Московский физико-технический институт
Физтех-школа прикладной математики и информатики

МАТЕМАТИЧЕСКАЯ ЛОГИКА

I СЕМЕСТР

Лектор: *Даниил Владимирович Мусатов*

h\nu

Автор: *Киселев Николай*
Репозиторий на Github

осень 2024

Содержание

1 Вступление

1.1 Литература

1. Верещагин Н.К., Шень А."Лекции по мат.логике":

   ч.1 Начало теории множеств

   ч.2 Языки и исчисления

   ч.3 Вычислимые функции

Синтаксис (Правила составления ормул) $\longleftrightarrow$ **Семантика** (сопоставление формального выражения некоторому смыслу). Мы начнем с **Семантики**. Из-за лингвистической истории этого вопроса, в каждом формальном языке ест **алфавит**.

2 Алфавит и языки

2.1 Определения

Определение 2.1. Алфавит — множество символов. Мы будем считать, что алфавит непуст и конечен.

Определение 2.2. Слово — конечная последовательность символов алфавита (может быть пустым). Оно состоит из букв (элементов алфавита). Пустое слово обозначается ε

Определение 2.3. Язык — множество слов. Пустой язык $\varnothing$

Определение 2.4. Синглтон — язык, состоящий только из пустого слова. $\{\varepsilon\}$

2.2 Операции

1. Конкатенация $u \cdot v$ — дописываение слова
2. Длина $|u|$ — длина слова
3. Возведение в степень $u^n = \underbrace{uu\dots u}_{n}$
4. Обращение $u^R = u_n u_{n-1} \dots u_1$, если $u = u_1 u_2 \dots u_n$ $(u \cdot v)^R = v^R u^R$

2.3 Отношения

1. Префикс $u \sqsubset v \Leftrightarrow \exists w : uw = v$
2. Суффикс $u \sqsupset v \Leftrightarrow \exists w : wu = v$
3. Подслово $u \subset v$ — вычеркнуть часть букв (сохраняя порядок), получив v из u

2.4 Операции над языками

0. Теоретико-множественные

1. Конкатенация $L \cdot M = \{uv | u \in L, v \in M\}$, причем

   (a) $L \cdot \varnothing = \varnothing \cdot L = \varnothing$

   (b) $L \cdot \{\varepsilon\} = \{\varepsilon\} \cdot L = L$

2. Возведение в степень $L^n = \underbrace{LLL \ldots L}_{n}$, причем $L^0 = \{\varepsilon\}$

3. Итерация (Звезда Клини) $L^* = L^0 \cup L^1 \cup L^2 \ldots$

4. Плюс Клини $L^+ = L^1 \cup L^2 \ldots$. Тогда $L^+ = L^* \cdot L$

Мы будем считать, что натуральные числа начинаются с 0, но во всех местах это на всякий случай будут писать.

Определение 2.5. Правильная скобочная последовательность (ПСП) — последовательность скобок, разбитых на пары, где в каждой паре "(" идет раньше ")".

$$(_1\ (_2\ )_1\ )_2 \text{— тоже правильная}$$

Определение 2.6. Правильная скобочная последовательность (ПСП) — последовательность скобок, индуктивно построенная из правил:

1. ε — ПСП

2. S — ПСП $\Leftrightarrow$ (S) — ПСП

3. S, T — ПСП $\Rightarrow$ $S \cdot T$ — ПСП

Определение 2.7. Баланс СП — #(открывающих скобок) − #(закрывающих скобок)

Определение 2.8. ПСП — такая СП, что ее баланс равен 0, а баланс любого префикса $\geqslant 0$.

Утверждение 2.1. *Все три определения ПСП равносильны*

Доказательство.

1. **Определение 2.5** $\Rightarrow$ **Определение 2.6**. Все скобки разбиты на пары $\Rightarrow$ баланс $= 0$. Более того, в паре "(" идет раньше ")", поэтому в каждом префиксе не может быть только ")" из одной пары. В каждой паре тогда сумма $\geqslant 0 \Rightarrow$ в префиксе сумма $\geqslant 0$.

2. **Определение 2.5** $\Rightarrow$ **Определение 2.8**. Такой алгоритм позволяет явным образом разбить скобки на пары.

3. **Определение 2.8** $\Rightarrow$ **Определение 2.5**. Доказательство: индукция по длине СП.

База: $S = \varepsilon$ — очевидно

Переход: $|S| > 0$. Тогда из **Определения 2.8** следует, что первый символ — "(". Рассмотрим кратчайший непустой префикс с балансом = 0. Если это все слово, то тогда $S = (S')$, т.к. это минимальный префикс, где баланс обратился в 0 (первую скобку надо было чем-то "убить", значит, последняя скобка идет с ней в паре). Тогда утверждение работает и для S' по предположению индукции. Иначе, это какой-то префикс T. Тогда $S = TL$. По предположению индукции, T, L — ПСП, т.к. баланс T равен 0. Значит Ч.Т.Д.

□

Получается, что все три определения эквивалентны.

3 Пропозициональные формулы

Есть знаки логических $\wedge, \vee, \rightarrow, \neg$, действий и скобки.

3.1 Формулы с одной бинарной связкой

Определение 3.1. Правильные алгебраические выражения (ПАВ) — формулы с одной бинарной связкой. Они задаются рекурсивным правилом:

1. p — переменная $\Rightarrow p$ — ПАВ
2. φ, ψ — ПАВы $\Rightarrow (\varphi * \psi)$ — ПАВ

По записи $((a * b) * (c * (d * e)))$ можно однозначно построить дерево.

Теорема 3.1. *ПАВы и деревья разбора взаимно однозначно сопоставляются друг другу. Мы докажем, что для любого ПАВ η не являющегося переменной, существует единственная пара (φ, ψ), такая, что $\eta \doteqdot (\varphi * \psi)$*

Доказательство.

Лемма 3.1 (О балансе скобок)**.** *Баланс любого префикса ПАВ $\geqslant 0$. При этом баланс равен 0 только для ε и всего ПАВ.*

Доказательство. Доказательство по индукции по построению

База: p — переменная — 2 префикса: ε, ПАВ, лемма верна

Переход: пусть для φ, ψ лемма верна. Докажем для $(\varphi * \psi)$. Рассмотрим префиксы: ε, (, потом баланс будет $\geqslant 1$ по предположению индукции (и так как у нас есть одна открывающая скобка) никогда не будет равен 0, только в начале φ и в конце, следовательно, он обнулится только, когда для самой первой скобки найдется пара, то есть в самом конце.

□

Теперь, пусть $A = (\varphi * \psi) \doteqdot (\zeta' * \xi') = B$ Б.О.О. у A звездочка, разделяющая φ, ψ стоит на месте k, а у B — на месте l. Б.О.О $k < l$. Но тогда $a_2a_3a_4 \ldots a_k$ — ПАВ. Но тогда $a_2a_3a_4 \ldots a_k = \varphi \sqsubset \zeta$, но по лемме о балансе у каждого выражения баланс 0 достигается только в начале и в конце. Противоречие, значит $\varphi \doteqdot \zeta$ □

3.2 Пропозициональные формулы

1. p — переменная $\Rightarrow p$ — ПФ
2. φ, ψ — ПФы $\Rightarrow (\varphi \wedge \psi), (\varphi \vee \psi), (\varphi \to \psi),$ — ПФы
3. φ — ПФ $\Rightarrow \neg\varphi$ — ПФ

Лемма 3.2 (О балансе скобок)**.** *Баланс любого префикса ПФ* $\geqslant 0$*. При этом баланс равен 0 только для* ε*, всего ПФ и цепочки отрицаний* $(\neg\neg\neg\ldots\neg)$*.*

Доказательство. Доказательство представляется читателю в качестве несложного упражнения $\square$

3.3 Булевы функции

$f : \{0,1\}^k \to \{0,1\}$ — булева функция от k переменных. Тогда общее число функций $= 2^{2^k}$. Для $k = 1$ общее количесвто функций равно 4.

p	$\bot$	p	$\neg p$	$\top$
0	0	0	1	1
1	0	1	0	1

Для $k = 2$ общее количесвто функций равно 16.

p	q	$\bot$	$\top$	p	q	$\neg p$	$\neg q$	$\wedge$	$\vee$	$\oplus$	$\to$	$\leftarrow$	$\leftrightarrow$	$\not\to$	$\not\leftarrow$	$\downarrow$	$\uparrow$
0	0	0	1	0	0	1	1	0	0	0	1	1	1	0	0	1	1
0	1	0	1	0	1	1	0	0	1	1	1	0	0	0	1	0	1
1	0	0	1	1	0	0	1	0	1	1	0	1	0	1	0	0	1
1	1	0	1	1	1	0	0	1	1	0	1	1	1	0	0	0	0
.	.	.	.	.	.	.	.	min	max	XOR	$\leqslant$	$\geqslant$	$\setminus$	$>$	$<$	NOR	NAND

Для $k > 2$:

1. $\wedge_k, \vee_k, \oplus_k$
2. $maj(p,q,r) = \begin{cases} 1, p+q+r \geqslant 2 \\ 0, p+q+r \leqslant 1 \end{cases}$
3. maj_{2k-1} — аналогично
4. $thr_{k,n} = \begin{cases} 1, p_1 + p_2 + \cdots + p_n \geqslant k \\ 0,\text{иначе} \end{cases}$ — аналоги
5. $p?q : r \begin{cases} q, p = 1 \\ r, q = 0 \end{cases}$ — тернарный оператор

Пропозициональные формулы $\longleftrightarrow$ **Булевы функции**

$\to$ вычисление

$\leftarrow$ представление

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

Строим дерево по нему. Потом значения переменных переносим в дерево

3.4 Правило вычисления значения формулы

Обозначения:

1. $p_1, p_2, \ldots p_n$ — переменные (символы)
2. $a_1, a_2, \ldots a_n$ — их значения
3. $[\varphi](a_1, a_2, \ldots a_n)$ — вычисление значения для аргументов $a_1, a_2, \ldots a_n$.

Определения:

1. $[p_i](a_1, a_2, \ldots a_n) = p_i$ — значение переменной
2. $[\neg\varphi](a_1, a_2, \ldots a_n) = neg([\varphi](a_1, a_2, \ldots a_n))$ — значение переменной. Причем $\neg$ — просто символ, а neg — булева функция.
3. $[\varphi \wedge \psi](a_1, a_2, \ldots a_n) = and([\varphi](a_1, a_2, \ldots a_n), [\psi](a_1, a_2, \ldots a_n))$.
4. $[\varphi \vee \psi](a_1, a_2, \ldots a_n) = or([\varphi](a_1, a_2, \ldots a_n), [\psi](a_1, a_2, \ldots a_n))$.
5. $[\varphi \to \psi](a_1, a_2, \ldots a_n) = implies([\varphi](a_1, a_2, \ldots a_n), [\psi](a_1, a_2, \ldots a_n))$.

