

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)	2
2	Лекция 2 (модели, ДНФ)	3
2.1	Модели	3
2.2	Виды формул	3
2.3	ДНФ	4
2.4	Алгоритмическая сложность	4
2.4.1	Задача о нахождении ДНФ по таблице истинности	4
2.4.2	Задача о проверке тавтологичности	4
3	Лекция 3 (полнота и максимальность)	6
4	Лекция 4 (теорема Поста)	9
4.1	Продолжение про классы функций	9
4.2	Замены	11
5	Лекция 5 (выводы)	12
5.1	Правила вывода	12
5.2	Конкретные правила	13
6	Лекция 6 (продолжение про выводы)	14
6.1	Примеры допустимых правил	14
6.2	Противоречивость и непротиворечивость	16
7	Лекция 7	18
7.1	Основное множество правил	18
8	Лекция 8	22
8.1	Доказательства аксиом	23
9	Лекция 9 (логика предикатов)	26

1 Лекция 1 (введение)

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

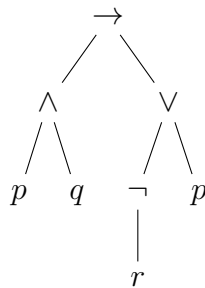
Определение 1.2. Формула — последовательность символов из алфавита, определяемая по индукции:

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

Формулы удобно представлять в виде дерева, например для формулы

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

дерево выглядит следующим образом:



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

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

Тогда B — префикс ($B \sqsubseteq A$), если $B = a_1 \dots a_k \ (k \leq n)$.

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. $A \in \text{Prop}$
2. $A \in \{ \top, \perp \}$
3. $\exists! B: A = \neg B$
4. $\exists! B, C: A = (B * C)$, где $*$ $\in \{ \wedge, \vee, \rightarrow \}$

2 Лекция 2 (модели, ДНФ)

2.1 Модели

Определение 2.1. *Модель* — функция $\text{Var} \rightarrow \mathbb{B} = \{0, 1\}$. 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 $M(A)$:

- $M(\top) = 1$, $M(\perp) = 0$;
- 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 $A = (B_1 \odot B_2)$, $\odot \in \{\vee, \wedge, \rightarrow\}$.

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

2.2 Виды формул

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

Пример: $p \rightarrow p$, $p \vee \neg p$

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 на Земные"

Утверждение можно записать следующей формулой:

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

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 $q = \top$, $(p \rightarrow q \vee r) = \top$, $(r \rightarrow s) = \top$, $s = \top$. 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. \square

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, \perp)

x	\perp	x	$\neg x$	\top
0	0	0	1	1
1	0	1	0	1

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:

- $x \uparrow x = \neg x$
- $x \uparrow y = \neg(x \wedge y)$
- $\neg(x \uparrow y) = \neg\neg(x \wedge y) = x \wedge y$
- $x \vee y = \neg(\neg x \wedge \neg y)$

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. $\forall f_1, \dots, f_n \in [G] \wedge g(x_1, \dots, x_n) \in G \hookrightarrow g(f_1(x_1, \dots, x_{m_1}), \dots, f_n(x_1, \dots, x_{m_n})) \in [G]$
3. $[G]$ содержит все тождественные проекции, т.е. $\forall n \in \mathbb{N}, i < n: p_i^n(x_1, \dots, x_n) \equiv x_i$

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 $\forall f \in F_n \setminus G \hookrightarrow G \cup \{f\}$ — полный класс. Эквивалентно, $[G \cup \{f\}] = F_n$.

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

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 $f(x_1, \dots, x_n) = g(f_1(x_1, \dots, x_n), \dots, f_m(x_1, \dots, x_n))$. По предположению индукции $f_i \in [G] \forall i$. Таким образом, $f \in [G]$ как композиция.

□

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

Доказательство. \Leftarrow — очевидно ©

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

1. Случай 1: $[H]$ — максимальна, тогда всё хорошо.
2. Случай 2: $[H]$ — не максимальна $\implies \exists f \in F_n \setminus [H]: [[H] \cup \{f\}] \neq F_n$. 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.

