорна и трансфинитной индукцией или из теоремы Поста.

$\square$

Теорема 3.1 (Поста)**.** $T_0 = \{ f \mid f(0, \ldots, 0) = 0 \}$

Лемма 3.3. *T_0 — максимальный замкнутый класс.*

Доказательство. • Замкнутость:

$$\underbrace{g}_{\in T_0}(\underbrace{f_1(\vec{0})}_{\in T_0}, \dots, \underbrace{f_n(\vec{0})}_{\in T_0}) = 0$$

- Максимальность: Пусть $h \notin T_0$, тогда $h(0, \dots, 0) = 1$. Получаем два случая:
  - $h(1, \dots, 1) = 1 \implies h(x, \dots, x) \equiv 1$
    Возьмём полную систему $\{\oplus, \wedge, 1\}$. 1 уже имеем, а для каждой из остальных функций множества принадлежность к классу T_0 очевидна.
  - $h(1, \dots, 1) = 0 \implies h(x, \dots, x) \equiv \neg x$
    Заметим, что также имеем в T_0 конъюнкцию (т.к. $0 \wedge 0 \equiv 0 \implies \wedge \in T_0$). Тогда с помощью неё и отрицания выразим все остальные операции.

□

Определение 3.7. $T_1 = \{ f \mid f(1, \dots, 1) = 1 \}$. Лемма и её доказательство аналогичны T_0, за исключением того, что если $h(x, \dots, x) = 0$, то берём полную систему $\{ \to, \bot \}$.

4 Лекция 4 (теорема Поста)

4.1 Продолжение про классы функций

Определение 4.1. M — класс монотонных функций, содержащий функции, неубывающие по каждому аргументу. Т.е., если для наборов аргументов

$$f(x_1, \ldots, x_n), f(y_1, \ldots, y_n)$$

верно

$$x_1 \leqslant y_1, \ldots, x_n \leqslant y_n,$$

то выполняется

$$f(\vec{x}) \leqslant f(\vec{y}).$$

Пример монотонной функции: $x_1 \land x_2$.

Пример немонотонной функции: $x_1 \to x_2$.

Лемма 4.1. *M является максимальным замкнутым классом.*

Доказательство. Докажем замкнутость. Возьмём набор функций

$$g(x_1, \ldots, x_n), f_1(y_1, \ldots, y_m), \ldots, f_n(y_1, \ldots, y_m) \in M.$$

Рассмотрим $g(f_1(\vec{y}), \ldots, f_n(\vec{y}))$, и возьмём $\vec{y'}$ такой, что $\forall i\colon y_i \leqslant y'_i$. Тогда $\forall i\colon f_i(\vec{y}) \leqslant f_i(\vec{y'})$, откуда получаем $g(f_1(\vec{y}), \ldots, f_n(\vec{y})) \leqslant g(f_1(\vec{y'}), \ldots, f_n(\vec{y'}))$.

Теперь докажем максимальность. Возьмём $h \notin M$. Заметим, что $0, 1 \in M$. Тогда $\exists x_1 \leqslant y_1, \ldots, x_m \leqslant y_m\colon h(\vec{x}) > h(\vec{y})$, т.е. $h(\vec{x}) = 1$ и $h(\vec{y}) = 0$. Пусть $\vec{x} \preccurlyeq \vec{y} \iff x_1 \leqslant y_1 \land \cdots \land x_n \leqslant y_n$.

Лемма 4.2 (Вспомогательная лемма)**.** *Пусть $\vec{x} \preccurlyeq \vec{y}$. Тогда $\exists \vec{x}^1, \ldots, \vec{x}^k\colon \vec{x}^1 = \vec{x} \land \vec{x}^k = \vec{y}$ и $\vec{x}^i$ отличается от $\vec{x}^{i+1}$ в одной координате и $\vec{x} = \vec{x}^1 \preccurlyeq \vec{x}^2 \preccurlyeq \cdots \preccurlyeq \vec{x}^k = \vec{y}$.*

Доказательство. Доказательства не было, интуитивно — путь в n-мерном булевом кубе от вершины $\vec{x}$ до вершины $\vec{y}$. □

Посмотрим значение функции h на точках $\vec{x}^i$. Тогда $h(\vec{x}^1) = 1$, $h(\vec{x}^k) = 0$. Понятно, что тогда $\exists i\colon h(\vec{x}^i) = 1 \land h(\vec{x}^{i+1}) = 0$. Пусть у $\vec{x}^i$ на j-ой позиции стоит 0, а у $\vec{x}^{i+1}$ — 1. Получаем

$$h(\ldots \underbrace{0}_{j} \ldots) = 1, h(\ldots \underbrace{1}_{j} \ldots) = 0 \implies h(\ldots \underbrace{p}_{j} \ldots) = \neg p$$

Таким образом получили отрицание. С другой стороны, конъюнкция также монотонна, а с помощью этих двух функций уже выразим все остальные. □

Определение 4.2. S — класс самодвойственных функций, т.е функций, удовлетворяющих условию

$$f(\overline{x_1}, \ldots, \overline{x_n}) = \overline{f}(x_1, \ldots, x_n)$$

Пример несамодвойственной функции: $x \land y$.

Пример самодвойственной функции: $\neg x$, $x \oplus y \oplus z$.

Лемма 4.3. *S является максимальным замкнутым классом.*

Доказательство. Докажем замкнутость. Пусть

$$f_1, \dots, f_n \colon \mathbb{B}^m \to \mathbb{B}; g \colon \mathbb{B}^n \to \mathbb{B} \in S$$

Рассмотрим $g(f_1(\overline{y_1}, \dots, \overline{y_m}), \dots, f_n(\overline{y_1}, \dots, \overline{y_m})) = g(\overline{f_1(\vec{y})}, \dots, \overline{f_n(\vec{y})}) = \overline{g(f_1(\vec{y}), \dots, f_n(\vec{y}))}$.

Докажем максимальность. Пусть $h \notin S$, тогда $\exists x_1, \dots, x_n \colon h(\overline{x_1}, \dots, \overline{x_n}) = h(x_1, \dots, x_n)$.

Обозначим $p^0 = \neg p$, $p^1 = p$. Тогда $h(p^{x_1}, \dots, p^{x_n}) = h(\overline{p^{x_1}}, \dots, \overline{p^{x_n}})$. Заметим, что

$$h(0^{x_1}, \dots, 0^{x_n}) = h(\overline{x_1}, \dots, \overline{x_n}),\ h(1^{x_1}, \dots, 1^{x_n}) = h(x_1, \dots, x_n)$$

Пусть $g(p) := h(p^{x_1}, \dots, p^{x_n})$, тогда возможно два случая:

1. $g(p) \equiv 1$, тогда получаем $\neg 1 = 0$
2. $g(p) \equiv 0$, тогда получаем $\neg 0 = 1$

То есть имеем константы 0 и 1.

Рассмотрим $V(x_1, x_2, x_3) = x_1 \wedge x_2 \oplus x_2 \wedge x_3 \oplus x_1 \wedge x_3$. Тогда в поле $\mathbb{F}_2$ получаем:

$$\begin{aligned}(x_1+1)(x_2+1) + (x_2+1)(x_3+1) + (x_1+1)(x_3+1) &= \dots = \\ &= x_1x_2 + x_2x_3 + x_1x_3 + 1 = \\ &= \overline{x_1x_2 + x_2x_3 + x_1x_3}\end{aligned}$$

Т.е. $V \in S$. Заметим, что $V(x_1, x_2, 0) = x_1 \wedge x_2$, а также, что $\neg \in S$. В итоге получаем полную систему $\{\neg, V, 0\}$. □

Определение 4.3. *Многочлен Жегалкина* — многочлен над полем $\mathbb{F}_2$. Эквивалентно можно считать, что это формула с операциями $\wedge, \oplus, 1$, представляющая из себя сумму $\oplus$ элементарных конъюнкций (*одночленов Жегалкина*) и, возможно, 1.

Лемма 4.4. *Все булевы функции однозначно (с точностью до перестановки слагаемых и сомножителей) представляются в виде многочлена Жегалкина.*

Доказательство. Всего одночленов Жегалкина от n переменных 2^n. Всего многочленов Жегалкина, соответственно, 2^{2^n}. Булевых функций $\mathbb{B}^n \to \mathbb{B}$ тоже 2^{2^n}. А т.к. каждая булева функция представима в виде многочлена Жегалкина (т.е. есть сюръекция) и их число одинаково, то имеем и биекцию между ними. □

Определение 4.4. *Степень* многочлена Жегалкина равна количеству переменных в нём. *Линейными* называются многочлены, в которых все одночлены степени не больше 1.

Определение 4.5. L — класс функций, эквивалентных некоторому линейному многочлену Жегалкина.