Булева функция получается из пропозициональной формулы, если провести вычисления для всех $(a_1, a_2, \ldots a_n)$.

3.5 ДНФ и КНФ

Определение 3.2. Литерал — переменная или отрицательная переменная p или $\neg p$

Определение 3.3. Конъюнкт — конъюнкция литералов $(p \wedge q \wedge \neg r)$

Определение 3.4. Дизъюнкт — конъюнкция литералов $(p \vee q \vee \neg r)$

Определение 3.5. КНФ — конъюнкция дизъюнктов

Определение 3.6. ДНФ — дизъюнкция конъюнктов

Теорема 3.2. *Любая булева функция выражается как КНФ, а также как ДНФ*

Доказательство. Пусть $f(a_1, a_2 \ldots a_n)$ принимает значение 1 на множестве X, а значение 0 на множестве $\overline{X}$ (универсум тут равен $\{0,1\}^n$).

ДНФ: Для каждого $x \in X$ запишем конъюнкт, который на нем выдает истину, например:

$$(0,1,1,0,1) \leftrightarrow (\neg a_1 \wedge a_2 \wedge a_3 \wedge \neg a_4 \wedge a_5)$$

Такая функция выдает ложь на всех остальных элеменах множества $\{0,1\}^n$. Потом делаем конъюнкцию всех таких формул и получаем $f(a_1, a_2, \ldots a_n)$. Получается, что хотя бы 1 (на самом деле ровно 1, т.к. каждая функция зануляется на всех элементах, кроме одного) должна выдать истину, следовательно, она будет принимать истину только на тех значениях, на которых мы захотим.

КНФ: Для каждого $x \in \overline{X}$ запишем дизъюнкт, который на нем выдает 0, например:

$$(0, 1, 1, 0, 1) \leftrightarrow (a_1 \vee \neg a_2 \vee \neg a_3 \vee a_4 \vee \neg a_5)$$

Такая функция выдает истину на всех остальных элеменах множества $\{0, 1\}^n$. Потом делаем дизъюнкцию всех таких формул и получаем $f(a_1, a_2, \dots a_n)$. Получается, что итоговая формула будет иметь такой смысл: "не зануляйся там, где я этого не хочу", и будет принимать 0 только там, где хотя бы одно (на самом деле ровно одно) из наших выражений будет выдавать 0.

□

Определение 3.7. Совершенная ДНФ (КНФ), или СКНФ, СДНФ — это КНФ (ДНФ), где в каждой скобке стоит ровно n переменных.

3.6 Сокращенное ДНФ (КНФ)

Есть две операции:

1. ДНФ $= (A \wedge x) \vee (A \wedge \overline{x}) \vee \cdots \Rightarrow$ приписываем $\vee A$
2. ДНФ $= (A \wedge B) \vee A \Rightarrow$ удаляем $(A \wedge B)$

Определение 3.8. ДНФ(КНФ) с которой нельзя проделать эти две опреации называется сокращенной.

3.6.1 Метод Куайна

Проделываем следующий алгоритм:

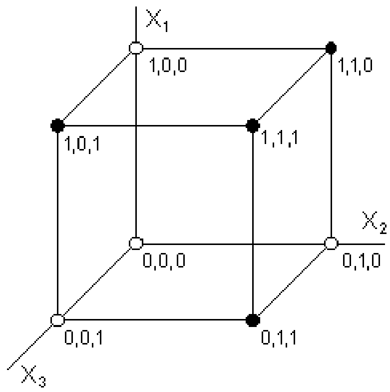
1. Берем СДНФ (СКНФ)
2. Делаем (1), пока можем
3. Делаем (2), пока можем
4. Рисуем таблицу:

	A_1	A_2	$\dots$	A_n
B_1	+	+	$\dots$	
B_2	+		$\dots$	
$\vdots$		+	$\vdots$	+
B_m			$\dots$	+

Нам нужно найти минимальное покрытие всех столбцов строками.

3.6.2 Визуализация еще одного метода

Рисуем куб в n-мерном пространстве, координаты вершины которого лежат в $\{0, 1\}$:



Отмечаем точки, на которых функция принимает 1. Заметим, что любой конъюнкт принимает значение 1 на какой-то гиперграни (грани, ребре или вершине для случая $n = 3$). Поэтому пытаемся найти минималное покрытие такими гипергранями. Так и строим.

3.6.3 Карта Карно

тык

3.7 Многочлены Жегалкина

Вместо $\neg, \vee, \wedge$ используем $\cdot, \oplus$

Замечание. 1. $x^2 = x$

2. $x \oplus x = 0$

Определение 3.9. Пусть даны $x_1, x_2, \ldots x_n$ — переменные. Тогда одночленом жегалкина называется произведение каких то из этих переменных, в том числе 1, как произведение пустого подмножества переменных.

Определение 3.10. Многочленом жегалкина называется сумма каких-то одночленов, в том числе 0, как сумма пустого множества одночленов.

Порядок в произведениях и суммах не важен

1. (a) $\neg p = p \oplus 1$
   (b) $p \wedge q = p \cdot q$
   (c) $p \vee q = p \oplus q \oplus pq$
   (d) $p \to q = \neg p \vee q = (p \oplus 1) \oplus q \oplus (p \oplus 1)q = 1 \oplus p \oplus pq$
   (e) $maj_3(p, q, r) = \begin{cases} 1, p + q + r \geqslant 2 \\ 0, p + q + r \leqslant 1 \end{cases} = pq \oplus qr \oplus rp$

Теорема 3.3. *Любую булеву функцию можно представить, как многочлен Жегалкина (с точностью до перестановки множителей и слагаемых).*

Первое доказательство.

1. Количество булевых функций — 2^{2^n}
2. Количество одночленов жегалкина — 2^n
3. Количество многочленов жегалкина — 2^{2^n}

— итого на каждый многочлен приходится не более одной функции. Докажем, что никакие два многочлена не могут соответствовать одной функции $\Leftrightarrow$ докажем, что у каждой функции есть представление среди многочленов жегалкина. Доказательство: по функции можно сделать КНФ, а по КНФ можно сделать многочлен, т.к. в КНФ участвуют только конъюнкция ($\wedge$), дизъюнкция ($\vee$), отрицание ($\neg$), а их мы умеет получать многочленами жегалкина. $\square$

Второе доказательство. Пусть это не так, тогда есть $p \neq q$, такие, что $\forall x\ p(x) = q(x)$. Рассмотрим $S(x) = q(x) \oplus p(x)$. Тогда $S \neq 0$, но $S(x) = 0\ \forall x$. Рассмотрим одночлен, в котором меньше всего множителей. Б.О.О. это будет $x_1 x_2 x_3 \ldots x_k$. Тогда

$$S(x) = x_1 x_2 \ldots x_k \oplus (\text{в каждом из этих одночленов будет множитель не из } x_1 \ldots x_k)$$

Но тогда, если мы возьмем $x_1, x_2, \ldots, x_k = 1$, а все остальные переменные за 0, то $S(x)$ будет равно 1, т.к. в правой части в каждом из одночленов будет 0. Противоречие. $\square$

Все функции можно выразить через $\neg, \vee, \wedge$ (КНФ/ДНФ). Даже можно только используя $\neg, \wedge$, используя **Законы Де-Моргана**

1. $p \wedge q = \neg(\neg p \vee \neg q)$
2. $p \vee q = \neg(\neg p \wedge \neg q)$

Многочлены жегалкина позволяют выразить все функции через $\wedge, \oplus, 1$. А можно ли выразить все через $\wedge, \vee, \rightarrow$? Нет, т.к. любая формула, использующая их, будет выдавать 1 при входных данных $1, 1, 1, \ldots, 1$

3.8 Классы Поста

3.8.1 Классы P_0, P_1

Определение 3.11. P_0 — класс функций, которые сохраняют 0. (Для которых $f(0, 0, \ldots 0) = 0$)

Определение 3.12. P_1 — класс функций, которые сохраняют 1. (Для которых $f(1, 1, \ldots 1) = 1$)

Определение 3.13. Суперпозиция функций $f, g_1, g_2, \ldots g_k$, где k — количество аргументов — это $h(x_1, x_2, \ldots x_n) = f(g_1(x_1, x_2, \ldots x_n), g_2(x_1, x_2, \ldots x_n), \ldots g_k(x_1, x_2, \ldots x_n))$. Более формально:

1. Суперпозиция 0-порядка — это проекторы $pr_i(x_1, x_2, \ldots, x_n) = x_i$

2. Суперпозиция $(m+1)$-порядка — это где f — одна из базовых функций, а $g_1, g_2, \dots g_n$ — не более m-ого порядка каждая.

Определение 3.14. Пусть C — множество функций. Тогда множество всех суперпозиций функций из C называется замыканием C и обозначается $[C]$.

Теорема 3.4. *Все базовые функции из P_a $\Rightarrow$ все их суперпозиции тоже.*

Доказательство.

$$\underbrace{f(\underbrace{g_1(\underbrace{x_1, x_2, \dots x_n}_{a,a,a\dots a})}_{a}, \underbrace{g_2(\underbrace{x_1, x_2, \dots x_n}_{a,a,a\dots a})}_{a}, \dots \underbrace{g_n(\underbrace{x_1, x_2, \dots x_n}_{a,a,a\dots a})}_{a})}_{a}$$

$\square$

Определение 3.15. Пусть C — множество функций. Тогда множество всех суперпозиций функций из C называется замыканием C и обозначается $[C]$.

3.8.2 Монотонные функции

Определение 3.16. f — монотонная функция, если $\forall (a_1, a_2 \dots a_n)$, $\forall (b_1, b_2 \dots b_n)$ верно следующее: $((a_1 \leqslant b_1) \wedge (a_2 \leqslant b_2) \wedge \dots \wedge (a_n \leqslant b_n)) \Rightarrow f(a_1, a_2 \dots a_n) \leqslant g(a_1, a_2 \dots a_n)$

Теорема 3.5. *Для монотонных функций тоже выполнено, что их суперпозиции монотонны, т.к.*

Доказательство.

$$\underbrace{f(\underbrace{g_1(\underbrace{x_1, x_2, \dots x_n}_{\nearrow,\nearrow,\nearrow\dots\nearrow})}_{\nearrow}, \underbrace{g_2(\underbrace{x_1, x_2, \dots x_n}_{\nearrow,\nearrow,\nearrow\dots\nearrow})}_{\nearrow}, \dots \underbrace{g_n(\underbrace{x_1, x_2, \dots x_n}_{\nearrow,\nearrow,\nearrow\dots\nearrow})}_{\nearrow})}_{\nearrow}$$

$\square$

3.8.3 Самодвойственные функции

Определение 3.17. Функция f^* (двойственная к f) — это такая функция, что

$$\neg f(\neg p_1, \neg p_2, \dots, \neg p_n) = f^*(p_1, p_2, \dots p_n)$$

Пример.