□

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

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 $\{\rightarrow, \perp\}$.

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

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

верно

$$x_1 \leq y_1, \dots, x_n \leq y_n,$$

то выполняется

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

Пример монотонной функции: $x_1 \wedge x_2$.

Пример немонотонной функции: $x_1 \rightarrow x_2$.

Лемма 4.1. M является максимальным замкнутым классом.

Доказательство. Докажем замкнутость. Возьмём набор функций

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

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

Теперь докажем максимальность. Возьмём $h \notin M$. Заметим, что $0, 1 \in M$. Тогда $\exists x_1 \leq y_1, \dots, x_m \leq y_m: h(\vec{x}) > h(\vec{y})$, т.е. $h(\vec{x}) = 1$ и $h(\vec{y}) = 0$. Пусть $\vec{x} \preceq \vec{y} \iff x_1 \leq y_1 \wedge \dots \wedge x_n \leq y_n$.

Лемма 4.2 (Вспомогательная лемма). Пусть $\vec{x} \preceq \vec{y}$. Тогда $\exists \vec{x}^1, \dots, \vec{x}^k: \vec{x}^1 = \vec{x} \wedge \vec{x}^k = \vec{y}$ и \vec{x}^i отличается от \vec{x}^{i+1} в одной координате и $\vec{x} = \vec{x}^1 \preceq \vec{x}^2 \preceq \dots \preceq \vec{x}^k = \vec{y}$.

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

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

$$h(\dots \underbrace{0}_j \dots) = 1, h(\dots \underbrace{1}_j \dots) = 0 \implies h(\dots \underbrace{p}_j \dots) = \neg p$$

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

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

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

Пример несамодвойственной функции: $x \wedge y$.

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

Лемма 4.3. *S является максимальным замкнутым классом.*

Доказательство. Докажем замкнутость. Пусть

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

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 $\exists x_1, \dots, x_n: h(\overline{x_1}, \dots, \overline{x_n}) = h(x_1, \dots, x_n)$.

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

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

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 $\{\neg, V, 0\}$. \square

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 однозначны (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 $\mathbb{B}^n \rightarrow \mathbb{B}$ 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. \square

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 $g(x_1, \dots, x_n) = x_1 x_2 \dots x_m + \dots$. Рассмотрим $g(x_1, x_2, 1, \dots, 1)$:

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

$x_1, x_2 \in L$, 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 $\{\wedge, \neg\}$. \square

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:

- \Leftarrow : Если H содержится в каком-то собственном замкнутом классе, то он не полон;
- \Rightarrow : 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 $f_0(x, \dots, x)$ либо равна 1, либо $\neg x$.
 - Возьмём функцию $f_1 \in H: f_1 \notin T_1$. Тогда $f_1(x, \dots, x)$ 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

\square

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. \square

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:

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

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: $\frac{p}{p}, \frac{p \rightarrow q, q \rightarrow r}{p \rightarrow r}$ (силлогизм); пример некорректных правил: $\frac{p}{p}, \frac{p}{p \wedge q}$.

Определение 5.2. Правило вывода $\frac{\Delta}{\psi}$ является частным случаем правила $\frac{\Gamma}{\phi}$, если существуют формулы $\theta_1, \dots, \theta_n$ и переменные p_1, \dots, 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, $\frac{(x \rightarrow x) \wedge (\neg y)}{x \rightarrow x}$ — частный случай правила $\frac{p \wedge q}{p}$.

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 случая 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:

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

Тогда примером вывода будет:

$$\begin{array}{l} p \rightarrow \neg p \\ \neg \neg(p \rightarrow \neg p) \end{array}$$

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

$$\frac{\neg p \rightarrow q}{p \rightarrow q}.$$

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

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 $\varphi_1, \dots, \varphi_n: \forall i: \Gamma \models \varphi_i$.