Лемма 4.5. *L является максимальным замкнутым классом.*

Доказательство. Пусть $g \notin L$; $0, 1 \in L$ и определим $g(x_1, \ldots, x_n) = x_1 x_2 \ldots x_m + \ldots$. Рассмотрим $g(x_1, x_2, 1, \ldots, 1)$:

$$g(x_1, x_2, 1, \ldots, 1) = \begin{cases} x_1 x_2 \\ x_1 x_2 + 1 \\ x_1 x_2 + x_1 \\ x_1 x_2 + x_2 \\ x_1 x_2 + x_1 + 1 \\ x_1 x_2 + x_2 + 1 \\ x_1 x_2 + x_1 + x_2 \\ x_1 x_2 + x_1 + x_2 + 1 \end{cases}$$

$x_1, x_2 \in L$, тогда в каждом случае можем добавить нужное число раз $x_1, x_2, 1$ к выражению, чтобы получить $x_1 x_2 \equiv x_1 \wedge x_2$. Получаем полную систему $\{\wedge, \neg\}$. □

Теорема 4.1 (Поста)**.** *Множество булевых функций H не является полным тогда и только тогда, когда оно содержится в одном из классов T_0, T_1, M, S, L.*

Доказательство. План доказательства:

- $\Longleftarrow$: Если H содержится в каком-то собственном замкнутом классе, то он не полон;
- $\Longrightarrow$: Покажем обратное. Пусть H не лежит целиком ни в одном из перечисленных классов:
  - Возьмём функцию $f_0 \in H$: $f_0 \notin T_0$. Тогда $f_0(x, \ldots, x)$ либо равна 1, либо $\neg x$.
  - Возьмём функцию $f_1 \in H$: $f_1 \notin T_1$. Тогда $f_1(x, \ldots, x)$ либо равна 0, либо $\neg x$.
  - Если есть $\neg x$: используем несамодвойственную функцию f_S и получим одну из констант.
  - Если есть 0 и 1, тогда используем немонотонную функцию f_M и получим отрицание $\neg x$.
  - У нас есть 0, 1 и $\neg$. Используя нелинейную функцию f_L можем получить $\wedge$

□

4.2 Замены

Определение 4.6. Замену переменной p на формулу ψ в формуле φ обозначается $\varphi[p/\psi]$.

Теорема 4.2. *Пусть формулы ψ_1 и ψ_2 имеют одинаковые таблицы истинности ($\psi_1 \equiv \psi_2$), тогда для любой формулы φ*

$$\varphi[p/\psi_1] \equiv \varphi[p/\psi_2]$$

Доказательство. По индукции:

База: для $\varphi = \perp / \top$ очевидно, как и для $\varphi = q \neq p$. Для $\varphi = p$ получаем $\varphi[p/\psi_1] = \psi_1$ и $\varphi[p/\psi_2] = \psi_2$, а они равны.

Шаг: $\varphi = \varphi_1 \wedge \varphi_2$

$\varphi[p/\psi_1] = \varphi_1[p/\psi_1] \wedge \varphi_2[p/\psi_1]$, аналогично для ψ_2. Тогда, по предположению индукции, $\varphi_1[p/\psi_1] \equiv \varphi_1[p/\psi_2]$ и $\varphi_2[p/\psi_1] \equiv \varphi_2[p/\psi_2]$, а объединение этих формул не влияет на эквивалентность. □

5 Лекция 5 (выводы)

5.1 Правила вывода

Определение 5.1. *Правилом вывода* будем называть пару, состоящую из множества формул Γ и одной формулы φ. При этом Γ может быть пустым. Γ будем называть множеством *посылок*, а формулу φ *заключением*. Правила вывода обычно записывают так:

$$\frac{\Gamma}{\varphi} \text{ или } \frac{\psi_1, \ldots, \psi_n}{\varphi}$$

Теоретически можно рассматривать правила, в которых Γ бесконечно, такие правила называются *инфинитарными*, но мы так делать не будем, у нас всё конечно.

Пусть Γ — множество формул (необязательно конечное), и φ — формула. Будем говорить, что из Γ *логически следует* φ, если в любой модели M, в которой истинны все формулы из Γ истинна и формула φ (обозначение: $\Gamma \models \varphi$). Правило $\frac{\Gamma}{\varphi}$ называется *корректным*, если $\Gamma \models \varphi$.

Пример корректных правил: $\dfrac{p}{p}$, $\dfrac{p \to q, q \to r}{p \to r}$ (силлогизм); пример некорректных правил: $\dfrac{-}{p}$, $\dfrac{p}{p \wedge q}$.

Определение 5.2. Правило вывода $\dfrac{\Delta}{\psi}$ является частным случаем правила $\dfrac{\Gamma}{\phi}$, если существуют формулы $\theta_1, \ldots, \theta_n$ и переменные $p_1, \ldots, p_n$, такие что первое правило получается из второго путём одновременной подстановки формул θ_i вместо каждого вхождения переменной p_i во всех посылках правила ψ (с сохранением их порядка), а также в его заключении.

Например, $\dfrac{(x \to x) \wedge (\neg y)}{x \to x}$ — частный случай правила $\dfrac{p \wedge q}{p}$.

Мы будем рассматривать наши правила выводов как схемы, т.е. одно правило — по сути бесконечно много правил, включающее все частные случаи данного правила.

Определение 5.3. Пусть у нас есть множество правил вывода $\mathcal{R}$, *выводом* в $\mathcal{R}$ из множества *гипотез* Γ будем называть последовательность формул, каждая из которых либо принадлежит Γ, либо получена с помощью частного сдучая некоторого правила из $\mathcal{R}$, при этом множество посылок должно состоять только из формул, которые появлялись в выводе раньше.

Формула φ *выводится* из Γ в $\mathcal{R}$ ($\Gamma \vdash_{\mathcal{R}} \varphi$), если существует вывод из Γ в $\mathcal{R}$, заканчивающийся формулой φ.

Если формула φ выводится из пустого множества гипотез в $\mathcal{R}$, то мы говорим, что φ выводима в $\mathcal{R}$ и записывается как $\vdash_{\mathcal{R}} \varphi$.

Пример:

$$\mathcal{R} = \left\{ \frac{p \to q, q \to r}{p \to r}, \frac{p}{\neg\neg p} \right\}, \ \Gamma = \{ p \to \neg p \}$$

Тогда примером вывода будет:

$$p \to \neg p$$
$$\neg\neg(p \to \neg p)$$

Первое правило из $\mathcal{R}$ мы использовать для вывода не можем. Добавим в Γ гипотезу $\neg p \to q$. Тогда, можем дополнить вывод до

$$\neg p \to q$$
$$p \to q.$$

Таким образом, $\Gamma \vdash_{\mathcal{R}} p \to q$

Теорема 5.1 (Теорема о корректности)**.** *Если все правила в $\mathcal{R}$ корректны и $\Gamma \vdash_{\mathcal{R}} \varphi$, то $\Gamma \models \varphi$.*

Доказательство. По индукции. Знаем, что для $\varphi_1, \ldots, \varphi_n \colon \forall i \colon \Gamma \models \varphi_i$.

База: $i = 1 \implies$

1. $\varphi_1 \in \Gamma \implies \varphi_1$ истинная в модели;
2. $\dfrac{}{\varphi_1}$ — частный случай правила из $\mathcal{R}$. Отсюда φ_1 — тавтология $\implies \mathcal{M} \models \varphi_1$.

Шаг: пусть $\forall j < i \colon \Gamma \models \varphi_j$. Докажем для φ_i.

1. $\varphi_i \in \Gamma \implies \mathcal{M} \models \varphi_i$
2. $\exists j_1, \ldots, j_k < i \colon \dfrac{\varphi_{j_1}, \ldots, \varphi_{j_k}}{\varphi_i}$ — частный случай правила из $\mathcal{R}$. Тогда по предположению индукции $\varphi_{j_1}, \ldots, \varphi_{j_k}$ истинны в $\mathcal{M}$.

   Лемма 5.1. *Если $\dfrac{\varphi_1, \ldots, \varphi_n}{\varphi}$ корректно и $\dfrac{\eta_1, \ldots, \eta_n}{\eta}$ — частный случай (P), то оно тоже корректно.*

   Доказательство. Имеем $\eta_1 = \varphi_1[p_1/\theta_1, p_2/\theta_2, \ldots, p_n/\theta_n], \ldots, \eta = \varphi[p_1/\theta_1, p_2/\theta_2, \ldots, p_n/\theta_n]$
   P — корректна $\implies \forall M \colon \varphi_1, \ldots, \varphi_n$ истинны $\implies \varphi$ — истинна.
   Пусть $\eta_1, \ldots, \eta_n$ истинны в модели M. Возьмём M' такую, что $\forall i \colon M' \models p_i \iff \mathcal{M} \models \theta_i$.
   Утверждение: $\forall \varphi \colon \mathcal{M} \models \varphi \iff \mathcal{M} \models \varphi[p/\theta_1]$. Доказывается индукцией по длине φ. □

   Тогда по лемме φ_i истинна в $\mathcal{M}$.

□

5.2 Конкретные правила

Определение 5.4. *Modus Ponens*:

$$\frac{p, p \to q}{q}$$

Определение 5.5. *Аксиомы Гильберта*:

1. $(I1)$:
$$q \to (p \to q)$$
2. (D):
$$(p \to (q \to r)) \to ((p \to q) \to (p \to r))$$
3. (N):
$$(\neg q \to \neg p) \to (p \to q)$$

6 Лекция 6 (продолжение про выводы)

Определение 6.1. Правило $\frac{\Gamma}{\varphi}$ называется *допустимым* в множестве правил вывода $\mathcal{R}$, если

$$\Gamma \vdash_{\mathcal{R}} \varphi$$

Лемма 6.1. *Если $\frac{\Gamma}{\varphi}$ — допустимое в $\mathcal{R}$ правило, а $\frac{\Delta}{\psi}$ — частный случай правила $\frac{\Gamma}{\varphi}$, то*

$$\Delta \vdash_{\mathcal{R}} \psi$$

Доказательство. Пусть есть вывод $\Gamma \vdash_{\mathcal{R}} \varphi$:

1. ξ_1
2. $\dots$
3. $\xi_n = \varphi$

Существует подстановка, переводящая Γ в Δ и φ в ψ. Сделаем такую подстановку во все формулы вывода. □

Теорема 6.1 (The Lemma Theorem)**.** *Если правило ρ допустимо (доказуемо) в множестве правил вывода $\mathcal{R} \cup \lambda$ и при этом λ допустимо в $\mathcal{R}$, то и ρ допустимо в $\mathcal{R}$.*