1. $\wedge^* = \vee$
2. $\vee^* = \wedge$
3. $\oplus^* = \leftrightarrow$

Определение 3.18. Самодвойственные функции — это такие, которые двойственны сами себе.

3.8.4 Линейные функции

Определение 3.19. Линейные функции — это те, которые задаются линейными многочленами жегалкина.

3.8.5 Критерий Поста

Определение 3.20. Полная система связок — это такая, в которой все функции можно выразить.

Пример.

$$\{\neg, \wedge, \vee, \rightarrow\}, \{\neg, \vee\}, \{\neg, \wedge\}, \{\rightarrow, 0\}, \{1, \oplus, \wedge\}$$

Итак, вспомним, какие у нас уже были системы:

1. P_0 — $\{\wedge, \vee, \rightarrow\}$ — сохраняют 1
2. P_1 — $\{\wedge, \oplus\}$ — сохраняют 0
3. M — $\{\wedge, \vee, 0, 1\}$ — монотонные
4. D — $\{\neg, maj\}$ — все самодвойственные (без доказательства)
5. L — $\{\neg, \oplus\}$ — все линейные (без доказательства)

Теорема 3.6 (Критерий Поста)**.** *Система связок полна* $\Leftrightarrow$ *она не является подмножеством ни одного из 5 классов* $\Leftrightarrow$ *система содержит некие функции* $f_0 \notin P_0$, $f_1 \notin P_1$, $g \notin M$, $h \notin D$, $k \notin L$,

Доказательство. Создадим полную систему связок пошагово:

1. $f_0(0, 0, \ldots 0) = 1$, т.к. f_0 не сохраняет 1.
   (a) $f_0(1, 1, \ldots, 1) = 1 \Rightarrow f_0 \sim 1$
   (b) $f_0(1, 1, \ldots, 1) = 0 \Rightarrow f_0(p, p, \ldots p) = \neg p$
2. $f_1(1, 1, \ldots 0) = 0$, т.к. f_1 не сохраняет 1.
   (a) $f_1(0, 0, \ldots, 0) = 0 \Rightarrow f_1 \sim 0$
   (b) $f_1(0, 0, \ldots, 0) = 1 \Rightarrow f_1(p, p, \ldots p) = \neg p$

   Итого есть 4 варианта. Если мы нашли $\neg$ и константу (0 или 1), то вторую из них можно получить при помощи $\neg$ и перейти к 5 шагу. Если мы получили только $\neg$, то переходим к шагу 4, иначе к шагу 3.
3. $0, 1, g \notin M$ — получим $\neg$.

   Лемма 3.3. *Если g не монотонна, то $\exists i \exists (a_1 \ldots a_n)$, такие, что*

$$g(a_1, a_2 \ldots a_{i-1}, 0, a_{i+1}, \ldots, a_n) = 1 \wedge$$

$$g(a_1, a_2 \ldots a_{i-1}, 1, a_{i+1}, \ldots, a_n) = 0$$

Доказательство. По определению. □

Тогда мы нашли отрицание, т.к. $g(a_1, a_2 \dots a_{i-1}, p, a_{i+1}, \dots, a_n) = \neg p$

4. $\neg, h \notin D$ — получим $0, 1$. Так как $h \notin D \Leftrightarrow \exists (a_1, a_2, \dots, a_n)$:

$$h(a_1, a_2, \dots, a_n) = h(\neg a_1, \neg a_2, \dots \neg a_n)$$

Тогда рассмотрим такую функцию от p: $h(p, \neg p, \dots, \neg p)$, где на месте нулей в наборе a_i стоят $\neg p$, а на месте единиц стоят p. Пример: $h(1, 0, 0, 1, 0, 1, 1, 0) = h(0, 1, 1, 0, 1, 0, 0, 1)$, тогда рассматриваем $h(p, \neg p, \neg p, p, \neg p, p, p, \neg p)$. Тогда

$$h(p, \neg p, \dots, p, \neg p) = h(\neg p, p, \dots, \neg p, p)$$

И тогда $h(p, \neg p, \dots, p, \neg p)$ — некая константа. Тогда можно получить и вторую константу.

5. $0, 1, \neg, k \notin L$ — получим все. Из определения L следует (Б.О.О. переменные имеют индексы x_1, x_2):

$$k(x_1, x_2, \dots x_n) = x_1 x_2 A(x_3, \dots, x_n) + x_1 B(x_3, \dots, x_n) + x_2 C(x_3, \dots, x_n) + D(x_3, \dots, x_n)$$

И многочлен A — непустой. Но тогда $\exists (a_3, \dots a_n) : A(a_3 \dots a_n) = 1$. Тогда $k(x_1, x_2, a_3, \dots a_n) = x_1 x_2 + b x_1 + c x_2 + d$ Использование отрицания позволяет менять 1. Тогда нужно рассмотреть 3 случая.

   (a) $b = c = 0$ Тогда получили $x_1 x_2$ и выразили, таким образом, $x_1 \wedge x_2$.
   (b) $b = c = 1$ Тогда получили $x_1 x_2 + x_1 + x_2$ и выразили, таким образом, $x_1 \vee x_2$.
   (c) $b = 1, c = 0$ Тогда получили $x_1 x_2 + x_2 + 1$, и выразили, таким образом, $\to$.

Все три операции вместе с $0, 1, \neg$ позволяют составить полную систему связок.

□

3.9 Типы пропозициональных формул

Определение 3.21. Тавтология — всегда истинная формула

Определение 3.22. Противореиче — всегда ложная формула

Определение 3.23. Опровержимая формула — не противоречие

Определение 3.24. Выполнимая формула — не тавтология

3.10 Важные тавтологии (логические законы)

1. Закон непротиворечия $\neg(A \wedge \neg A)$

2. Закон двойного отрицания $A \leftrightarrow \neg\neg A$

3. Закон исключенного третьего $A \vee \neg A$

   Теорема 3.7 (Пример неконструктивного доказательства). *Существуют* $\alpha, \beta \in \mathbb{R} \setminus \mathbb{Q} : \alpha^\beta \in \mathbb{Q}$

   Доказательство.

$$\left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = 2$$

   Тогда либо $\sqrt{2}^{\sqrt{2}} = x$ — иррациональное число, и тогда $x^{\sqrt{2}}$ удовлетворяет условию, иначе $\sqrt{2}^{\sqrt{2}}$ подходит. □

4. Контрпозиция $(A \to B) \leftrightarrow (\neg B \to \neg A)$

5. Законы де Моргана

   (a) $\neg(A \wedge B) \leftrightarrow (\neg A \vee \neg B)$

   (b) $\neg(A \vee B) \leftrightarrow (\neg A \wedge \neg B)$

4 Задача о выполнимости условий

Даны несколько формул, спрашивается, могут ли они одновременно быть истинными?

$$\varphi_1 \wedge \varphi_2 \wedge \cdots \wedge \varphi_n$$

4.1 Пример превращения математической задачи в задачу о выполнимаости

4.2 Задача о четырех красках

У нее была очень долгая история, когда ее решали о опровергали, но в итоге в 1976г. Эту задачу решили при помощи перебора. Переформулируем в терминах выполнимости условий. Вершинам планарного графа сопоставим 2 бита (p, q) (цвет). Таким образом, если u, v — различные области на карте, то нужно, чтобы $(p_v \neq p_u) \vee (q_v \neq q_u)$.

5 Исчисление высказываний

Определение 5.1. Логический вывод — это последовательность формул, в которой каждая формула либо является аксиомой, либо получается из более ранних по одному из правил вывода.

Все теории отличаются аксиомами и правилами вывода. Обычно, когда нам в школе рассказывали аксиомы плоскости или, не дай бог, пространства, мы рассматривали сами аксиомы, но не способы их вывода. Итак, постараемся отвлечься от смысла, будем лишь наблюдать за синтаксисом. Идея такая: для того, чтобы формализовать математику, нам нужен четкий список правил, по которым она работает (тавтологий). Т.к. доказательство это, буквально, текст, мы сейчас будем работать исключительно с синтаксисом, но не семантикой. Проще говоря, мы хотим научиться получать все возможные тавтологии, причем конечным набором правил. Один из таких наборов правил приведен ниже:

5.1 Схемы аксиом

1. $A \to (B \to A)$
2. $(A \to (B \to C)) \to ((A \to B) \to (A \to C))$
3. $(A \wedge B) \to A$
4. $(A \wedge B) \to B$
5. $A \to (B \to (A \wedge B))$
6. $A \to (A \vee B)$
7. $B \to (A \vee B)$
8. $(A \to C) \to ((B \to C) \to ((A \vee B) \to C))$ — разбор случаев
9. $\neg A \to (A \to B)$
10. $(A \to B) \to ((A \to \neg B) \to \neg A)$ — рассуждение от противного.
11. $A \vee \neg A$

5.2 Правило Вывода

Определение 5.2. Modus Ponens —

$$\frac{A, A \to B}{B}$$

5.3 Обозначения

1. $\vdash A$ — A — выводима
2. $\models A$ — A — тавтология

5.4 Примеры вывода

Пример.

$$\vdash (A \vee B) \to (B \vee A)$$

1. $A \to (B \vee A)$
2. $B \to (B \vee A)$
3. $(A \to (B \vee A)) \to ((B \to (B \vee A)) \to ((A \vee B) \to (B \vee A)))$
4. $(B \to (B \vee A)) \to ((A \vee B) \to (B \vee A))$
5. $(A \vee B) \to (B \vee A)$

Пример.

$$\vdash (A \to A)$$

1. $A \to ((A \to A) \to A)$
2. $(A \to ((A \to A) \to A)) \to ((A \to (A \to A)) \to (A \to A))$
3. $(A \to (A \to A)) \to (A \to A)$
4. $A \to (A \to A)$
5. $A \to A$

Теорема 5.1. *A — выводима $\Rightarrow$ A — тавтология*

Доказательство. Аксиомы — тавтологии.

$$\left.\begin{array}{r} A \text{ — тавтология} \\ A \to B \text{ — тавтология} \end{array}\right\} \Rightarrow B \text{ — тавтология}$$

□

Теорема 5.2 (О полноте). *Правда ли, что A — тавтология $\Rightarrow$ A — выводима?*

Доказательство. Доказательство будет дальше □

5.5 Дополнительные правила вывода

Определение 5.3. Вывод из множества посылок Γ — это последовательноть $\varphi_1, \varphi_2 \ldots, \varphi_n$, где φ_i — либо аксиома, либо $\in \Gamma$, либо получается по m.p.

5.5.1 Лемма о Дедукции

Лемма 5.1 (О дедукции)**.** $\Gamma \vdash (A \to B) \Leftrightarrow \Gamma \cup \{A\} \vdash B$

Доказательство.