База: $i = 1 \implies$

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

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

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

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

Доказательство. Имеем $\eta_1 = \varphi_1[p_1/\theta_1, p_2/\theta_2, \dots, p_n/\theta_n], \dots, \eta_n = \varphi_n[p_1/\theta_1, p_2/\theta_2, \dots, p_n/\theta_n]$
 P — корректна $\implies \forall M: \varphi_1, \dots, \varphi_n$ истинны $\implies \varphi$ — истинна.

Пусть η_1, \dots, η_n истинны в модели M . Возьмём M' такую, что $\forall i: M' \models p_i \iff M \models \theta_i$.

Утверждение: $\forall \varphi: \mathcal{M} \models \varphi \iff \mathcal{M} \models \varphi[p/\theta_1]$. Доказывается индукцией по длине φ . □

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

5.2 Конкретные правила

Определение 5.4. *Modus Ponens:*

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

Определение 5.5. *Аксиомы Гильберта:*

1. (I1):

$$q \rightarrow (p \rightarrow q)$$

2. (D):

$$(p \rightarrow (q \rightarrow r)) \rightarrow ((p \rightarrow q) \rightarrow (p \rightarrow r))$$

3. (N):

$$(\neg q \rightarrow \neg p) \rightarrow (p \rightarrow q)$$

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. \square

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 $\lambda = \frac{\Delta}{\psi}$, $\rho = \frac{\Gamma}{\varphi}$, 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 $\frac{\xi_{j_1}, \dots, \xi_{j_l}}{\xi_i}$ 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 $\Gamma \vdash_{\mathcal{R}} \varphi$. \square

6.1 Примеры допустимых правил

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

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

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

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

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

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

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

1. ...
2. $\varphi \rightarrow \psi$

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

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

□

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

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 $i \leq n$ верно

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

Разберём случаи:

- Возьмём $\xi_i = \varphi$. Докажем, что $\Gamma \vdash_{\mathcal{R}} (\varphi \rightarrow \varphi)$. Но уже доказывали (в ДЗ), что из пустого множества посылок доказуемо выражение $p \rightarrow p$, а $\varphi \rightarrow \varphi$ — его частный случай.
- Пусть теперь $\xi_i \in \Gamma$. Тогда нужно построить вывод $\Gamma \vdash_{\mathcal{R}} (\varphi \rightarrow \xi_i)$. Тогда
 1. ξ_i
 2. $\xi_i \rightarrow (\varphi \rightarrow \xi_i)$ (I1)
 3. $\varphi \rightarrow \xi_i$ (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 $\xi_j \rightarrow \xi_i$. По предположению индукции $\Gamma \vdash_{\mathcal{R}} (\varphi \rightarrow \xi_j)$ и $\Gamma \vdash_{\mathcal{R}} \underbrace{(\xi_j \rightarrow \xi_i)}_{\xi_k}$. Тогда получаем следующий вывод:

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

□

6.2 Противоречивость и непротиворечивость

Рассмотрим аксиому

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

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 $\neg(p \rightarrow p)$ выводится из Γ в \mathcal{R} ($\Gamma \vdash_{\mathcal{R}} \neg(p \rightarrow p)$)
- 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: $\neg(p \rightarrow p)$ 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. $\neg\varphi \rightarrow (\varphi \rightarrow \psi)$ (I2)
6. $\varphi \rightarrow \psi$ (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.,

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

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

Тогда имеем вывод

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

□

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

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

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

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

□

7 Лекция 7

7.1 Основное множество правил

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

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 $b \in \{\text{True}, \text{False}\}$, тогда

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

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

Определим множество формул

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

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

Лемма 7.1. Пусть φ — формула, и M оценивает все формулы из Γ_M 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 $M[\varphi] = \text{False}$. 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 $\vdash (\psi \rightarrow \neg\neg\psi)$ (правило NN). Вывод для $\neg\neg\psi$ выглядит так:

1. ...
2. ψ
3. $\psi \rightarrow \neg\neg\psi$ (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

- $\varphi = (\psi_1 \rightarrow \psi_2)$. 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 $\neg\psi_1, \neg\psi_2 \vdash (\psi_1 \rightarrow \psi_2)$ с помощью I2 ($\neg p \rightarrow (p \rightarrow q)$). Имеем вывод
 1. ...
 2. $\neg\psi_1$
 3. $\neg\psi_1 \rightarrow (\psi_1 \rightarrow \psi_2)$ (I2)
 4. $\psi_1 \rightarrow \psi_2$ (MP)
2. False, True. Докажем $\neg\psi_1, \psi_2 \vdash (\psi_1 \rightarrow \psi_2)$ (I2) или (I1). То же самое, т.к. ψ_2 в прошлом выводе не участвовал.
3. True, False. Докажем $\psi_1, \neg\psi_2 \vdash \neg(\psi_1 \rightarrow \psi_2)$ (NI). Получим вывод
 1. ...
 2. ψ_1
 3. ...
 4. $\neg\psi_2$
 5. $\psi_1 \rightarrow (\neg\psi_2 \rightarrow \neg(\psi_1 \rightarrow \psi_2))$ (NI)
 6. $\neg\psi_2 \rightarrow \neg(\psi_1 \rightarrow \psi_2)$ (MP)
 7. $\neg(\psi_1 \rightarrow \psi_2)$ (MP)
4. True, True. Докажем $\psi_1, \psi_2 \vdash (\psi_1 \rightarrow \psi_2)$. Соответствующий вывод:
 1. ...
 2. ψ_2
 3. $\psi_2 \rightarrow (\psi_1 \rightarrow \psi_2)$ (I1)
 4. $\psi_1 \rightarrow \psi_2$ (MP)

□

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 $\Gamma \vdash p \rightarrow \varphi$, а из второго $\Gamma \vdash \neg p \rightarrow \varphi$. Получим вывод:

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

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

□

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.ч. 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 $\Gamma' \vdash \varphi$. Прделаав так с каждой парой моделей мы уменьшим на 1 количество посылок. Действуя так мы сможем избавиться от всех посылок. □

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. \Leftarrow было в теореме о корректности.

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

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

Осталось показать, что

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

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

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:

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

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

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

4. $p \rightarrow p$ (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 $\Gamma \vdash \neg(p \rightarrow p)$, т.е. имеем вывод

1. ...

2. $\neg(p \rightarrow p)$,

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

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

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 $\varphi_0, \varphi_1, \dots$

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 $\Delta \vdash \neg(p \rightarrow p)$. Такой вывод использует конечное число формул, а значит $\exists n: \Gamma_n \vdash \neg(p \rightarrow p) \implies \Gamma_n$ — противоречиво, что противоречит построению Γ_n

- Максимальность

Пусть оно не максимально, т.е. $\exists \varphi \notin \Delta: \Delta \cup \{\varphi\}$ — непротиворечиво. Тогда $\exists n: \varphi = \varphi_n$, но тогда $\Gamma_{n+1} = \Gamma_n \cup \{\varphi_n\}$

1. $\Gamma_n \cup \{\varphi_n\}$ — противоречиво, тогда $\Gamma_n \cup \{\varphi_n\} \vdash \neg(p \rightarrow p)$, откуда следует $\Delta \vdash \neg(p \rightarrow p)$, а значит Δ противоречиво, 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:

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

Доказательство. • Пусть оба $\in \Delta$, тогда получаем $\Delta \vdash \psi$ и $\Delta \vdash \neg\psi$ и Δ противоречиво

Пусть оба $\notin \Delta$. Тогда по максимальной 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:

– $(\psi_1 \rightarrow \psi_2) \in \Delta$ и $\psi_1 \in \Delta$ и $\neg\psi_2 \in \Delta$, тогда $\Delta \vdash (\psi_1 \rightarrow \psi_2)$ и $\Delta \vdash \psi_1$. По МР получаем $\Delta \vdash \psi_2$, но $\Delta \vdash \neg\psi_2$, откуда Δ противоречиво.

