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)

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

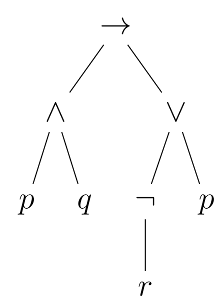
Определение 1.2. *Формула* — последовательность символов из алфавита, определяемая по индукции:

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:

$$((p \to q \lor r) \land (r \to s) \land s) \to \neg q$$

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 $q = \top$, $(p \to q \lor r) = \top$, $(r \to s) = \top$, $s = \top$. 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. Для любой булевой функции существует булева

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:

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

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. $\forall n \in \mathbb{N}, i < n \colon p_i^n(x_1, \dots, x_n) \equiv x_i$

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

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

Лемма 3.1. *Свойства замыкания:*

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

Доказательство. $\subset$ — 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 $f(x_1, \dots, x_n) = g(f_1(x_1, \dots, x_n), \dots, f_n(x_1, \dots, x_n))$. 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. $\impliedby$ — 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.

□

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:

- $h(1, \dots, 1) = 1 \implies h(x, \dots, x) \equiv 1$
- $h(1, \dots, 1) = 0 \implies h(x, \dots, x) \equiv \neg x$

Имея отрицание (из второго пункта) получим конъюнкцию, а имея её и отрицание выразим все остальные операции.
Если же $h(x, \dots, x) = 1$, то просто возьмём полную систему $\{\oplus, \wedge, 1\}$. Для каждой и функций множества принадлежность к классу T_0 очевидна.

$\square$

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 $\{\to, \perp\}$.

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

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

то выполняется

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

Пример монотонной функции: $x_1 \wedge x_2$.

Пример немонотонной функции: $x_1 \to x_2$.

Лемма 4.1. *M является максимальным замкнутым классом.*

Доказательство. Докажем замкнутость. Возьмём набор функций

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

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

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

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

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 $\exists i\colon h(\vec{x}^i) = 1 \wedge h(\vec{x}^{i+1}) = 0$. 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. □

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

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

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 $\neg 0 = 1$

Рассмотрим $x_1 \wedge x_2 \oplus x_2 \wedge x_3 \oplus x_1 \wedge x_3$. Тогда в поле $\mathbb{F}_2$ получаем:

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

□

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 $g(x_1, \dots, x_n) = x_1x_2 \dots x_m + \dots$ □

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 0, 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 $\wedge$

$\square$

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:

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

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. 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* $\dfrac{\phi_1, \ldots, \phi_n}{\phi}$ *корректно и* $\frac{\eta_1, \ldots, \eta_n}{\eta}$ *— частный случай* (P)*, то оно тоже корректно.*

   Доказательство. Имеем $\eta_1 = \psi_1[p_1/\theta_1, p_2/\theta_2, \ldots, p_n/\theta_n], \ldots, \xi = \varphi[p_1/\theta_1, p_2/\theta_2, \ldots, p_n/\theta_n]$
   P — корректна $\implies \forall \mathcal{M} \colon \psi_1, \ldots, \psi_n$ истинны $\implies \varphi$ — истинна.
   Пусть $\eta_1, \ldots, \eta_n$ истинны в модели $\mathcal{M}$. Возьмём $\mathcal{M}'$ такую, что $\forall i \colon \mathcal{M}' \models p_i \iff \mathcal{M} \models \theta_i$.
   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 $\frac{\Delta}{\varphi}$ — частный случай правила $\frac{\Gamma}{\psi}$, то*

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

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. TODO □

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. Пусть есть набор формул Γ, $\varphi \to \psi$, φ. Тогда по modus ponens ψ. □

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 $\xi_1, \xi_2, \ldots, \xi_n = \psi$ — вывод из $\Gamma \cup \{ \varphi \}$. 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 вид.
- Пусть теперь $\xi_i \in \Gamma$. Тогда нужно построить вывод $\Gamma \vdash_{\mathcal{R}} (\varphi \to \xi_i)$. Тогда

1. ξ_i
2. $\xi_i \to (\varphi \to \xi_i)$ $(I0)$
3. $\varphi \to \xi_i$ (MP)

- ξ_i получена по правилу $(I1)$ или (D) (с пустым множеством посылок). То же самое вроде.
- 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 вывод будет иметь вид $\ldots \varphi \to \xi_j \ldots \varphi \to (\xi_j \to \xi_i)$.

  Формула $(\varphi \to (\xi_j \to \xi_i)) \to ((\varphi \to \xi_j) \to (\varphi \to \xi_i))$ есть частный случай (D). Тогда, применив modus ponens к нему и последнему правилу предыдущего абзаца получаем $((\varphi \to \xi_j) \to (\varphi \to \xi_i))$. Получаем $(\varphi \to \xi_i)$ (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. $5 \implies 1$, $1 \implies 2$: очевидно.

$2 \implies 3$:

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 вида $\ldots \varphi \ldots \neg\varphi$. Тогда пусть ψ — любая формула, тогда можем записать $(\neg\varphi \to (\varphi \to \psi))$ $(I2)$, $\varphi \to \psi (MP)$, ψ (MP)

$4 \implies 5$: опять очевидно. □

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. $\neg\varphi \to \neg(p \to p)$
2. $(\neg\varphi \to (p \to p)) \to ((p \to p) \to \varphi)$ (N)
3. $(p \to p) \to \varphi$ (MP)
4. $p \to p$
5. φ

□

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

Построим вывод. Гипотеза — $\neg p$, тогда

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

□