$\Rightarrow$

$$\left.\begin{array}{l} \left.\begin{array}{c} \dots \\ \dots \\ \dots \\ A \to B \end{array}\right\} \text{вывод } A \to B \text{ из } \Gamma \\ A \text{ — элемент } \Gamma \cup \{A\} \text{ (посылка)} \\ B \text{ — m.p.} \end{array}\right\} \text{вывод } B \text{ из } \Gamma \cup \{A\}$$

$\Leftarrow$ Пусть $\Gamma \cup \{A\} \vdash B$. Тогда существует вывод $\varphi_1, \varphi_2, \dots \varphi_n = B$. Каждое φ_i — либо аксиома, либо $\in \Gamma$, либо $= A$, либо выводится по m.p. Мы докажем по индукции, что $\Gamma \vdash A \to \varphi_i$.

(a) φ_i — аксиома. Вывод:

i. φ_i

ii. $\varphi_i \to (A \to \varphi_i)$ — аксиома 1.

iii. $A \to \varphi_i$ — m.p.

(b) $\varphi_i \in \Gamma$ — аналогично

(c) $\varphi_i = A$. На прошлой лекции мы выводили $A \to A$.

(d) φ_i по m.p.: $\exists j, k < i : \varphi_k = (\varphi_j \to \varphi_i)$. По предположению индукции,

$$\left.\begin{array}{c} \left.\begin{array}{c} \dots \\ \dots \\ \dots \\ A \to \varphi_j \end{array}\right\} \text{вывод из } \Gamma \\ \dots \\ \dots \\ A \to (\varphi_j \to \varphi_i) \text{ — m.p.} \end{array}\right\} \text{вывод из } \Gamma$$

$$\Rightarrow (A \to (\varphi_j \to \varphi_i)) \to ((A \to \varphi_j) \to (A \to \varphi_i)) \text{ — аксиома 2}$$

$$\Rightarrow (A \to \varphi_j) \to (A \to \varphi_i) \text{ — m.p.}$$

$$\Rightarrow A \to \varphi_i \text{ — m.p.}$$

□

Пример (Силлогизм)**.**

$$\begin{array}{c} (A \to B) \to ((B \to C) \to (A \to C)) \\ \{A \to B\} \vdash (B \to C) \to (A \to C) \\ \{A \to B, B \to C\} \vdash (A \to C) \\ \{A, A \to B, B \to C\} \vdash C \end{array}$$

Тогда вывод последней формулы можно провести следующим образом:

1. A — посылка
2. $A \to B$ — посылка
3. B — m.p. 1, 2
4. $B \to C$ — посылка
5. C — m.p 3, 4

Пример. $\vdash (A \wedge B) \to (B \wedge A) \Leftrightarrow (A \wedge B) \vdash (B \wedge A)$‘

1. $(A \wedge B)$ — посылка
2. $(A \wedge B) \to B$ — аксиома 4
3. B — m.p. 1, 2
4. $(A \wedge B) \to A$ — аксиома 3
5. A — m.p. 1, 4
6. $B \to (A \to (B \wedge A))$ — аксиома 5
7. $A \to (B \wedge A)$ — m.p. 3, 6
8. $(B \wedge A)$ — m.p. 5, 7

Пример. $\vdash (A \to \neg A) \to \neg A$

1..5. $A \to A$

6. $(A \to A) \to ((A \to \neg A) \to \neg A)$ — аксиома 10
7. $(A \to \neg A) \to \neg A$ — m.p. 5, 6

5.5.2 Рассуждение от противного

$$\frac{\Gamma, A \vdash B \quad\quad \Gamma, A \vdash \neg B}{\Gamma \vdash \neg A}$$

Доказательство.

$$\left.\begin{array}{l}\Gamma, A \vdash B \Leftrightarrow \Gamma \vdash A \to B \\ \Gamma, A \vdash \neg B \Leftrightarrow \Gamma \vdash A \to \neg B\end{array}\right\} \Rightarrow \Gamma \vdash \neg A (\text{аксиома } 10)$$

□

5.5.3 Законы де Моргана

я снова умер(

Короче, мы вывели дофига разных законов и порассуждали, зачем они нужны, как их использовать и тд.

5.5.4 Правило сечения

$$\frac{\Gamma \vdash A \qquad \Delta, A \vdash B}{\Gamma, \Delta \vdash B}$$

5.5.5 Введение/разбиение конъюнкции

$$\frac{\Gamma, A \wedge B \vdash C}{\Gamma, A, B \vdash C}$$

$$\frac{\Gamma, A, B \vdash C}{\Gamma, A \wedge B \vdash C}$$

$$\frac{\Gamma, \vdash A \wedge B}{\Gamma \vdash A \qquad \Gamma \vdash B}$$

$$\frac{\Gamma \vdash A \qquad \Gamma \vdash B}{\Gamma, \vdash A \wedge B}$$

5.5.6 Разбор случаев

$$\frac{\Gamma, A \vdash C \qquad \Gamma, B \vdash C}{\Gamma, A \vee B \vdash C}$$

5.5.7 Правила без названия

$$\frac{\Gamma \vdash A}{\Gamma \vdash A \vee B}$$
$$\frac{\Gamma \vdash B}{\Gamma \vdash A \vee B}$$

5.5.8 Правило контрпозиции

$$\frac{\Gamma, A \vdash B}{\Gamma, \neg B \vdash \neg A}$$

6 Теорема о полноте

Теорема 6.1 (О полноте). *Если φ — тавтология, то тогда она выводима.*

6.1 Первое доказательство

Определение 6.1. Обозначим $p^\varepsilon = \begin{cases} p, \varepsilon = 1 \\ \neg p, \varepsilon = 0 \end{cases}$

Лемма 6.1 (Базовая Лемма)**.**

1. $A, B \vdash A \wedge B$
2. $\neg A, B \vdash \neg(A \wedge B)$
3. $A, \neg B \vdash \neg(A \wedge B)$
4. $\neg A, \neg B \vdash \neg(A \wedge B)$
5. $A, B \vdash A \vee B$
6. $\neg A, B \vdash A \vee B$
7. $A, \neg B \vdash A \vee B$
8. $\neg A, \neg B \vdash \neg(A \vee B)$
9. $A, B \vdash A \to B$
10. $\neg A, B \vdash A \to B$
11. $A, \neg B \vdash \neg(A \to B)$
12. $\neg A, \neg B \vdash A \to B$
13. $\neg A \vdash \neg A$
14. $A \vdash \neg(\neg A)$

Лемма 6.2 (Основная Лемма)**.** *Пусть* φ *— формула от* n *переменных* $p_1, p_2, \dots p_n$, $(a_1, a_2, \dots a_n) \in \{0,1\}^n, \varphi(a_1, a_2, \dots a_n) = a \in \{0,1\}$. *Тогда* $p_1^{a_1}, p_2^{a_2}, \dots p_n^{a_n} \vdash \varphi^a$.

Доказательство. Индукция по построению формулы.

> **База:** переменная. $p_i^{a_i} \vdash p_i^{a_i}$.
>
> **Переход:** пусть, например, $\varphi = (\xi \wedge \nu)$. $\xi(a_1, a_2, \dots a_n) = a, \nu(a_1, a_2, \dots a_n) = b \Rightarrow \varphi(a_1, a_2, \dots a_n) = ab$. По базовой лемме, $p_1^{a_1}, p_2^{a_2}, \dots p_n^{a_n} \vdash \xi^a, p_1^{a_1}, p_2^{a_2}, \dots p_n^{a_n} \vdash \nu^b$. По базовой лемме, $\xi^a, \nu^b \vdash \varphi^{ab}$. Запишем три вывода подряд, получим желаемое

$\square$

Тогда если φ — тавтология, то при всех $(a_1, \dots a_n) : \varphi(a_1, a_2, \dots a_n) = 1$, тогда по правилу исчерпывающего разбора случаев, формула φ будет выводима, т.к. вне зависимости от любой переменной, φ будет истинна.

6.2 Второе доказательство

Пусть Γ — множество пропозициональных формул. Тогда:

Определение 6.2. Γ — совместно, если при некоторых значениях переменных, все формулы из Γ истинны.

Определение 6.3. Γ — противоречиво, если из нее можно вывести $\psi, \neg\psi$ одновременно для некоторого ψ.

Определение 6.4. Γ — полное, если для любого φ верно $\Gamma \vdash \varphi$ или $\Gamma \vdash \neg\varphi$.

Теорема 6.2. Γ *совместна* $\Leftrightarrow \Gamma$ *непротиворечива.*

Доказательство.

1. Γ — противоречива, тогда она совместна. Если Γ совместна, то все формулы из Γ верны на некотором наборе. Тогда если $\Gamma \vdash \varphi$, то и φ — тоже верна на этом наборе. Аналогично и для $\neg\varphi$. Но формулы $\varphi, \neg\varphi$ не могут быть одновременно истинны, тогда они не могут одновременно выводиться из Γ.

2. Γ — несовместна, тогда она противоречива. Пусть Δ непротиворечива.

   Лемма 6.3. Γ *непротиворечива* $\Rightarrow \Gamma \subset \Delta$ *для некоторого полного непротиворечивого* Δ.

   для счетного множества переменных. Если переменных счетное число, то и формул тоже счетное число. Пусть $\varphi_1, \varphi_2, \ldots$ — все формулы. Определим Γ_i по индукции:

   $$\Gamma_0 = \Gamma, \Gamma_i = \begin{cases} \Gamma_{i-1} \cup \{\varphi_i\}, \text{ если это непротиворечиво} \\ \Gamma_{i-1} \cup \{\neg\varphi_i\}, \text{ иначе} \end{cases}$$

   Заметим, что все Γ_i — непротиворечивы, т.к.

   $$\left.\begin{array}{l} \Gamma_{i-1} \cup \{\varphi_i\} \text{ — противоречиво } \Rightarrow \Gamma_{i-1} \vdash \neg\varphi_i \\ \Gamma_{i-1} \cup \{\neg\varphi_i\} \text{ — противоречиво } \Rightarrow \Gamma_{i-1} \vdash \varphi_i \end{array}\right\} \Rightarrow \Gamma_{i-1} \text{ — противоречиво}$$

   Тогда

   $$\Delta = \bigcup_{i=0}^{\infty} \Gamma_i$$

   — тоже непротиворечиво, т.к. в противном случае, вывод, при помощи котрого мы получили противоречие использует конечное число формул, но тогда он вывелся из какого-то конечного подмножества, но такого не может быть, т.к. все конечные подмножества непротиворечивы. $\square$

   Лемма 6.4. Δ — *полное и непротиворечивое, тогда оно совместное*

   Доказательство. Δ полное, тогда для переменной p_i верно $\Delta \vdash p_i$ или $\Delta \vdash \neg p_i$. Рассмотрим следующий набор значений:

   $$a_i = \begin{cases} 1, \Delta \vdash p_i \\ 0, \Delta \vdash \neg p_i \end{cases}$$

   $\square$

$\square$

Теоремы о полноте.