Доказательство. Пусть $\lambda = \dfrac{\Delta}{\psi}$, $\rho = \dfrac{\Gamma}{\varphi}$, а также два вывода:

- $\Gamma \vdash_{\mathcal{R} \cup \{\lambda\}} \varphi$:
  1. ξ_1
  2. $\dots$
  3. $\xi_n = \varphi$
- $\Delta \vdash_{\mathcal{R}} \psi$:
  1. η_1
  2. $\dots$
  3. $\eta_m = \psi$

Если в выводе ξ_i получено по правилу из $\mathcal{R}$, то всё хорошо. Если же ξ_i получено с помощью λ, то имеем правило вывода $\dfrac{\xi_{j_1}, \dots, \xi_{j_l}}{\xi_i}$ для $\xi_{j_1}, \dots, \xi_{j_l} \in \{\xi_1, \dots, \xi_{i-1}\}$, частный случай λ. Тогда по предыдущей лемме можем этот вывод заменить на вывод $\xi_{j_1}, \dots, \xi_{j_l} \vdash_{\mathcal{R}} \xi_i$:

1. η'_1
2. $\dots$
3. $\eta'_k = \xi_i$

и вставить его в доказательство вместо ξ_i. Делаем такую подстановку во все такие строки вывода и получаем новый вывод $\Gamma \vdash_{\mathcal{R}} \varphi$. □

6.1 Примеры допустимых правил

Пусть $\mathcal{R} = \{I1, D, N, MP\}$, тогда в $\mathcal{R}$ допустимы правила

$$(I0)\frac{}{p \to p},\ \frac{p \to q, q \to r}{p \to r},\ \frac{p \to q, p \to \neg q}{\neg p}$$

Теорема 6.2 (Теорема о дедукции)**.** *Если $\mathcal{R}$ — множество правил вывода, содержащее MP, $I1$ и D, и все остальные правила являются аксиомами (пустое множество посылок), то для любых формул φ, ψ и множества формул Γ верно*

$$\Gamma \cup \{\varphi\} \vdash_{\mathcal{R}} \psi \iff \Gamma \vdash_{\mathcal{R}} (\varphi \to \psi)$$

Доказательство. В одну сторону можно усилить утверждение

Лемма 6.2. *Если $\mathcal{R}$ — множество правил вывода, содержащее MP, то для любых формул φ, ψ и множества формул Γ верно*

$$\Gamma \vdash_{\mathcal{R}} (\varphi \to \psi) \implies \Gamma \cup \{\varphi\} \vdash_{\mathcal{R}} \psi$$

Доказательство. Имеем изначальный вывод $\Gamma \vdash_{\mathcal{R}} (\varphi \to \psi)$

1. ...
2. $\varphi \to \psi$

Тогда получаем следующий вывод $\Gamma \cup \{\varphi\} \vdash_{\mathcal{R}} \psi$:

1. ...
2. $\varphi \to \psi$
3. ψ (MP)

□

Осталось доказать, что $\Gamma \cup \{\varphi\} \vdash_{\mathcal{R}} \psi \implies \Gamma \vdash_{\mathcal{R}} (\varphi \to \psi)$.

Будем доказывать индукцией по длине вывода. Пусть имеем вывод $\Gamma \cup \{\varphi\} \vdash_{\mathcal{R}} \psi$:

1. ξ_1
2. ...
3. $\xi_n = \psi$

Будем доказывать, что для любого $i \leqslant n$ верно

$$\Gamma \vdash_{\mathcal{R}} (\varphi \to \xi_i)$$

Разберём случаи:

- Возьмём $\xi_i = \varphi$. Докажем, что $\Gamma \vdash_{\mathcal{R}} (\varphi \to \varphi)$. Но уже доказывали (в ДЗ), что из пустого множества посылок доказуемо выражение $p \to p$, а $\varphi \to \varphi$ — его частный случай.
- Пусть теперь $\xi_i \in \Gamma$. Тогда нужно построить вывод $\Gamma \vdash_{\mathcal{R}} (\varphi \to \xi_i)$. Тогда
  1. ξ_i
  2. $\xi_i \to (\varphi \to \xi_i)$ (I1)
  3. $\varphi \to \xi_i$ (MP)
- ξ_i получена по правилу I1 или D (с пустым множеством посылок). Вывод будет тот же самый, но первой строкой вывода ξ_i записан не потому что $\xi_i \in \Gamma$, а потому что ξ_i выводится из аксиом I1 и D.
- ξ_i получена по правилу MP из ξ_j и ξ_k. Тогда ξ_k имеет вид $\xi_j \to \xi_i$. По предположению индукции $\Gamma \vdash_{\mathcal{R}} (\varphi \to \xi_j)$ и $\Gamma \vdash_{\mathcal{R}} \underbrace{(\varphi \to (\xi_j \to \xi_i))}_{\xi_k}$. Тогда получаем следующий вывод:

1. ...
2. $\varphi \to \xi_j$
3. ...
4. $\varphi \to (\xi_j \to \xi_i)$
5. $(\varphi \to (\xi_j \to \xi_i)) \to ((\varphi \to \xi_j) \to (\varphi \to \xi_i))$ (D)
6. $((\varphi \to \xi_j) \to (\varphi \to \xi_i))$ (MP)
7. $(\varphi \to \xi_i)$ (MP)

□

6.2 Противоречивость и непротиворечивость

Рассмотрим аксиому

$$(I2)\ (\neg p \to (p \to q))$$

Пусть $\mathcal{R}$ — множество правил вывода, которое включает MP, I0 и I2, а также может дополнительно включать только правила вывода без посылок. Множество формул Γ называется (синтаксически) *противоречивым* (*inconsistent*) (относительно $\mathcal{R}$), если выполняется одно из следующих пяти эквивалентных условий:

- Формула $\neg(p \to p)$ выводится из Γ в $\mathcal{R}$ ($\Gamma \vdash_{\mathcal{R}} \neg(p \to p)$)
- Отрицание некоторой аксиомы выводимо из Γ
- $\Gamma \vdash_{\mathcal{R}} \varphi$ и $\Gamma \vdash_{\mathcal{R}} \neg\varphi$ для некоторой формулы φ
- Из Γ можно вывести в $\mathcal{R}$ любую формулу (вообще любую)
- Отрицание всех аксиом доказуемы в $\mathcal{R}$ из Γ

Множество формул, которое не является противоречивым, называется *непротиворечивым* (*consistent*).

Доказательство. $1 \implies 2$: $\neg(p \to p)$ само по себе есть отрицание аксиомы I0.

$2 \implies 3$: Пусть есть α — аксиомы из $\mathcal{R}$ и $\varphi = \alpha$, тогда $\Gamma \vdash_{\mathcal{R}} \alpha$. С другой стороны, $\Gamma \vdash_{\mathcal{R}} \neg\alpha$ из предположения.

$3 \implies 4$: Имеем вывод $\Gamma \vdash_{\mathcal{R}} \varphi$ и $\Gamma \vdash_{\mathcal{R}} \neg\varphi$. Объединим их в один вывод:

1. ...
2. φ
3. ...
4. $\neg\varphi$

Тогда дополним его:

5. $\neg\varphi \to (\varphi \to \psi)$ (I2)
6. $\varphi \to \psi$ (MP)
7. ψ (MP)

$4 \implies 5$: можно вывести любую формулу, значит можно вывести и отрицания аксиом.

$5 \implies 1$: отрицания всех аксиом доказуемы, значит доказуемо и отрицание I0. □

Теорема 6.3. *Пусть* $\{ MP, I1, D, N \} \subseteq \mathcal{R}$ *и, кроме MP, все правила в* $\mathcal{R}$ *без посылок. Для любого* *множества формул* Γ *и формулы* φ *верно, что* $\Gamma \cup \{ \neg\varphi \}$ *противоречиво в* $\mathcal{R}$*, тогда* $\Gamma \vdash_{\mathcal{R}} \varphi$*. Т.е.,*

$$\Gamma \cup \{ \neg\varphi \} \vdash_{\mathcal{R}} \neg(p \to p) \implies \Gamma \vdash_{\mathcal{R}} \varphi$$

Доказательство. По теореме о дедукции, левая часть последнего утверждения равносильна $\Gamma \vdash_{\mathcal{R}} (\neg\varphi \to \neg(p \to p))$.

Тогда имеем вывод

1. $\ldots$
2. $\neg\varphi \to \neg(p \to p)$
3. $(\neg\varphi \to \neg(p \to p)) \to ((p \to p) \to \varphi)$ (N)
4. $(p \to p) \to \varphi$ (MP)
5. $\ldots$ (вывод I0 с помощью $\{ \mathrm{MP}, \mathrm{I1}, \mathrm{D}, \mathrm{N} \}$)
6. $p \to p$ (I0)
7. φ

$\square$

Лемма 6.3. *Пусть* $\mathcal{R} = \{ MP, I1, D, N \}$*, тогда правило I2 допустимо в* $\mathcal{R}$*, т.е.*

$$\vdash_{\mathcal{R}} (\neg p \to (p \to q))$$

Доказательство. По теореме о дедукции вместо изначального утверждения можем доказать $\neg p \vdash_{\mathcal{R}} (p \to q)$. Построим вывод. Гипотеза — $\neg p$, тогда

1. $\neg p$
2. $\neg p \to (\neg q \to \neg p)$ (I1)
3. $\neg q \to \neg p$ (MP)
4. $(\neg q \to \neg p) \to (p \to q)$ (N)
5. $p \to q$ (MP)

$\square$

7 Лекция 7

7.1 Основное множество правил

$$
\begin{aligned}
(MP)\ & \frac{p, p \to q}{q} \\
(I0)\ & (p \to p) \\
(I1)\ & (q \to (p \to q)) \\
(D)\ & ((p \to (q \to r)) \to ((p \to q) \to (p \to r))) \\
(I2)\ & (\neg p \to (p \to q)) \\
(N)\ & ((\neg q \to \neg p) \to (p \to q)) \\
(NI)\ & (p \to (\neg q \to \neg(p \to q))) \\
(NN)\ & (p \to \neg\neg p) \\
(R)\ & ((q \to p) \to ((\neg q \to p) \to p))
\end{aligned}
$$

Будем писать $\vdash$ (без индекса) для выводимости в этом множестве правил.