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

□

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:

- $\varphi = \neg\psi$

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

$$(\psi_1 \rightarrow \psi_2) \in \Delta \iff (\psi_1 \notin \Delta \vee \psi_2 \in \Delta) \iff M_\Delta[\psi_1] = \text{False} \vee M_\Delta[\psi_2] = \text{True} \iff M_\Delta[\psi_1 \rightarrow \psi_2] = \text{True}$$

□

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

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

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

\Leftarrow 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. □

8.1 Доказательства аксиом

Напоминание про силлогизм:

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

- (I0):

$$p \rightarrow p$$

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

□

- (I2):

$$\neg p \rightarrow (p \rightarrow q)$$

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

□

- Вспомогательная аксиома

$$\vdash \neg \neg p \rightarrow p$$

Доказательство. По лемме о дедукции доказательство аксиомы эквивалентно доказательству $\neg \neg p \vdash p$. Хотим вывести $\vdash \neg \neg p \rightarrow (\neg \neg p \rightarrow p)$

1. $\neg \neg p \rightarrow (\neg \neg \neg p \rightarrow \neg \neg p)$ (I1)
2. $\neg \neg p \vdash \neg \neg \neg p \rightarrow \neg \neg p$
3. $(\neg \neg \neg p \rightarrow \neg \neg p) \rightarrow (\neg p \rightarrow \neg \neg p)$ (N)
4. $\neg \neg p \vdash \neg p \rightarrow \neg \neg p$ (т.к. умеем выводить $\neg \neg \neg p \rightarrow \neg \neg p$ из $\neg \neg p$)
5. $(\neg p \rightarrow \neg \neg p) \rightarrow (\neg \neg p \rightarrow p)$ (N)
6. $\neg \neg p \vdash \neg \neg p \rightarrow p$ (т.к. умеем выводить $\neg p \rightarrow \neg \neg p$ из $\neg \neg p$)
7. $\neg \neg p \vdash p$

□

- (NN):

$$p \rightarrow \neg \neg p$$

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

□

-

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

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

Лемма 8.4.

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

Доказательство. Вывод эквивалентен $p \rightarrow q \vdash \neg\neg p \rightarrow \neg\neg q \iff p \rightarrow q, \neg\neg p \vdash \neg\neg q$.

По одному из прошлых пунктов знаем $\vdash \neg\neg p \rightarrow p$, по силлогизму получаем $\vdash \neg\neg p \rightarrow q$,
 $\vdash q \rightarrow \neg\neg q$, $\vdash \neg\neg p \rightarrow \neg\neg q$. \square

Тогда получаем следующий вывод:

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

\square

- (NI):

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

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

9 Лекция 9 (логика предикатов)

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

$$\forall x[\text{Man}(x) \rightarrow \text{Mortal}(x)] \wedge \exists x[\text{Man}(x)] \rightarrow \exists x[\text{Mortal}(x)]$$

Великая теорема Ферма:

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

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 $n \geq 1$, 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 $\Omega \neq \emptyset$ — подмножество $P \subseteq \Omega^n$. Например, (A, \leq) , где $\leq \subseteq A \times A$.

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 $n \geq 0$ (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: \sim).
- **Бинарная операция** вида $(\phi * \psi)$, где $*$ — один из бинарных операторов $\vee, \wedge, \rightarrow$, 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:

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

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

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 константного символа c : $I(c) \in \Omega$
- для n -арного функционального символа f : $I(f) : \Omega^n \rightarrow \Omega$
- 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 $w \subseteq \Omega$: $A'(x) = w \wedge A'(y) = A(y)$ для всех переменных $y \neq x$.
- — $[[\exists x[\phi]]]_{M,A} = \text{True}$ — то же самое, только вместо $\forall w$ имеем $\exists w$.