Корректность $\vdash \varphi \Rightarrow \{\neg\varphi\}$ — противоречиво $\Rightarrow$ несовместно $\Rightarrow \forall a \neg\varphi(a) = 0 \Rightarrow \forall\varphi(a) = 1 \Rightarrow \varphi$ — тавтология

Полнота φ — тавтология $\Rightarrow \{\neg\varphi\}$ несовместна $\Rightarrow \{\neg\varphi\}$ — противоречиво, тогда, т.к. $\frac{\neg\varphi\vdash B \quad \neg\varphi\vdash B}{\vdash\neg(\neg\varphi)} \Rightarrow \vdash \varphi$

$\square$

$$\text{Формулы} \begin{cases} \text{выполнимые} \\ \text{опровержимые} \end{cases}$$

Мы хотим выразить различные задачи в терминах выполнимости формул.

7 Решение задач сведением к выполнимости формулы

7.1 Задача про раскраску графа

Дан граф $G = (V, E)$. Необходимо найти функцию $f : V \to \{1, 2, 3\} : (u, v) \in E \Rightarrow col(u) \neq col(v)$.

Цвет вершины u $\mapsto$	(p_u, q_u)
Не существует	00
1	01
2	10
3	11

Тогда $\forall p_u, q_u(p_u \vee q_u)$ и ребро может быть проведено между вершинами(u, v), если $(p_u \neq p_v) \vee (q_u \neq q_v)$. Итоговая формула — конъюнкция условий, и, если она выполнима, то задача имеет решение.

7.2 Задача про расстановку ферзей

Доска $n \times n, p_{ij}$ — истинна, если на (i, j)-ой клетке стоит ферзь. Тогда можно записать в терминах p_{ij} утверждение "ни один ферзь не бьет никакого другого". Это делается так:

1. $(p_{i1} \vee p_{i2} \vee p_{i3} \vee \cdots \vee p_{in})$ — на k-ой горизонтали стоит хотя бы один ферзь.
2. $(\neg p_{ij} \vee \neg p_{ik})$ — на i-ой горизонтали стоит хотя не более одного ферзя.
3. $(\neg p_{ik} \vee \neg p_{jk})$ — на i-ой вертикали стоит хотя не более одного ферзя.
4. $(\neg p_{ij} \vee \neg p_{i+k,j+k})$ — ферзи не бьют друг друга по направлению главной диагонали.
5. $(\neg p_{ij} \vee \neg p_{i-k,j+k})$ — ферзи не бьют друг друга по направлению побочной диагонали.

7.3 Задача о клике

Дан граф $G, q_{uv} = 1 \Leftrightarrow (u,v) \in E$. Требуется понять, существует ли клика из k вершин?

$$\bigvee_{(v_1,v_2,\ldots v_k)} \bigwedge_{i\neq j} q_{v_i v_j} \text{ — длина} \sim C_n^k$$

Тогда в общей формуле будет порядка

$$\frac{n!}{k!(n-k)!} > \frac{(n-k)^k}{k!} > \left(\frac{n-k}{k}\right)^k$$

множителей, что очень много. Попробуем по-другому записать условие задачи: введем переменные p_{iu} — ”вершина u является i-ой в клике”, $i \in \{1,\ldots k\}$. Тогда накладываются следующие условия:

1. $(p_{i1} \vee p_{i2} \vee \cdots \vee p_{in})$.
2. $i \neq j \Rightarrow (\neg p_{iv} \vee \neg p_{jv})$ — у одной вершины не может быть двух номеров.
3. $(u,v) \in E \Rightarrow (\neg p_{iu} \vee \neg p_{jv})$ — внутри клики все вершины соединены.

7.4 Правило резолюции

$$\frac{A \vee x \quad B \vee \neg x}{A \vee B}$$

$A \vee B$ называется резольвентой

7.4.1 Пустой дизъюнкт $\perp$

$$\frac{x \quad \neg x}{\perp}$$

$$\frac{x \vee y \quad \neg x \vee \neg y}{y \vee \neg y}$$

Пусть дана КНФ, будем рассматривать ее как набор дизъюнктов.

Утверждение 7.1. *Если на данном наборе выполняется $A \vee x, B \vee \neg x$, то и выполняется $A \vee B$.*

Следствие если исходная формула выполнима, то и все ее резольветны тоже.

7.5 Метод резолюций

Строим все новые резольвенты, пока не выведем $\perp$ или не прекратится появление новых дизъюнктов.

Теорема 7.1 (О корректности метода резолюций)**.** *Если исходная формула выполнима, то нельзя вывести $\perp$.*

Доказательство. Если можно вывести $\perp$, то он будет истинный но он $\equiv 0$. □

Теорема 7.2 (О полноте)**.** *Если нельзя вывести $\perp$, то формула выполнима*

Доказательство. Разобьем все дизъюнкты на классы. C_i — дизъюнкты, зависящие только от переменных $p_1, p_2, \dots p_i$. $C_0 = \varnothing$, т.к. $C_0 \subset \{\perp\}$. Будем доказывать по индукции, что выполнены все дизъюнкты из C_i.

База: C_0, все дизъюнкты выполнены.

Переход: Пусть все формулы из C_{i-1} выполнены на значениях $a_1, a_2 \dots a_{i-1}$. Рассмотрим формулы из C_i, которые не будут выполнены на этом наборе. Предположим, что среди них есть и формула с p_i и формула с $\neg p_i$: $p_i \vee D_0, \neg p_i \vee D_1$. Тогда $D_0(p_1, p_2, \dots p_i) = 0 = D_1(p_1, p_2, \dots p_i)$. Но $D_0 \vee D_1$ получается как резольвента этих двух формул, тогда она выполнима, т.к. лежит в C_{i-1}, противоречие. Тогда все формулы либо с p_i, либо с $\neg p_i$, тогда положим p_i так, чтобы этот множитель выполнялся.

□

7.5.1 Использование резолюций для проверки тавтологий

φ — тавтология $\Leftrightarrow$ $\neg\varphi$ — противоречие $\Leftrightarrow$ $\neg\varphi$ — не выполнима. φ — тавтология $\Leftrightarrow$ из некоторой задачи о выполнимости КНФ, построенной по $\neg\varphi$ можно вывести $\perp$.

7.5.2 Преобразование Цейтина

Пример. $(p \wedge q) \vee (r \to \neg s)$. Запишем:

$$\begin{array}{ccc} u = p \wedge q & \mapsto & (\neg u \vee p) \wedge (\neg u \vee q) \wedge (u \vee \neg p \vee \neg q) \\ t = \neg s & \mapsto & (\neg t \vee \neg s) \wedge (t \vee s) \\ v = r \to t & \mapsto & (r \vee v) \wedge (\neg t \vee v) \wedge (\neg v \vee \neg r \vee t) \\ w = u \vee v & \mapsto & (\neg u \vee w) \wedge (\neg v \vee w) \wedge (\neg w \vee u \vee v) \end{array}$$

Все формулы могут быть одновременно верны $\Rightarrow$ φ — не тавтология. Это равносильно получению 3-КНФ из всех этих формул (в каждой скобке $\leqslant 3$ литералов). На 2-КНФ метод резолюций работает за $O(n)$, но на 3-КНФ уже за экспоненциально долгое время. Хотелось бы придумать алгоритм, который работает быстрее. Эта проблема, также известная как проблема P vs NP на данный момент на имеет решения

8 Языки первого порядка

8.1 Алфавит

1. Индивидные переменные $x, y, z, \dots$

2. Функциональные символы (с указанием числа аргументов (например, ”−” может быть и бинарным, и унарным)) $f^{(1)}, g^{(2)}, \dots$, в том числе константные символы (функциональные символы валентности 0) $0, e, \pi, \dots$

3. Предикатные символы (с указанием валентности) $P^{(1)}, Q^{(3)}, \dots$

4. $\neg, \wedge, \vee, \to$

5. Кванторы $\forall, \exists$

6. Служебные символы "(", ",", ")"

Символы из пунктов 2, 3 называются сигнатурами

8.2 Термы

1. x — переменная, тогда x — терм

2. c — константный символ, то c — терм

3. $t_1, t_2, \dots t_k$ — термы, f — функциональный символ валентности k, то $f(t_1, t_2, \dots t_k)$ — терм.

8.3 Формулы

Формулы — это не термы, нумерация сквозная, чтобы у каждого правила был свой номер!!!

6. $t_1, t_2, \dots t_k$ — термы, P — предикатный символ валентности k, то $P(t_1, t_2, \dots t_k)$ — формула

7. φ — формула, тогда $\neg\varphi$ — формула

8. φ, ψ — формулы тогда $(\varphi * \psi)$, где "$*$" — это одна из бинарных логических связок, тоже формула.

9. φ — формулы тогда $\exists x\varphi, \forall x\varphi$ — тоже формула.

Тогда нам не запрещены записи вида $\exists x\forall xP(x)$ или $\exists xP(y)$. Часто добавляют отдельный вид атомарных формул с равенством $t_1 = t_2$. Но при таком определении появляются вопросы, например:

$$\exists x x < y$$

Что такое y? Что такое "$<$"? Откуда берем x?

8.4 Интерпретация

M — непустое множество — носитель интерпретации.

1. f — функциональный символ валентности $k > 0$. $[f] : M^k \to M$.

2. c — константный символ, тогда $[c] \in M$.

3. P — предикатный символ валентности k, тогда $[P] : M^k \to \{0, 1\}$.

Также, пусть Var — множество переменных. Оценкой называется произвольная функция $\pi : Var \to M$. Тогда, если заданы носитель интерпретации и оценка, то определены значения всех термов и формул.

Доказательство.