На самом деле, обязательными являются лишь правила I1, D, N.

Обозначим систему аксиом Гильберта как $\mathcal{H}$.

Определение 7.1. Пусть φ — формула, и $b \in \{\,\mathrm{True}, \mathrm{False}\,\}$, тогда

$$
\varphi^b = \begin{cases} \varphi, & b = \mathrm{True} \\ \neg\varphi, & b = \mathrm{False} \end{cases}
$$

Определение 7.2. Пусть M — некоторая конечная модель , т.е. отображение из конечного множества переменных в множество $\{\,\mathrm{True}, \mathrm{False}\,\}$.

Определим множество формул

$$
\Gamma_M = \bigcup_{M[p]=b} \{\, p^b \,\}
$$

Например, если $M = \{\, p\colon \mathrm{True}, q\colon \mathrm{False}, x\colon \mathrm{False} \,\}$, то $\Gamma_M = \{\, p, \neg q, \neg x \,\}$.

Лемма 7.1. *Пусть φ — формула, и M оценивает все формулы из φ и $M[\varphi]$ — истинностное значение формулы φ при оценке M, тогда*

$$
\Gamma_M \vdash \varphi^{M[\varphi]}
$$

Доказательство. Доказательство индукцией по длине формулы:

База: $\varphi = p$. Утверждение следует из того, что $p \vdash p$ и $\neg p \vdash \neg p$.

Шаг:

- $\varphi = \neg\psi$
  Если $M[\psi] = \text{True}$, то $M[\varphi]$ – False. Тогда по предположению индукции $\Gamma_M \vdash \psi^{\text{True}} = \psi$. Надо доказать, что $\Gamma_M \vdash \varphi^{\text{False}} = \neg\neg\psi$. Достаточно доказать, что $\vdash (\psi \to \neg\neg\psi)$ (правило NN). Вывод для $\neg\neg\psi$ выглядит так:
  1. ...
  2. ψ
  3. $\psi \to \neg\neg\psi$ (NN)
  4. $\neg\neg\psi$

  Если $M[\psi] = \text{False}$, то $M[\varphi] = \text{True}$. По ПИ имеем $\Gamma_M \vdash \neg\psi$, нужно доказать $\Gamma_M \vdash \varphi = \neg\psi$. Вывод будет тривиальным;
  1. $\neg\psi$
  2. φ
- $\varphi = (\psi_1 \to \psi_2)$. По предположению индукции $\Gamma_M \vdash \psi_1^{M[\psi_1]}$ и $\Gamma_M \vdash \psi_2^{M[\psi_2]}$. Надо разобрать 4 случая:
  1. $M[\psi_1] = \text{False}, M[\psi_2] = \text{False}$. Докажем $\neg\psi_1, \neg\psi_2 \vdash (\psi_1 \to \psi_2)$ с помощью I2 $(\neg p \to (p \to q))$. Имеем вывод
     1. ...
     2. $\neg\psi_1$
     3. $\neg\psi_1 \to (\psi_1 \to \psi_2)$ (I2)
     4. $\psi_1 \to \psi_2$ (MP)
  2. False, True. Докажем $\neg\psi_1, \psi_2 \vdash (\psi_1 \to \psi_2)$ (I2) или (I1). То же самое, т.к. ψ_2 в прошлом выводе не участвовал.
  3. True, False. Докажем $\psi_1, \neg\psi_2 \vdash \neg(\psi_1 \to \psi_2)$ (NI). Получим вывод
     1. ...
     2. ψ_1
     3. ...
     4. $\neg\psi_2$
     5. $\psi_1 \to (\neg\psi_2 \to \neg(\psi_1 \to \psi_2))$ (NI)
     6. $\neg\psi_2 \to \neg(\psi_1 \to \psi_2)$ (MP)
     7. $\neg(\psi_1 \to \psi_2)$ (MP)
  4. True, True. Докажем $\psi_1, \psi_2 \vdash (\psi_1 \to \psi_2)$. Соответствующий вывод:
     1. ...
     2. ψ_2
     3. $\psi_2 \to (\psi_1 \to \psi_2)$ (I1)
     4. $\psi_1 \to \psi_2$ (MP)

$\square$

Лемма 7.2. *Если* $\Gamma \cup \{ p \} \vdash \varphi$ *и* $\Gamma \cup \{ \neg p \} \vdash \varphi$*, то* $\Gamma \vdash \varphi$*.*

Доказательство. Следует из аксиомы (R).

По теореме о дедукции из первого утверждения $\Gamma \vdash p \to \varphi$, а из второго $\Gamma \vdash \neg p \to \varphi$. Получим вывод:

1. ...
2. $p \to \varphi$
3. ...

4. $\neg p \to \varphi$
5. $(p \to \varphi) \to ((\neg p \to \varphi) \to \varphi)$ (R)
6. $(\neg p \to \varphi) \to \varphi$ (MP)
7. φ

$\square$

Теорема 7.1 (О полноте в слабой форме)**.** *Если φ — тавтология, то $\vdash \varphi$, а значит и $\vdash_{\mathcal{H}} \varphi$.*

Доказательство. $\forall$ модели M, содержащей все переменные из φ имеем $M[\varphi] = \text{True}$, Тогда по лемме

$$\Gamma_M \vdash \varphi \text{ для любой модели } M.$$

Пусть p — некоторая переменная из φ, тогда все модели разобьются на пары, т.что в паре оценка отличается только в переменной p. Пусть M_1 и M_2 — две такие модели. Пусть

$$\Gamma_{M_1} = \Gamma' \cup \{ p \} \text{ и } \Gamma_{M_2} = \Gamma' \cup \{ \neg p \}$$

По предыдущей лемме получим $\Gamma' \vdash \varphi$. Проделав так с каждой парой моделей мы уменьшим на 1 количество посылок. Действуя так мы сможем избавиться от всех посылок. $\square$

Теорема 7.2 (О полноте в сильной форме)**.** *Пусть Γ — конечное множество формул и φ — формула, тогда*

$$\Gamma \models \varphi \iff \Gamma \vdash \varphi$$

Доказательство. $\Longleftarrow$ было в теореме о корректности.

$\Longrightarrow$ Пусть $\Gamma = \{ \psi_1, \dots, \psi_n \}$. По теореме о дедукции (применив n раз)

$$\Gamma \vdash \varphi \iff \vdash (\psi_1 \to (\dots(\psi_n \to \varphi)\dots))$$

Осталось показать, что

$$\Gamma \models \varphi \iff (\psi_1 \to (\dots(\psi_n \to \varphi)\dots)) \text{ — тавтология}$$

В правую сторону импликация известна, осталось доказать в левую. Пусть это не тавтология, тогда $\exists$ модель, её опровергащая. Тогда надо чтобы ψ_i были истинными, а φ — ложной. Но тогда $\Gamma \not\models \varphi$. $\square$

Переформулируем это утверждение в симметричной форме.

$\Gamma \models \varphi$ *эквивалентно тому, что* $\Gamma \cup \{ \neg\varphi \}$ *не имеет модели.*

$\Gamma \vdash \varphi$ *эквивалентно тому, что* $\Gamma \cup \{ \neg\varphi \}$ *противоречиво:*

$$\Gamma \cup \{ \neg\varphi \} \vdash \neg\varphi, \Gamma \cup \{ \neg\varphi \} \vdash \varphi \implies \Gamma \cup \{ \neg\varphi \} \text{ — \textit{противоречиво}}$$

В другую сторону знаем, что $\Gamma \cup \{ \neg\varphi \} \vdash \neg(p \to p)$*. Тогда:*

1. $\Gamma \vdash \neg\varphi \to \neg(p \to p)$
2. $(\neg\varphi \to \neg(p \to p)) \to ((p \to p) \to \varphi)$ *(N)*
3. $(p \to p) \to \varphi$

4. $p \to p$ *(I0)*
5. φ

Тогда изначальное утверждение эквивалентно следующему:

$$\Gamma \text{ не имеет модели} \iff \Gamma \text{ противоречиво}$$

или

$$\Gamma \text{ выполнимо} \iff \Gamma \text{ непротиворечиво}$$

Теорема 7.3 (О компактности (синтаксическая))**.** *Бесконечное множество формул непротиворечиво тогда и только тогда, когда любое его конечное подмножество непротиворечиво.*

Доказательство. Пусть Γ противоречиво, тогда можно вывести $\Gamma \vdash \neg(p \to p)$, т.е. имеем вывод

1. ...
2. $\neg(p \to p)$,

он использует конечное число формул из Γ. Пусть Γ_0 — все формулы, используемые в доказательстве. Тогда $\Gamma_0 \vdash \neg(p \to p)$.

В другую сторону, если существует $|\Gamma_0| < \infty, \Gamma_0 \subseteq \Gamma$ и Γ_0 противоречива, то Γ также противоречива. □

Теорема 7.4 (О компактности (семантическая))**.** *Бесконечное подмножество формул* Γ *выполнимо (имеет модель) тогда и только тогда, когда любое его конечное подмножество выполнимо.*

8 Лекция 8

Теорема 8.1 (О полноте в сильной форме)**.** *Произвольное множество формул* Γ *выполнимо тогда и только тогда, когда* Γ *непротиворечиво.*

Доказательство.