1. $t \eqcirc x \Rightarrow [t](\pi) = \pi(x)$
2. $t \eqcirc C \Rightarrow [t](\pi) = [C]$
3. $t \eqcirc f(t_1, t_2, \dots t_k) \Rightarrow [t](\pi) = [f]([t_1](\pi), [t_2](\pi), \dots [t_k](\pi))$
4. $\varphi \eqcirc P(t_1, t_2, \dots t_k) \Rightarrow [t](\pi) = [P]([t_1](\pi), [t_2](\pi), \dots [t_k](\pi))$
5. $\varphi \eqcirc \neg \Rightarrow \psi[\varphi](\pi) = neg([\psi](\pi))$
6. Для бинарных связок все как и в ПФах.
7. Обсудим потом

$\square$

... см. предыдущую лекцию

7. $\varphi = \exists x\, \psi$. Тогда
$$[\varphi](\pi) = 1 \Leftrightarrow \text{ найдется } a \in M : [\psi](\pi_{x \mapsto a}) = 1$$
$$\pi_{x \mapsto a}(y) = \begin{cases} \pi(y), y \neq x \\ a, y = x \end{cases}$$
Но тогда
$$[\varphi](\pi) = \bigvee_{a \in M} [\psi](\pi_{x \mapsto a})$$
8. $\varphi = \forall x\, \psi$. Тогда
$$[\varphi](\pi) = \bigwedge_{a \in M} [\psi](\pi_{x \mapsto a})$$

8.4.1 Параметры

Определение 8.1. Параметры терма t ($Par(t)$), это множество, которое задается рекурсивно:

1. $t = x \in Var \Rightarrow Par(t) = x$
2. $t = c^{(0)} \Rightarrow Par(t) = \varnothing$
3. $t = f(t_1, t_2, \dots t_n) \Rightarrow Par(t) = \bigcup_{i=1}^{n} Par(t_i)$

Определение 8.2. Параметры формулы t ($Par(t)$), это множество переменных, которое задается рекурсивно:

1. $\varphi = P(t_1, t_2, \dots t_n) \Rightarrow Par(\varphi) = \bigcup_{i=1}^{n} Par(t_i)$.
2. $\varphi = \neg\psi \Rightarrow Par(\varphi) = Par(\psi)$.
3. $\varphi = \psi * \xi \Rightarrow Par(\varphi) = Par(\psi) \cup Par(\xi)$
4. $\varphi = \exists x \psi \Rightarrow Par(\varphi) = Par(\psi) \setminus \{x\}$.
5. $\varphi = \forall x \psi \Rightarrow Par(\varphi) = Par(\psi) \setminus \{x\}$.

Теорема 8.1.

1. *Если* π, π' — *оценки и для любой переменной* $x \in Par(t), \pi(x) = \pi'(x)$, *то* $[t](\pi) = [t](\pi')$

2. *Если* π, π' — *оценки и для любой переменной* $x \in Par(t), \pi(x) = \pi'(x)$, *то* $[\varphi](\pi) = [\varphi](\pi')$

Доказательство.

1. Ведем индукцию по построению терма t

   (a) $t = x \Rightarrow [t](\pi) = \pi(x) = \pi'(x) = [t](\pi')$

   (b) $t = c \Rightarrow [t](\pi) = [c] = [t](\pi')$

   (c) $t = f(t_1, t_2, \ldots t_n) \Rightarrow [t](\pi) = [f]([t_1](\pi), [t_2](\pi), \ldots [t_n](\pi)) = [f]([t_1](\pi'), [t_2](\pi'), \ldots [t_n](\pi'))$

2. Ведем индукцию по построению формулы f

   (a) $\varphi = P(t_1, t_2, \ldots t_n) \Rightarrow [\varphi](\pi) = [P]([t_1](\pi), [t_2](\pi), \ldots [t_n](\pi)) = [P]([t_1](\pi'), [t_2](\pi'), \ldots [t_n](\pi'))$

   (b) $\varphi = \psi * \xi \Rightarrow [\varphi](\pi) = *([\psi](\pi), [\xi](\pi)) = *([\psi](\pi'), [\xi](\pi')) = [\varphi](\pi')$

   (c) $\varphi = \exists x \psi$.
   $$[\varphi](\pi) = \bigvee_{a \in M} [\psi](\pi_{x \mapsto a}) = \bigvee_{a \in M} [\psi](\pi'_{x \mapsto a}) = [\varphi](\pi')$$

   (d) $\varphi = \forall x \psi$.

□

8.4.2 Типы формул

Определение 8.3. Формула φ называется замкнутой (или предположением), если $Par(\varphi) = \varnothing$. Тогда пишут просто $[\varphi]$, причем, если $[\varphi] = 1$, то пишут, что φ истинна на своем носителе.

Определение 8.4. Формула φ называется общезначной, если она верна для любого носителя интерпретации и любой оценке.

Определение 8.5. $\varphi \sim \psi$, если $\forall$ интерпретации $\forall$ оценки $[\varphi](\pi) = [\psi](\pi)$.

Замечание. $\varphi \sim \psi \Leftrightarrow \varphi \leftrightarrow \psi$ — общезначная

8.4.3 Примеры общезначних формул

Я привел их без доказательства, проделайте это в качестве нетрудного упражнения на дом

1. $\forall x P(x) \to (\exists y Q(x, y) \to \forall x P(x))$

2. $\forall x \varphi \to \exists x \varphi$

3. $\exists x \forall y \varphi \to \forall y \exists x \varphi$

4. $\forall x \forall y \varphi \to \forall y \forall x \varphi$
5. $\forall x(\varphi \land \psi) \leftrightarrow \forall x \varphi \land \forall x \psi$
6. $\exists x(\varphi \land \psi) \to \exists x \varphi \land \exists x \psi$
7. $\exists x(\varphi \land \psi) \leftrightarrow \exists x \varphi \land \psi$, при $(x \notin Par(\psi))$
8. $\exists x(\varphi \lor \psi) \leftrightarrow \exists x \varphi \lor \exists x \psi$
9. $\forall x(\varphi \lor \psi) \leftarrow \forall x \varphi \lor \forall x \psi$
10. $\forall x(\varphi \lor \psi) \leftrightarrow \forall x \varphi \lor \psi$, при $(x \notin Par(\psi))$
11. $\neg \exists x \varphi \leftrightarrow \forall x \neg \varphi$
12. $\neg \forall x \varphi \leftrightarrow \exists x \neg \varphi$
13. $\exists x(\varphi \to \psi) \leftrightarrow (\forall x \varphi \to \exists x \psi)$

8.5 Предварённая нормальная форма

Определение 8.6. Предваренная нормальная форма — это такая формула, в которой сначала идут кванторы, а потом бескванторная форма.

$$\underbrace{\forall \exists \exists \ldots}_{\text{кванторы}} \underbrace{(\ldots\ldots\ldots\ldots\ldots)}_{\text{"бескванторная форма"}}$$

Теорема 8.2. *У любой формулы первого порядка существует эквивалентная ей ПНФ*

Доказательство. Будем проводить следующие эквивалентные преобразования:

1. $\neg \exists x \varphi \longleftrightarrow \forall x \neg \varphi$
2. (a) $\forall x \varphi \land \forall x \psi \longleftrightarrow \forall x(\varphi \land \psi)$
   (b) $\exists x \varphi \lor \exists x \psi \longleftrightarrow \exists x(\varphi \lor \psi)$
3. $\exists x(\varphi \land \psi) \to (\exists x \varphi \land \exists x \psi)$ — но это не эквивалентность, поэтому это использовать нельзя. Как тогда? Нужно сделать замену переменной:

   $$\exists x \varphi \longleftrightarrow \exists y \varphi({}^{y}/_{x})$$

   Где $\varphi({}^{y}/_{x})$ — все свободные вхождения x заменили на y. При этом эти вхождения не должны подпадать под действие кванторов по y и y не входит свободно в формулу φ. Примера некорректных замен:

   (a) $\exists x \forall y A(x, y) \not\leftrightarrow \exists y \forall y A(y, y)$
   (b) $\exists x A(x, y) \not\leftrightarrow \exists y A(y, y)$

   Причем, если мы заменяем на новую переменную, такая замена всегда будет корректна.

4. $\exists x \varphi * \psi$. Если x — не параметр ψ, то $(\exists x \varphi) * \psi \longleftrightarrow \exists x(\varphi * \psi)$. Но тогда, если x — параметр ψ, то $(\exists x \varphi) * \psi \longleftrightarrow (\exists y \varphi({}^{y}/_{x})) * \psi \longleftrightarrow \exists y(\varphi({}^{y}/_{x}) * \psi)$ (y не встречается ни в φ, ни в ψ).

$\square$

8.6 Предикаты и выразимость

Значение формулы зависит только от значения ее параметров. Формула с k параметрами при фиксированной интерпретации задает k-местный предикат.

Определение 8.7. Предикат называется выразимым в данной интерпретации, если его можно задать формулой первого порядка.

Пример.

$$\langle \mathbb{N}, S, = \rangle, S(n) = n + 1$$

Тогда:

1. $x = 0 \Leftrightarrow \neg\exists y(x = S(y))$
2. $x = 1 \Leftrightarrow \exists y(x = S(y) \wedge \underbrace{y = 0}_{\text{подставляем предыдущее}})$

Пример.

$$\langle \mathbb{N}, \cdot, = \rangle$$

Тогда:

1. $x = 0 \Leftrightarrow \neg\forall y(y \cdot x = x)$
2. $x = 0 \Leftrightarrow \neg\forall y(y \cdot x = y)$
3. $x \vdots y \Leftrightarrow \exists z(x = y \cdot z)$
4. p — простое $\Leftrightarrow (p \neq 1 \wedge \forall q(p \vdots q \to (q = 1 \vee q = p)))$
5. $d = \text{НОД}(x, y) \Leftrightarrow (x \vdots d \wedge y \vdots d \forall k((x \vdots k \wedge y \vdots k) \to d \vdots k)$
6. $c = \text{НОК}(x, y) \Leftrightarrow (c \vdots x \wedge c \vdots y \forall k((k \vdots x \wedge k \vdots y) \to k \vdots c)$

Пример.

$$\langle 2^A, \subset \rangle$$

Тогда:

1. $x = y \Leftrightarrow (x \subset y \wedge y \subset x)$
2. $x = \varnothing \Leftrightarrow \forall y(x \subset y)$
3. $|x| = 1 \Leftrightarrow (x \neq \varnothing) \wedge \forall y(y \subset x \to (y = x \vee y = \varnothing))$
4. $z = x \cup y \Leftrightarrow (x \subset z \wedge y \subset z \wedge \forall t((x \subset t \wedge y \subset t)) \to z \subset t)$

8.7 Элиминация кванторов

Рассмотрим следующее множество:

$$\langle \mathbb{N}, S, 0, = \rangle$$

Теорема 8.3. *Любая формула, записанная в этой сигнатуре $S, 0, =$ эквивалентна в интерпретации некоторой бескванторной формуле.*

Доказательство. Ведем индукцию по построению формулы.

База: Атомарные формулы — бескванторные

Переход:

$\neg$: $\varphi \rightleftharpoons \neg\psi \Rightarrow$ по предположению индукции, $\psi \sim \psi'$, ψ' — бескванторная, тогда $\varphi \sim \neg\psi'$ — тоже бескванторная

$\wedge, \vee, \rightarrow$: $\varphi \rightleftharpoons (\psi * \eta) \Rightarrow$ по предположению индукции, $\psi \sim \psi', \eta \sim \eta'$, причем ψ', η' — бескванторные, $\Rightarrow \varphi \sim (\psi' * \eta')$ — тоже бескванторная

$\forall$: $\forall x\varphi \leftrightarrow \neg\exists x\neg\varphi$

$\exists$: $\exists x\varphi$. Как быть? Одна из идей: заменить бесконечную конъюнкцию на конечную. Но сначала приведем саму формулу φ к бескванторному виду φ'.