Определение 8.1. Множество формул Γ называется *полным*, если оно непротиворечиво и «максимально», т.е. для любой формулы $\varphi \notin \Gamma$ верно, что $\Gamma \cup \{\, \varphi \,\}$ — противоречиво.

Лемма 8.1 (Линденбаум)**.** *Любое непротиворечивое множество можно дополнить до полного.*

Доказательство. Перечислим все формулы $\varphi_0, \varphi_1, \ldots$

Будем строить Γ_n по индукции. $\Gamma_0 = \Gamma$,

$$\Gamma_{n+1} = \begin{cases} \Gamma_n \cup \{\, \varphi_n \,\}, & \text{если } \Gamma_n \cup \{\, \varphi_n \,\} \text{ — непротиворечиво} \\ \Gamma_n, & \text{иначе} \end{cases}$$

$$\Delta = \bigcup_{n \in \mathbb{N}} \Gamma_n$$

Проверим, что Δ непротиворечиво и максимально.

- Непротиворечивость
  Если Δ противоречиво, то $\Delta \vdash \neg(p \to p)$. Такой вывод использует конечное число формул, а значит $\exists n\colon \Gamma_n \vdash \neg(p \to p) \implies \Gamma_n$ — противоречиво, что противоречит построению Γ_n
- Максимальность
  Пусть оно не максимально, т.е. $\exists \varphi \notin \Delta\colon \Delta \cup \{\, \varphi \,\}$ — непротиворечиво. Тогда $\exists n\colon \varphi = \varphi_n$, но тогда $\Gamma_{n+1} = \Gamma_n \cup \{\, \varphi_n \,\}$
  1. $\Gamma_n \cup \{\, \varphi_n \,\}$ — противоречиво, тогда $\Gamma_n \cup \{\, \varphi_n \,\} \vdash \neg(p \to p)$, откуда следует $\Delta \vdash \neg(p \to p)$, а значит Δ противоречива, противоречие
  2. $\Gamma_n \cup \{\, \varphi_n \,\}$ — непротиворечиво, тогда $\varphi_n = \varphi \in \Delta$, противоречие

□

Лемма 8.2 (Свойства полных множеств)**.** *Пусть* Δ *— полное множество формул, тогда:*

- $\neg\psi \in \Delta \iff \psi \notin \Delta$
- $(\psi_1 \to \psi_2) \in \Delta \iff (\psi_1 \notin \Delta \vee \psi_2 \in \Delta)$

Доказательство.
- Пусть оба $\in \Delta$, тогда получаем $\Delta \vdash \psi$ и $\Delta \vdash \neg\psi$ и Δ противоречиво
  Пусть оба $\notin \Delta$. Тогда по максимальности добавление ψ и $\neg\psi$ приводит к противоречивости:

$$\begin{cases} \Delta \cup \{\, \psi \,\} \text{ — противоречиво} \implies \Delta \vdash \neg\psi \\ \Delta \cup \{\, \neg\psi \,\} \text{ — противоречиво} \implies \Delta \vdash \neg\neg\psi \end{cases}$$

- Имея первый пункт, достаточно исключить следующие 3 случая:
  - $(\psi_1 \to \psi_2) \in \Delta$ и $\psi_1 \in \Delta$ и $\neg\psi_2 \in \Delta$, тогда $\Delta \vdash (\psi_1 \to \psi_2)$ и $\Delta \vdash \psi_1$. По MP получаем $\Delta \vdash \psi_2$, но $\Delta \vdash \neg\psi_2$, откуда Δ противоречиво.

- $\neg(\psi_1 \to \psi_2) \in \Delta$ и $\neg\psi_1 \in \Delta$ (равносильно $\psi_1 \notin \Delta$ по первому пункту). Имеем $\neg\psi_1 \to (\psi_1 \to \psi_2)$ по I2; по MP получим $\Delta \vdash \psi_1 \to \psi_2$, и имея $\Delta \vdash \neg(\psi_1 \to \psi_2)$ получаем противоречие.
- $\neg(\psi_1 \to \psi_2) \in \Delta$ и $\psi_2 \in \Delta$. Вывод аналогичен предыдущему пункту:
  1. $\psi_2 \to (\psi_1 \to \psi_2)$ (I1)
  2. $\psi_1 \to \psi_2$ (MP)
  3. $\neg(\psi_1 \to \psi_2)$ по условию, противоречие.

$\square$

Определение 8.2. Пусть Δ — полное множество формул. Определим модель M_Δ следующим образом:

$$M_\Delta[p] = \begin{cases} \text{True}, & p \in \Delta \\ \text{False}, & p \notin \Delta \end{cases}$$

Лемма 8.3. *Для произвольной формулы φ верно, что*

$$M_\Delta[\varphi] = \text{True} \iff \varphi \in \Delta$$

Доказательство. Докажем индукцией по φ.

База: верна по определению $M_\Delta[\varphi]$

Шаг:

- $\varphi = \neg\psi$
  $$M_\Delta[\varphi] = \begin{cases} \text{True}, & M_\Delta[\psi] = \text{False} \iff \psi \notin \Delta \iff \varphi = \neg\psi \in \Delta \\ \text{False}, & M_\Delta[\psi] = \text{True} \iff \psi \in \Delta \iff \varphi = \neg\psi \notin \Delta \end{cases} \quad \text{из предыдущей леммы.}$$
- $\varphi = (\psi_1 \to \psi_2)$.
  $(\psi_1 \to \psi_2) \in \Delta \iff (\psi_1 \notin \Delta \vee \psi_2 \in \Delta) \iff M_\Delta[\psi_1] = \text{False} \vee M_\Delta[\psi_2] = \text{True} \iff M_\Delta[\psi_1 \to \psi_2] = \text{True}$

$\square$

Докажем наконец изначальную теорему (да, это было доказательство теоремы на полторы страницы):

$\Longrightarrow$ Если Γ выполнимо, то $\exists M$, оценивающая все переменные, в которой все формулы из Γ истинны.

Пусть Γ противоречиво, тогда $\Gamma \vdash \neg(p \to p)$, но в силу того, что все правила корректны, т.е. сохраняют истинность, то в модели M должна быть истинная формула $\neg(p \to p)$, что невозможно.

$\Longleftarrow$ Теперь, пусть Γ непротиворечиво, тогда его можно расширить по лемме Линденбаума до полного множества Δ. Тогда в модели M_Δ будут истинны все формулы из Γ благодаря предыдущей лемме. $\square$

8.1 Доказательства аксиом

Напоминание про силлогизм:

$$\frac{p \to q, q \to r}{p \to r}$$

- (I0):
$$p \to p$$

Доказательство. 1. $p \to ((p \to p) \to p)$ (I1)
2. $(p \to ((p \to p) \to p)) \to ((p \to (p \to p)) \to (p \to p))$ (D)
3. $(p \to (p \to p)) \to (p \to p)$ (MP)
4. $p \to (p \to p)$ (I1)
5. $p \to p$ (MP)

□

- (I2):
$$\neg p \to (p \to q)$$

Доказательство. 1. $\neg p \to (\neg q \to \neg p)$ (I1)
2. $(\neg q \to \neg p) \to (p \to q)$ (N)
3. $\neg p \to (p \to q)$ (силлогизм)

□

- Вспомогательная аксиома
$$\vdash \neg\neg p \to p$$

Доказательство. По лемме о дедукции доказательство аксиомы эквивалентно доказательству $\neg\neg p \vdash p$. Хотим вывести $\vdash \neg\neg p \to (\neg\neg p \to p)$
1. $\neg\neg p \to (\neg\neg\neg\neg p \to \neg\neg p)$ (I1)
2. $\neg\neg p \vdash \neg\neg\neg\neg p \to \neg\neg p$
3. $(\neg\neg\neg\neg p \to \neg\neg p) \to (\neg p \to \neg\neg\neg p)$ (N)
4. $\neg\neg p \vdash \neg p \to \neg\neg\neg p$ (т.к. умеем выводить $\neg\neg\neg\neg p \to \neg\neg p$ из $\neg\neg p$)
5. $(\neg p \to \neg\neg\neg p) \to (\neg\neg p \to p)$ (N)
6. $\neg\neg p \vdash \neg\neg p \to p$ (т.к. умеем выводить $\neg p \to \neg\neg\neg p$ из $\neg\neg p$)
7. $\neg\neg p \vdash p$

□

- (NN):
$$p \to \neg\neg p$$

Доказательство. 1. $(\neg\neg\neg p \to \neg p) \to (p \to \neg\neg p)$ (N)
2. $\vdash \neg\neg\neg p \to \neg p$ (предыдущий пункт, частный случай для $\neg p$)
3. $\vdash p \to \neg\neg p$ (MP)

□

-
$$\vdash (p \to q) \to (\neg q \to \neg p)$$

Доказательство. По теореме о дедукции она выводима тогда и только тогда, когда выводима $(p \to q) \vdash \neg q \to \neg p$. Докажем вспомогательную лемму

Лемма 8.4.
$$\vdash (p \to q) \to (\neg\neg p \to \neg\neg q)$$

Доказательство. Вывод эквивалентен $p \to q \vdash \neg\neg p \to \neg\neg q \iff p \to q, \neg\neg p \vdash \neg\neg q$.
По одному из прошлых пунктов знаем $\vdash \neg\neg p \to p$, по силлогизму получаем $\vdash \neg\neg p \to q$, $\vdash q \to \neg\neg q$, $\vdash \neg\neg p \to \neg\neg q$. □

Тогда получаем следующий вывод:

1. $p \to q \vdash \neg\neg p \to \neg\neg q$
2. $p \to q \vdash \neg q \to \neg p$ (N)