Заметим, что атомарные формулы у нас могут быть только вида

$$S(S(\ldots(S(u))\ldots)) = S(S(\ldots(S(v))\ldots))$$

Где u, v — либо переменные, либо 0. Но тогда:

$$\begin{array}{cc} u \rightleftharpoons v \rightleftharpoons x & \text{формула } \perp \text{ или } \top \\ S(S(\ldots(S(x))\ldots)) = 0 & \perp \\ S(S(\ldots(S(y))\ldots)) = x & x = y + c \\ S(S(\ldots(S(x))\ldots)) = y & x = y - c \end{array}$$

Итого: $\exists x\varphi$, причем φ — булевая комбинация $\perp, \top$ и равенств вида $x = d, x = y + c, x = y - c$. Рассмотрим $t_1, t_2, \ldots t_k$ — все "правые" части этих равенств. В таком случае, при $x \notin \{t_1, t_2, \ldots t_k\}$, формула не будет зависеть от x, т.к. все равенства вида $x = t_i$ будут заведомо ложны. Тогда

$$\exists x\varphi \sim \varphi|_{\text{все } x_i = t \text{ ложны}} \vee \bigvee \varphi[^{t_i}/_x]$$

(Все выражения с вычитанием преобразуются в сложение в другой части)

□

Определение 8.8. 2 интерпретации одной сигнатуры называются элементарно эквивалентными, если в них верны одни и те же формулы первого порядка.

Теорема 8.4. $\langle \mathbb{R}, \leqslant \rangle \sim \langle \mathbb{Q}, \leqslant \rangle$

Доказательство. В обеих интерпретациях верна теорема об элиминации кванторов, причем элиминация происходит посимвольно одинаково. Отличие от предыдущего — в формуле $\exists x\varphi$ заменим ψ на эквивалентную ей ДНФ.

$$\begin{array}{ll} x = y & (x \leqslant y \land y \leqslant x) \\ x < y & (x \leqslant y \land \neg(y \leqslant x)) \end{array}$$

$$\varphi = C_1 \lor C_2 \lor \cdots \lor C_n$$

Причем C_i — конъюнкции $x_j \leqslant y_j \leftrightarrow (x_j < y_j \lor x_j = y_j)$ или $\neg(x_j \leqslant y_j) \leftrightarrow x_j > y_j$. Тогда раскроем по дистрибутивности скобки в C_i, получится $\varphi = C_1' \lor C_2' \lor \cdots \lor C_n'$, где C_i' — конъюнкция формул вида $x_j = y_j$ или $x_j < y_j$.

$$\exists x\varphi \sim \exists x(C_1' \lor \cdots \lor C_n') \sim \exists x C_1' \lor \exists x C_2' \lor \cdots \lor \exists x C_n'$$

Причем,

$$\exists x C_i' \leftrightharpoons \exists x((x > a_1) \land \cdots \land (x > a_p) \land (x < b_1) \land \cdots \land (x < b_q) \land (x = c_1) \land \cdots \land (x = c_r) \ldots$$

$$\cdots \land (\text{формулы, значение которых не зависит от } x))$$

Но тогда, в силу того, что оба наши порядка плотны, такое число x либо одновременно существует и там и там, либо одновременно не существует, следовательно, изначальные порядки эквивалентны. □

8.8 Игра Эренфойхта

Определение 8.9. Игра Эренфойхта. Пусть заданы две интерпретации A, B, сигнатуры, состоящие только из предикатных символов $(p_1, \ldots p_n)$. Играют два игрока (их обычно называют Новатор и Консерватор или Спойлер и Дубликатор). Новатор фиксирует число ходов m. На i-ом ходу выбраны $a_1, a_2, \ldots a_{i-1} \in A, b_1, b_2, \ldots b_{i-1} \in B$ и Новатор выбирает либо $a_i \in A$, а Консерватор выбирает $b_i \in B$, или наоборот. Цель новатора — чтобы на каком-то наборе для какого-то предиката, стало выполнено $p_j(a_{i_1}, a_{i_2}, \ldots a_{i_l}) \neq p_j(b_{i_1}, b_{i_2}, \ldots b_{i_l})$. Цель консерватора — ему помешать.

8.8.1 Примеры

Пример.

$$\langle \mathbb{N}, \leqslant \rangle, \langle \mathbb{Z}, \leqslant \rangle$$

Хотим понять, что $\exists x \forall y\ x \leqslant y$ — верно в $\mathbb{N}$, но не в $\mathbb{Z}$. 2 хода:

№ хода	Новатор	Консерватор
1	$0 \in \mathbb{N}$	$b \in \mathbb{Z}$
2	$b - 1 \in \mathbb{Z}$	$a \in \mathbb{N}$

Получилось, что $a \geqslant 0$ верно, но $b - 1 \geqslant b$ ложно.

Пример.

$$\langle \mathbb{Z}, \leqslant \rangle, \langle \mathbb{Q}, \leqslant \rangle$$

$$\forall y \forall z(y < z \to \exists v(y < v < z))$$

3 хода:

№ хода	Новатор	Консерватор
1	$0 \in \mathbb{Z}$	$b_0 \in \mathbb{Q}$
2	$1 \in \mathbb{Z}$	$b_1 \in \mathbb{Q}$
3	Победили, если $b_0 > b_1$, иначе называем $\frac{b_0+b_1}{2}$	$a \in \mathbb{Z}$

Получилось, что $0 < a < 1$ должно быть верно в $\mathbb{Z}$, а это неправда, тогда Новатор победил.

Пример.

$$\langle \mathbb{Q}, \leqslant \rangle, \langle \mathbb{R}, \leqslant \rangle$$

$$\forall y \forall z (y < z \to \exists v (y < v < z))$$

Выигрывает консерватор, даже если не фиксировать количество ходов. Новатор ставит точку либо совпадающую с уже выбранными, либо больше всех, либо меньше всех, либо внутри интервала. Ввиду плотности $\mathbb{Q}$, консерватор всегда сможет повторить выбор.

Пример.

$$\langle \mathbb{Z}, \leqslant \rangle, \langle \{0, 1\} \times \mathbb{Z}, \text{лексикографическое сравнение} \rangle$$

Выигрывает консерватор, но только для фиксированного числа ходов. Разобьем интервалы между точками, которые могут быть, на две группы: малые и большие (бесконечные или конечные, но длина больше, чем 2^l, где l — количество ходов до конца игры). Поддерживаем инвариант: между соответствующим точками либо малые и одинаковые, либо большие интервалы (может быть, разные). Новатор не может поделить один интервал на 2 малых. В любом случае мы сможем повторить ход.

Теорема 8.5. *Если в игре Эренфойхта победит Новатор, то интерпретации не являются эквивалентными, и являются таковыми иначе.*

9 Исчисление предикатов

Хотим расширить исчисление высказываний на формулы первого порядка, то есть, чтобы множество выводимых формул было равно множеству общезначных формул.

$$\{\text{выводимые формулы}\} = \{\text{общезначные формулы}\}$$

Теорема 9.1 (Теорема о корректности)**.**

$$\{\textit{выводимые формулы}\} \subset \{\textit{общезначные формулы}\}$$

Теорема 9.2 (Слабая форма Теоремы о полноте)**.**

$$\{\textit{выводимые формулы}\} \supset \{\textit{общезначные формулы}\}$$

9.1 Аксиомы

1...11. A1-11

12. $\forall x \varphi \to \varphi(^t/_x)$, t — терм, подстановка корректна

13. $\varphi(^t/_x) \to \exists x\varphi$, t — терм, подстановка корректна

    $\varphi(^t/_x)$ — результат замены свободного выхождения x на t, при этом свободные переменные t не попадают под действие кванторов φ.

    Подстановка точно корректна, если:

    (a) t — замкнутый терм (состоящий только из констант)

    (b) $t \rightleftharpoons x$

14.

9.2 Правила Бернайса (правила вывода)

1. Σ-правило. Если x — не параметр ψ, то

$$\frac{\varphi \to \psi}{\exists x\varphi \to \psi}$$

2. Π-правило. Если x — не параметр ψ, то

$$\frac{\psi \to \varphi}{\psi \to \forall x\varphi}$$

9.3 Примеры вывода

Пример.

$$\forall x\varphi \to \exists x\varphi$$

1. $\forall x\varphi \to \varphi$ — A12
2. $\varphi \to \exists x\varphi$ — A13
3. $\forall x\varphi \to \exists x\varphi$ — Силлогизм

Пример.

$$\exists x\forall y\varphi \to \forall y\exists x\varphi$$

1. $\forall y\varphi \to \varphi$ — A12
2. $\varphi \to \exists x\varphi$ — A13
3. $\forall y\varphi \to \exists x\varphi$ — Силлогизм
4. $\exists x\varphi\forall y\varphi \to \exists x\varphi$ — Σ-правило
5. $\exists x\forall y\varphi \to \forall y\exists x\varphi$ — Π-правило

Пример (Вывод правила обощения)**.**

Определение 9.1. Правило обобщения:

$$\frac{\varphi}{\forall x\varphi}$$

Это значит, что $\vdash \varphi \Rightarrow \vdash \forall x\varphi$

1. φ
2. ψ — Любая замкнутая аксиома
3. $\varphi \to (\psi \to \varphi)$ — A1
4. $\psi \to \varphi$ — m.p. 1, 3
5. $\psi \to \forall x \varphi$ — П-правило 4
6. $\forall x \varphi$ — m.p. 2, 5

Пример.

$$\neg \exists x \varphi \leftrightarrow \forall x \neg \varphi$$

1. $\forall x \varphi \to \varphi$ — A12
2. $\neg \varphi \to \neg \forall x \varphi$ — контрапозиция
3. $\exists x \neg \varphi \to \neg \forall x \varphi$ — Σ-правило 2

Пример.

$$\neg \forall x \varphi \leftrightarrow \exists x \neg \varphi$$

1. $\forall x \neg \varphi \to \neg \varphi$
2. $\varphi \to \neg \forall x \neg \varphi$
3. $\exists x \varphi \to \neg \forall x \neg \varphi$
4. $\neg \forall x \varphi \leftrightarrow \exists x \neg \varphi$

Определение 9.2. Вывод из посылок — вывод, где в качестве посылок используются замкнутые фомрулы. (Посылки также называют аксиомами)

Определение 9.3. Теория — множество замкнтых формул

Определение 9.4. Модель теории — интерпретация, где все формулы теории истинны.

9.4 Лемма о дедукции для исчисления предикатов

Лемма 9.1 (О дедукции)**.** *Пусть* Γ *— теория,* A *— замкнутая формула,* B *— произвольная формула. Тогда* $\Gamma \vdash A \to B \Leftrightarrow \Gamma, A \vdash B$*.*

Доказательство.

$\Rightarrow$.
1. $A \to B$ — вывод
2. A — посылка
3. B — m.p. 1, 2

$\Leftarrow$. Пусть $C_1, C_2, \dots C_n$ — вывод B из Γ, A. По индукции докажем, что $\Gamma \vdash A \to C_i$.

База

Переход

i. C_i — аксиома, или элемент Γ, или получена по m.p. — аналог для Исчисления Высказываний.

ii. C_i — получена по Σ-правилу. Тогда $C_i = (\exists x\varphi \to \psi), C_j = (\varphi \to \psi), j < i$. По предположению индукции, $\Gamma \vdash (A \to (\varphi \to \psi))$. Тавтология: $(A \to (\varphi \to \psi)) \leftrightarrow (\varphi \to (A \to \psi)) \Rightarrow \Gamma \vdash (\varphi \to (A \to \psi)) \Rightarrow \Gamma \vdash (\exists x\varphi \to (A \to \psi)) \underbrace{\Longrightarrow}_{\Sigma\text{-правило}} \Gamma \vdash (A \to (\exists x\varphi \to \psi)) \Rightarrow \Gamma \vdash (A \to C_i)$.

iii. C_i — получена по Π-правилу.

$$\Gamma \vdash (A \to (\psi \to \varphi)) \Rightarrow \left[\begin{array}{l} \Gamma \vdash (A \to (\psi \to \forall x\varphi)) \\ \Gamma \vdash ((A \wedge \psi) \to \varphi) \end{array}\right.$$

□

Определение 9.5. Теория Γ называется полной, если $\forall\varphi$ верно $\Gamma \vdash \varphi$ или $\Gamma \vdash \neg\varphi$.

Определение 9.6. Теория Γ называется экзистенциально полной, если $\Gamma \vdash \exists x\psi \Rightarrow \Gamma \vdash \psi({}^t/_x)$ для некоторого замкнутого терма t.

Лемма 9.2. *Любая непротиворечивая теория вложена в какую-то полную*

Лемма 9.3. Γ — *непротиворечивая теория в сигнатуре* $\sigma \Rightarrow$ *существует* $\tau \subset \sigma, \Delta \supset \Gamma$, Δ — *экзистенциально полная непротиворечивая теория в сигнатуре* τ.

Теорема 9.3 (Сильная форма Теоремы о полноте ИП)**.** *У любой непротиворечивой теории существует модель*

Доказательство. Потом □

Доказательство слабой формы теоремы о полноте ИП. φ — общезначная $\Rightarrow \forall x\varphi$ — общезначная $\Rightarrow$ у $\{\neg\forall x\varphi\}$ нет модели $\Rightarrow \{\neg\forall x\varphi\}$ — противоречива $\Rightarrow \left\{\begin{array}{l} \{\neg\forall x\varphi\} \vdash A \\ \{\neg\forall x\varphi\} \vdash \neg A \end{array}\right. = \left\{\begin{array}{l} \vdash \{\neg\forall x\varphi\} \to A \\ \vdash \{\neg\forall x\varphi\} \to \neg A \end{array}\right. \Rightarrow \vdash \neg\neg\forall x\varphi \Rightarrow \vdash \forall x\varphi \Rightarrow \varphi$. □

9.5 Теорема Геделя о Полноте

Определение 9.7. Δ полная в сигнатуре σ, если для любой замкнутой формулы ψ этой сигнатуры $\Delta \vdash \varphi$ или $\Delta \vdash \neg\varphi$.

Лемма 9.4. Γ — *непротиворечивая теория в сигнатуре* $\sigma \Rightarrow$ *существует теория* $\Delta \supset \Gamma$ — *непротиворечивая, полная в сигнатуре* σ.

Для конечного или счетного количесвта переменных. $\Rightarrow$ Все формулы можно занумеровать натуральными числами $(\varphi_1, \varphi_2 \ldots)$. Обозначим:

$$\Gamma_0 := \Gamma, \Gamma_{i+1} = \left\{\begin{array}{ll} \Gamma_i \cup \{\varphi_i\}, & \text{если непротиворечиво} \\ \Gamma_i \cup \{\neg\varphi_i\}, & \text{иначе} \end{array}\right.$$

Заметим, что все Γ_i непротиворечивы, т.к. Γ — непротиворечива, и если Γ_{i+1} прориворечива, то и $\Gamma_i \cup \{\varphi_i\}, \Gamma_i \cup \{\neg\varphi_i\}$ — тоже, но тогда $\Gamma \vdash \neg\varphi_{i+1}, \Gamma \vdash \neg\neg\varphi_{i+1}$, Но тогда и все предыдущие были противоречивы, в том числе, Γ, противоречие. Рассмотрим

$$\Delta = \bigcup_{i=0}^{\infty} \Gamma_i$$

Δ непротиворечива, т.к. иначе в нем было бы конечное противоречивое подмножество, а это неправда, т.к. все Γ_i непротиворечивы. □

Определение 9.8. Теория Γ экзистенциально полна относительно сигнатуры σ, если для любой замкнутой формулы вида $\exists x\varphi$, если $\Gamma \vdash \exists x\varphi$, то для некоторого константного символа $c \in \sigma$ (или замкнутого терма) выполнено, что $\Gamma \vdash \varphi({}^{c}/_{x})$

Лемма 9.5. Γ — *непротиворечивая теория в сигнатуре* $\sigma \Rightarrow$ *существует непротиворечивая теория* $\Delta \supset \Gamma$ *и сигнатура* $\tau \supset \sigma$, *т.ч. если* $\Gamma \vdash \exists x\varphi$ *и* φ *в сигнатуре* σ, *то для некоторого константного символа* $c \in \tau$ *выполнено, что* $\Delta \vdash \varphi({}^{c}/_{x})$

Доказательство. Если $\Gamma \vdash \exists x\varphi$, то добавим в сигнатуру константу c_φ, а в теорию — формулу $\varphi({}^{c_\varphi}/_{\varphi})$. Почему не будет противоречия? Пусть $\Gamma \cup \{\varphi({}^{c_\varphi}/_{x})\} \vdash \psi, \neg\psi$. По лемме о дедукции $\Gamma \vdash \varphi({}^{c_\varphi}/_{x}) \to \psi, \Gamma \vdash \varphi({}^{c_\varphi}/_{x}) \to \neg\psi$. Можно считать, что ψ замкнута, иначе применим Аксиому 9. Получим, что $\Gamma \vdash \varphi({}^{y}/_{x}) \to \psi$, где y — свободная переменная. По Σ-правилу Бернайса, $\Gamma \vdash \exists y\varphi({}^{y}/_{x}) \to \psi$. Переименуем переменную $y \to x$: получится $\Gamma \vdash \exists x\varphi \to \psi$. Т.к. $\Gamma \vdash \exists x\varphi$, то $\Gamma \vdash \psi$. Аналогично $\Gamma \vdash \neg\psi \Rightarrow \Gamma$ — прориворечива, противоречие. □

Лемма 9.6. Γ — *непротиворечивая теория в сигнатуре* $\sigma \Rightarrow$ *существует теория* $\Delta \supset \Gamma$ *и сигнатура* $\tau \supset \sigma$, *т.ч.* Δ — *непротиворечивая, полная и экзистениально полная относительно* τ.

Доказательство. Идея: поочередно применяем две предыдущие леммы.

$$\begin{array}{ccl}
\Gamma_0 = \Gamma & \sigma_0 = \sigma & \\
\Gamma_1 \supset \Gamma_0 & \sigma_1 = \sigma_0 & \Gamma_1 \text{ полная относительно } \sigma_1 \\
\Gamma_2 \supset \Gamma_1 & \sigma_2 = \sigma_1 & \Gamma_2 \text{ экзистенциально полная относительно } \sigma_1 \\
\Gamma_3 \supset \Gamma_2 & \sigma_3 = \sigma_2 & \Gamma_3 \text{ полная относительно } \sigma_3 \\
\vdots & \vdots & \vdots \\
\Delta = \bigcup_{i=0}^{\infty} \Gamma_i & \tau = \bigcup_{i=0}^{\infty} \sigma_i &
\end{array}$$

φ — замкнутая формула в сигнатуре $\tau \Rightarrow \varphi$ — замкнутая формула $\Rightarrow \Gamma_{i+1} \vdash \varphi$ или $\Gamma_{i+1} \vdash \neg\varphi \Rightarrow \Delta \vdash \varphi$ или $\Delta \vdash \neg\varphi$. Аналогично для экзистенциальной полноты. □

Лемма 9.7. *Полная, непротиворечивая, экзистенциально полная теория имеет модель*

Доказательство. Носитель — замкнутые термы (составленные из констант). Будем обозначать за "t" — терм, как элемент носителя. Вычисляем термы и предикаты следующим образом:

$$[f]("t_1", "t_2", "t_3" \dots) = "[f](t_1, t_2, t_3, \dots)"$$

$$[P]("t_1", "t_2", "t_3" \dots) = \begin{cases} 0, \Delta \vdash P(t_1, t_2, t_3, \dots) \\ 1, \Delta \vdash \neg P(t_1, t_2, t_3, \dots) \end{cases}$$

Утверждение 9.1. *Все формулы из Δ истинны в этой интерпретации , а все замкнутые формулы не из Δ ложны.*

Доказательство. Ведем индукцию по построению формулы.

1. Атомарные формулы — по определению
2. $\varphi = \neg\psi$ $\Delta \nvdash \varphi \Leftrightarrow \Delta \vdash \psi \Rightarrow \psi$ истинно $\Rightarrow \varphi$ ложна
3. $\varphi = (\psi * \mu)$ — Аналогично
4. $\varphi = \exists x \psi$
$$\Delta \vdash \exists x\psi \Leftrightarrow \Delta \vdash \psi({}^t/_x) \Rightarrow \psi({}^t/_x) \text{ истинна} \Rightarrow \exists x\psi \text{ истинна}$$
$$\Delta \vdash \neg\exists x\psi \Rightarrow \text{ для всех } t \text{ формула } \psi({}^t/_x) \text{ ложна, тогда } \exists x\psi \text{ тоже ложна}$$
$$\text{иначе, если } \psi({}^t/_x) \text{ истинно, то } \Delta \vdash \psi({}^t/_x) \Rightarrow \Delta \vdash \exists x\psi$$
5. $\varphi = \forall x\psi$ — аналогично

□

□

Теорема 9.4 (Мальцева о Компактности)**.** *Если* Γ *— теория и любая конечная подтеория имеет модель, то и вся* Γ *имеет модель*

Доказательство.

1. Γ — противоречивая $\Rightarrow$ конечная подтеория противоречива $\Rightarrow$ не имеет модели
2. Γ — непротиворечива $\Rightarrow$ имеет модель

□