□

- (NI):

$$\vdash (p \to (\neg q \to \neg(p \to q)))$$

Доказательство. Достаточно вывести $p \vdash \neg q \to \neg(p \to q)$. Если сможем доказать $p \vdash (p \to q) \to q$, то получим требуемое (по предыдущему пункту $\neg q \to \neg(p \to q) \equiv (p \to q) \to p$). По теореме о дедукции это эквивалентно $p, p \to q \vdash q$, по MP это верно. □

9 Лекция 9 (логика предикатов)

«Все люди смертны, люди существуют, следовательно смертные существуют.»:

$$\forall x[\text{Man}(x) \to \text{Mortal}(x)] \land \exists x[\text{Man}(x)] \to \exists x[\text{Mortal}(x)]$$

Великая теорема Ферма:

$$\forall x[\forall y[\forall z[\forall n[n \geqslant 3 \to \neg(x^n + y^n = z^n)]]]]$$

Определение 9.1. Следующие строки являются (*корректными* (*valid*)) *термами* в логике предикатов:

- **Имя переменной**: последовательность буквенно-цифровых символов, начинающаяся с буквы из диапазона $u - z$. Например, x, $y12$, $zLast$.
- **Имя константы**: последовательность буквенно-цифровых символов, начинающаяся с цифры или буквы из диапазона $a - e$, либо одиночный символ подчёркивания (без других символов до или после). Например, 0, $e1$, $7x$, _.
- **n-арный вызов функции** вида $f(t_1, \dots, t_n)$, где f — имя функции, обозначаемое последовательностью буквенно-цифровых символов, начинающейся с буквы из диапазона $f - t$, где $n \geqslant 1$, и каждый t_i сам является (корректным) термом.

Примеры корректных термов: $plus(x, y)$, $s(s(0))$, $f(g(x), h(7, y), c)$.

Определение 9.2. *Предикат* P на множестве $\Omega \neq \varnothing$ — подмножество $P \subseteq \Omega^n$. Например, $(A, \leqslant)$, где $\leqslant \subseteq A \times A$.

Определение 9.3 (Индуктивное определение формулы)**.** Следующие строки являются *(корректными) формулами* в логике предикатов:

- **Равенство** вида $t_1 = t_2$, где t_1, t_2 — (корректные) термы. Например, $0 = 0$, $s(0) = 1$, $plus(x, y) = plus(y, x)$.
- **n-арный предикат** вида $R(t_1, \dots, t_n)$, где R — имя предиката, обозначаемое строкой буквенно-цифровых символов, начинающийся с буквы из диапазона $F - T$, где $n \geqslant 0$ (допускаются нульарные предикаты), и каждый t_i — терм. Например, $R(x, y)$, $Plus(s(0), x, s(x))$, $Q()$.
- **Отрицание** вида $\neg\phi$, где ϕ — формула (в Python: ~).
- **Бинарная операция** вида $(\phi * \phi)$, где * — один из бинарных операторов $\lor, \land, \to$, а ϕ, ψ — формулы (в Python — |, &, −>).
- **Кванторная конструкция** вида $Qx[\phi]$, где Q — либо квантор всеобщности $\forall$ (в Python — A), либо квантор существования $\exists$ (в Python — E), x — имя переменной, а ϕ — формула. Подформула ϕ, находящаяся внутри квадратных скобок в конструкции $Qx[\phi]$, называется *областью действия* квантора.

Примеры формул:

- $\forall x[x = x]$
- $\exists x[R(7, y)]$
- $\forall x[\exists y[R(x, y)]]$

- $\forall x[(R(x) \lor \exists x[Q(x)])]$

Есть два подхода к записи формул:

1. Как у нас, есть «полный» набор возможных символов и формально все можно использовать.
2. Мы сначала фиксируем набор символов, которые можно использовать (называется *сигнатура*), и определяем формулу в данной сигнатуре.

Теорема 9.1 (Об однозначности разбора терма)**.** *Существует единственное дерево разбора для каждого корректного терма.*

Теорема 9.2 (Об однозначности разбора формулы)**.** *TODO*

Определение 9.4 (Семантика)**.** *Моделью* (в логике предикатов) будем называть пару $M = (\Omega, I)$, где Ω — непустое множество элементов, которое будем называть *универсумом* (*носителем*) нашей модели, а I — *интерпретацией*, которая интерпретирует константные, функциональные и предикатные символы. При этом

- для константого символа c: $I(c) \in \Omega$
- для n-арного функционального символа f: $I(f) : \Omega^n \to \Omega$
- для n-арного предикатного символа P: $I(P) \subseteq \Omega^n$

Определение 9.5 (Истинность формул)**.** *Оценка* (*assignment*) A — отображение некоторого множества переменных в носитель модели Ω.

Значение терма t в данной модели M при данной оценке A определяется по индукции (это значение будем обозначать $[[t]]_{M,A}$)

Примеры:

- $[[c]]_{M,A} = I(c)$ — константа
- $[[x]]_{M,A} = A(x)$ — переменная
- $[[f(t_1, \dots, t_n)]] = I(f)([[t_1]]_{M,A}, \dots, [[t_n]]_{M,A})$ — функция

Как подсчитывать значение выражения:

- $[[t_1 = t_2]]_{M,A} = \text{True} \iff [[t_1]]_{M,A} = [[t_2]]_{M,A}$
- $[[P(t_1, \dots, t_n)]] = \text{True} \iff ([[t_1]]_{M,A}, \dots, [[t_n]]_{M,A}) \subseteq I(P)$
-
  - $[[\forall x[\phi]]]_{M,A} = \text{True} \iff [[\phi]]_{M,A'} = \text{True}$ для всех $w \subseteq \Omega$: $A'(x) = w \land A'(y) = A(y)$ для всех переменных $y \neq x$.
  - $[[\exists x[\phi]]]_{M,A} = \text{True}$ — то же самое, только вместо $\forall w$ имеем $\exists w$.

10 Лекция 10

Определение 10.1 (Истинность формул (формулы))**.** Истинность формул φ в данной модели $M = (\Omega, I)$ при данной оценке A определяется по индукции:

- $[[t_1 = t_2]]_{M,A} = \begin{cases} \text{True}, & \text{если } [[t_1]]_{M,A} = [[t_2]]_{M,A} \\ \text{False}, & \text{иначе} \end{cases}$
- $[[R(t_1, \dots, t_n)]]_{M,A} = \begin{cases} \text{True}, & \text{если } ([[t_1]]_{M,A}, \dots, [[t_n]]_{M,A}) \in [I(R)] \\ \text{False}, & \text{иначе} \end{cases}$
- $[[\neg\varphi]]_{M,A} = \neg[[\varphi]]_{M,A}$
- $[[\varphi * \psi]]_{M,A} = [[\varphi]]_{M,A} * [[\psi]]_{M,A}$, где $* \in \{\wedge, \vee, \to\}$
- $[[\forall x\varphi]]_{M,A} = \begin{cases} \text{True}, & \text{если для всех } u \in \Omega\colon [[\varphi]]_{M,A[x\mapsto u]} = \text{True} \\ \text{False}, & \text{иначе} \end{cases}$
- $[[\exists x\varphi]]_{M,A} = \begin{cases} \text{True}, & \text{если найдётся } u \in \Omega\colon [[\varphi]]_{M,A[x\mapsto u]} = \text{True} \\ \text{False}, & \text{иначе} \end{cases}$

Определение 10.2 (Связность/свободность переменных)**.** При «навешивании» квантора на формулу $Qx[\varphi]$ переменная x в формуле φ становится *связной*. Переменные, которые не являются связными, называются *свободными*. Одна и та же переменная может быть в одном месте свободной, а в другом месте – связной.

Пример:

$$(\forall x[P(x,y) \to x = f(x,y)] \wedge \exists y[x = y])$$

Связные переменные — x в первом кванторе, y во втором кванторе.

Определение 10.3. Формула φ называется *истинной в модели* M, если для любой оценки A

$$[[\varphi]]_{M,A} = \text{True}$$

Обозначение: $M \models \varphi$

Определение 10.4. Формула φ называется *общезначимой*, если она истинна в любой модели. Обозначение: $\models \varphi$.

Определение 10.5. Формулы φ_1, φ_2 называются *эквивалентными*, если для любой модели M и любой оценки A верно:

$$[[\varphi_1]]_{M,A} = [[\varphi_2]]_{M,A}$$

Обозначение: $\varphi_1 \equiv \varphi_2$.

Лемма 10.1 (Сведение эквивалентности к общезначимости)**.**

$$\varphi_1 \equiv \varphi_2 \iff \models \varphi_1 \leftrightarrow \varphi_2$$

Полезные эквивалентности:

$$\begin{gathered}
\exists x[\varphi(x)] \equiv \exists y[\varphi(y)] \\
\forall x[\varphi(x)] \equiv \forall y[\varphi(y)] \\
\neg\exists x[\varphi] \equiv \forall x[\neg\varphi] \\
\neg\forall x[\varphi] \equiv \exists x[\neg\varphi] \\
\exists x[\varphi] \land \psi \equiv \exists x[\varphi \land \psi] \text{ если } \psi \text{ не содержит } x \\
\forall x[\varphi] \land \psi \equiv \forall x[\varphi \land \psi] \text{ если } \psi \text{ не содержит } x \\
\text{аналогично для } \lor
\end{gathered}$$

Определение 10.6. Формула имеет предваренную нормальную форму, если все предикаты вынесены «наружу».

Теорема 10.1. *У любой формулы есть эквивалентная ей формула в предваренной нормальной форме.*

10.1 Выразимые предикаты

Пусть $M = (\Omega, I)$ — некоторая модель. Рассмотрим k переменных $x_1, \dots, x_n$ и формулу φ такую, что её множество свободных переменных содержится в множестве $\{ x_1, \dots, x_n \}$. Тогда можно считать, что значение формулы φ зависит от k параметров. При этом формуле φ будет соответствовать функция $\Omega^k \to \{ \mathrm{False}, \mathrm{True} \}$. Эквивалентным образом можно считать, что это не функция, а предикат P_φ арности k;

$$(u_1, \dots, u_k) \in P_\varphi \iff [[\varphi]]_{M, A[x_i \mapsto u_i]} = \mathrm{True}$$

Пример 1: $(\mathbb{N}, 0, s, +, \cdot, =)$ — модель. Рассмотрим формулу

$$\varphi = \exists z[x_1 + z = x_2]$$

Свободные переменные — x_1, x_2. Тогда задаётся предикат арности 2

$$P_\varphi = \{ (u_1, u_2) \mid u_1 \leqslant u_2 \}$$

Пример 2: модель та же, формула

$$\psi = \exists z \exists y[\neg z = 0 \land \neg z = s(0) \land \neg y = 0 \land \neg y = s(0) \land x = yz]$$

Тогда задаётся следующий предикат:

$$P_\psi = \{ n \mid n - \text{составное} \land n \geqslant 2 \}$$

Определение 10.7 (Выразимые предикаты)**.** Предикат R на множестве Ω называется *выразимым* в модели M, если существует формула φ такая, что $R = P_\varphi$.

Подмножество Ω по сути является предикатом арности 1. Поэтому мы будем также говорить и о выразимых множествах.

10.2 Изоморфизмы

Определение 10.8 (Изоморфизм)**.** Пусть $M_1 = (\Omega_1, I_1)$ и $M_2 = (\Omega_2, I_2)$ — две модели такие, что интерпретации интерпретируют одни и те же имена и арности этих имён совпадают. Функция $\alpha\colon \Omega_1 \to \Omega_2$ называется *изоморфизмом*, если она биекция и выполнены следующие условия:

1. $\alpha(I_1[c]) = I_2[c]$ для каждого константного имени из I_1;
2. $\alpha(I_1[f](u_1, \dots, u_k)) = I_2[f](\alpha(u_1), \dots, \alpha(u_k))$ для каждого функционального имени f из I_1 и $(u_1, \dots, u_k) \in \Omega_1^k$;
3. $(u_1, \dots, u_k) \in I_1[R] \iff (\alpha(u_1), \dots, \alpha(u_k)) \in I_2[R]$ для каждого предикатного имени R из I_1 и $(u_1, \dots, u_k) \in \Omega_1^k$.

Теорема 10.2. *Пусть $M_1 = (\Omega_1, I_1)$ и $M_2 = (\Omega_2, I_2)$ и α — изоморфизм, тогда для лююбого терма t и любой формулы φ верно, что (свободные) переменные, которые содержатся во множестве $\{ x_1, \dots, x_k \}$ верно следующее:*

1. $\alpha([[t]]_{M_1, A[x_i \mapsto u_i]}) = [[t]]_{M_2, A[x_i \mapsto \alpha(u_i)]}$

2. $[[\varphi]]_{M_1, A[x_i \mapsto u_i]} = [[\varphi]]_{M_2, A[x_i \mapsto \alpha(u_i)]}$

Доказательство. 1. Докажем по индукции.

База:

- $$\alpha([[c]]_{M_2, A[\dots]}) = \alpha(I_1[c]) = I_2[c] = [[c]]_{M_2, A[\dots]}$$
- $$\alpha([[x_i]]_{M_1, A[x_i \mapsto u_i]}) = \alpha(u_i) = [[x_i]]_{M_2, A[x_i \mapsto u_i]}$$

Шаг:

$$\begin{aligned}\alpha([[f(t_1, \dots, t_n)]]_{M_1, A[\dots]}) &= \alpha(I_1[f]([[t_1]]_{M_1, A}, \dots, [[t_n]]_{M_1, A})) = \\ &= I_2[f](\alpha([[t_1]]_{M_1, A}), \dots, \alpha([[t_n]]_{M_1, A})) = \\ &= I_2[f]([[t_1]]_{M_2, A[\dots]}, \dots, [[t_n]]_{M_2, A[\dots]}) = [[f(t_1, \dots, t_n)]]\end{aligned}$$

2.
- Знаем, что
$$[[t_1 = t_2]]_{M_1, A_1} \iff [[t_1]]_{M_1, A_1} = [[t_2]]_{M_1, A_1}$$
Тогда, используя инъективность функции α получим, что это эквивалентно
$$\underbrace{\alpha([[t_1]]_{M_1, A_1})}_{[[t_1]]_{M_2, A_2}} = \underbrace{\alpha([[t_2]]_{M_1, A_1})}_{[[t_2]]_{M_2, A_2}} \iff [[t_1 = t_2]]_{M_2, A_2} = \text{True}$$
- $$\begin{aligned}[[R(t_1, \dots, t_n)]]_{M_1, A_1} = \text{True} &\iff ([[t_1]]_{M_1, A_1}, \dots, [[t_n]]_{M_1, A_1}) \in I_1(R) \iff \\ &\iff (\alpha([[t_1]]_{M_1, A_1}), \dots, \alpha([[t_n]]_{M_1, A_1})) \in I_2(R) \iff \\ &\iff ([[t_1]]_{M_2, A_2}, \dots, [[t_n]]_{M_2, A_2}) \in I_2(R) \iff [[R(t_1, \dots, t_n)]]_{M_2, A_2}\end{aligned}$$

- Для бинарных функций доказательства аналогичны, докажем для конъюнкции:

$$\begin{aligned}[[\varphi_1 \land \varphi_2]]_{M_1,A_1} &= [[\varphi_1]]_{M_1,A_1} \land [[\varphi_2]]_{M_1,A_1} = \\ &= [[\varphi_1]]_{M_2,A_2} \land [[\varphi_2]]_{M_2,A_2} = \\ &= [[\varphi_1 \land \varphi_2]]_{M_2,A_2}\end{aligned}$$

- $$[[\forall y[\varphi]]]_{M_1,A_1} = \text{True} \iff \forall u \in \Omega_1([[\varphi]]_{M_1,A_1[y\mapsto u]} = \text{True})$$
$$[[\forall y[\varphi]]]_{M_2,A_2} = \text{True} \iff \forall u' \in \Omega_2([[\varphi]]_{M_2,A_2[y\mapsto u']} = \text{True})$$
  $\Longleftarrow$: Пусть $[[\varphi]]_{M_1,A[x_i\mapsto u_i, y\mapsto u]} = \text{False} \iff [[\varphi]]_{M_2 A[x_i\mapsto \alpha(u_i), y\mapsto \alpha(u)=u']} = \text{False}$
  $\Longrightarrow$:

TODO: дописать □

Определение 10.9. *Автоморфизмом* называется изоморфизм в себя, т.е. функция $\alpha\colon \Omega \to \Omega$, являющаяся изоморфизмом для модели $M = (\Omega, I)$.

Очевидно, что тождественное отображение является автоморфизмом. Такой автоморфизм будем называть *тривиальным.* Но существуют и нетривиальные автоморфизмы.

Определение 10.10. Предикат $R \subseteq \Omega^k$ *сохраняется при отображении* $\alpha\colon \Omega \to \Omega$, если $(u_1, \ldots, u_k) \in R \iff (\alpha(u_1), \ldots, \alpha(u_k)) \in R$.

Теорема 10.3 (Критерий невыразимости)**.** *Если предикат R не сохраняется при автоморфизме, то он невыразим никакой формулой.*

Доказательство. Рассмотрим предикат $R \subseteq \Omega^k$, тогда $\exists \varphi\colon P_\varphi = R$. Возьмём $(u_1, \ldots, u_k)$. Тогда

$$\begin{aligned}(u_1, \ldots, u_k) \in R &\iff [[\varphi]]_{M,A[x_i\mapsto u_i]} = \text{True} \iff \\ &\iff [[\varphi_1]]_{M,A[x_i\mapsto \alpha(u_i)]} = \text{True} \iff \\ &\iff (\alpha(u_1), \ldots, \alpha(u_k)) \in R\end{aligned}$$

□

11 Лекция 11

В пропозициональной логике мы смогли свести все высказывания к высказываниям лишь с операторами $\neg$ и $\to$. То же самое можно сделать и в логике предикатов; в логике предикатов можно избавиться от равенства и функциональных имён.

Рассмотрим две модели:

$$M_1 = (\mathbb{N}; 0, s, +, \cdot, =),\ M_2 = (\mathbb{N}; 0, S, P, M, =)$$

Пусть для этих моделей верно следующее:

$$\begin{aligned} x = s(y) &\iff (x, y) \in S \\ x = y + z &\iff (x, y, z) \in P \\ x = y \cdot z &\iff (x, y, z) \in M \end{aligned}$$

Возьмём формулу

$$\exists y[\exists t[x = \underbrace{y \cdot y}_{z1} + \underbrace{t \cdot t}_{z2}]]$$

Тогда её также можно переписать, не используя функции и равенство:

$$\begin{aligned} &\exists y \exists t[\exists z1[\underbrace{y \cdot y = z1}_{M(z1,y,y)} \wedge \exists z2[\underbrace{z2 = t \cdot t}_{M(z2,t,t)} \wedge \exists z3[\underbrace{z3 = z1 + z2}_{P(z3,z1,z2)} \wedge x = z3]]]] \equiv \\ &\equiv \exists y \exists t[\exists z1[M(z1, y, y) \wedge \exists z2[M(z2, t, t) \wedge \exists z3[P(z3, z1, z2) \wedge x = z3]]]] \end{aligned}$$

Идея состоит в том, что каждую функцию f арности k заменяют на предикат F арности $k+1$, такой что

$$y = f(x_1, \ldots, x_k) \iff (y, x_1, \ldots, x_k) \in F$$

При этом будем использовать *каноническое представление* предикатных имён, соответствующих функциональным. Для этого будем заменять первую букву в имени функции на заглавную.

Осталось убедиться, что всё, что можно было выразить в старой модели, можно будет выразить в новой и наоборот.

Определение 11.1. Для модели M с функциями будем называть модель M' *бесфункциональным аналогом* модели M, если в M' удалены все функции и добавлены предикаты, соответствующие функциям в M, и они имеют канонические имена.

Определение 11.2. Пусть φ — формула, которая может содержать функции. Будем говорить, что формула φ' является *бесфункциональным аналогом* формулы φ, если

- φ' содержит те же предикаты, что и φ, при этом φ' будет содержать ещё предикаты, соответствующие функциям из φ, переименованным каноническим образом;
- TODO

Хотелось бы, чтобы для новой формулы выполнялось и обратное утверждение, т.е., если φ' истинна в некоторой модели M', то найдётся модель M, в которой истинна φ и M' является бесфункциональным аналогом M.

Действительно, если φ' истинна в некоторой модели, то нет гарантии, что предикат F, соответствующий функции f в исходной формуле, можно представить в виде $y = f(x_1, \dots)$. Чтобы это всегда можно было сделать, нужно добавить условия того, что все предикаты, соответствующие функциям, должны обладать тотальностью и функциональностью.

Теорема 11.1. *Для любого множества Γ формул (которые могут содержать функции) существует множество формул Γ' без функций, получаемое из Γ с помощью эффективной синтаксической процедуры, такое, что Γ имеет модель тогда и только тогда, когда Γ' имеет модель. Более того, имея модель Γ', существует простой и естественный способ преобразовать её в модель Γ и наоборот.*

Вообще говоря, равенство ведёт себя как предикат, но имеет некоторые особенности. Заменим его на предикат $SAME$, т.е. везде вместо $t_1 = t_2$ будем писать $SAME(t_1, t_2)$. При этом, если предикат $SAME$ будет интерпретироваться равенством,

$$(x, y) \in SAME \iff x = y,$$

то истинность после замены будет сохраняться.

Как и в случае с функциями, хотелось бы, чтобы выполнялось и обратное, т.е. любую модель новой формулы можно было получить естественным преобразованием из некоторой модели старой формулы. Для этого надо добавить свойства, которым удовлетворяют равенства, переписанные для $SAME$.

Аксиомы равенства для $SAME$:

1. $SAME$ — отношение эквивалентности:

$$\forall x[SAME(x, x)]$$

$$\forall x[\forall y[SAME(x, y) \to SAME(y, x)]]$$

$$\forall x[\forall y[\forall z[((SAME(x, y) \wedge SAME(y, z)) \to SAME(x, z))]]]$$

2. Все предикаты и функции «уважают» $SAME$. Для каждой функции f арности k в модели надо добавить:

$$\forall x_1 \dots \forall x_k \forall y_1 \dots \forall y_k[(SAME(x_1, y_1) \wedge \dots, \wedge SAME(x_k, y_k)) \to SAME(f(x_1, \dots, x_k), f(y_1, \dots, y_k))]$$

   Для каждого предиката R арности k:

$$\forall x_1 \dots \forall x_k \forall y_1 \dots \forall y_k[(SAME(x_1, y_1) \wedge \dots SAME(x_k, y_k)) \to (R(x_1, \dots, x_k) \to R(y_1, \dots, y_k))]$$

Теорема 11.2. *Пусть M' — модель формулы φ_s, тогда существует модель M, которая является моделью φ и наоборот.*

Доказательство. Пусть $M' = (\Omega', I')$ — модель φ'_s. Возьмём $M = (\Omega, I)$, определённую следующим образом:

- $\Omega = \Omega'/SAME = \{ [m] \mid m \in \Omega' \}$, (фактор-множество), где $[m] = \{ m' \mid (m, m') \in SAME \}$.
-   - $I(c) = [I'(c)]$

- $I(f) = f_M([m_1], \dots, [m_k]) = [f'_M(m_1, \dots, m_k)]$
- $I(R) = R_M \colon ([m_1], \dots, [m_k]) \in R_M \iff (m_1, \dots, m_k) \in R_{M'}$

Остаётся проверить корректность определения.

$$SAME(m_1, m'_1) \land \ldots \land SAME(m_k, m'_k) \implies SAME(f_{M'}(m_1, \dots, m_k), f_{M'}(m'_1, \dots, m'_k))$$

Теперь покажем, что для любого терма t верно $[[t]]_{M,A} = [[[t]]_{M',A'}]$, где $A(x) = [A'(x)]$. Доказывается индукцией по длине терма.

Для любой формулы ψ, использующей те же функции и предикаты, что φ, верно $[[\psi]]_{M,A} = [[\psi]]_{M',A'}$. Доказывается индукцией по длине формулы. $\square$

12 Лекция 12 TODO

13 Лекция 13

13.1 Выводы

Определение 13.1. *Выводом* в исчислении предикатов называется последовательность строк, каждая строка при этом может быть:

1. *Тавтологией*, которые представляют собой булевы формулы-тавтологии, в которых переменные заменены на формулы логики предикатов;
2. *Аксиомой*, которые будут задаваться схемами. Список схем может отличаться.

$$(\forall x[\varphi(x)] \to \varphi(t)), \text{ где } \varphi \text{ — формула, } x \text{ — переменная, } t \text{ — терм}$$

3. Или получены из предыдущих строк с помощью *правила вывода*. Правил вывода с непустым множеством посылок у нас будет два: *Modus Ponens (MP)*:

$$\frac{\varphi, (\varphi \to \psi)}{\psi}$$

и *правило обобщения (Gen)*:

$$\frac{\varphi}{\forall x[\varphi]}.$$

Замечание. Мы знаем теорему о полноте для логики высказываний, поэтому мы могли бы вместо тавтологий добавить схемы аксиом Гильберта (заменяя переменные на формулы). Множество выводимых формул при этом не изменяется, но усложняются выводы.

Определение 13.2. Схемы мы будем представлять в виде обычных формул, но с другим пониманием имён:

В формуле	В схеме
имя константы	терм
имя переменной	переменная
имя предиката	формула

Заметим, что тут нам пригодится то, что мы разрешили иметь нульарные предикатные имена в формулах.

13.2 Ограничения на подстановки

Хотелось бы, чтобы после вставки смысл формулы не менялся. В частности, подстановка не должна портить истинность.

Рассмотрим следующую схему:

$$\forall x[\varphi(x)] \to \varphi(c).$$

Она очевидно истинна при любой разумной интерпретации. Теперь вместо $\varphi(x)$ подставим $\exists y[y = x]$, а вместо c подставим $y + 1$, получится

$$\forall x[\exists y[x = y]] \to \exists y[y + 1 = y].$$

Это неверное утверждение, например, в $\mathbb{N}$.

Нужно вводить ограничения, а именно:

1. Термы не должны содержать переменные, такие что терм попадёт в область действия квантора по этой переменной;
2. Не должно быть кванторов по переменным, которые попадают в область действия кванторов по тем же переменным.

Определение 13.3 (Общезначимость)**.** Формула φ называется *общезначимой*, если она истинна во всех моделях при всех оценках, в которых интерпретируются все имена, используемые в этой формуле.

Схема называется *общезначимой*, если все корректные подстановочные варианты этой схемы являются общезначимыми.

Доказательство общезначимости

$$\forall x[\varphi(x)] \to \varphi(t).$$

Доказательство. $\models_{M,A} \forall x[\varphi(x)] \iff \forall m \in M\colon \models_{M,A[x\mapsto m]} \varphi(x) \implies \models_{M,A[x\mapsto m']} \varphi(x) \iff \models_{M,A} \varphi(c)$, где $[[t]]_{M,A} = m'$ □

13.3 Схемы аксиом

- Универсальная конкретизация (UI):

$$(\forall x[\varphi(x)] \to \varphi(c));$$

- Экзистенциальное введение (EI):

$$(\varphi(c) \to \exists x[\varphi(x)]);$$

- Универсальное упрощение (US):

$$(\forall x[(\psi \to \varphi(x))] \to (\psi \to \forall x[\varphi(x)])),\ \text{если } \psi \text{ не содержит свободной переменной } x;$$

- Экзистенциальное упрощение (ES):

$$(\forall x[(\varphi(x) \to \psi)] \to (\exists x[\varphi(x)] \to \psi)),\ \text{если } \psi \text{ не содержит свободной переменной } x$$

Теорема 13.1 (О корректности)**.** *Все схемы аксиом выше корректны, т.е. при правильной подстановке дают общезначимые формулы, а правила вывода (MP) и (GEN) сохраняют общезначимость.*

Доказательство. (UI) проверяли, доказательство (EI) аналогичное. Проверка (MP) аналогична доказательству для логики высказываний. Докажем утверждение для (Gen):

$$\frac{\varphi(x)}{\forall x[\varphi(x)]}.$$

По сути надо доказать следующие две леммы:

Лемма 13.1. *Пусть M — модель, A — оценка, для любых формул φ, ψ верно*

$$(\models_{M,A} (\varphi \to \psi)) \land (\models_{M,A} \varphi) \implies \models_{M,A} \psi$$

Лемма 13.2. *Пусть M — модель, $\varphi(x)$ — формула. Тогда, если для любой оценки A истинно $\models_{M,A} \varphi(x)$, то для любой оценки A истинно $\models_{M,A} \forall x[\varphi(x)]$.*

TODO? $\square$