Конспект по Матлогу. Часть 3

Штукенберг Дмитрий

под редакцией Чепелина Вячеслава

Содержание

1 Лекция 10.

1.1 Введение в теорию множеств

def: **Теория множеств** — теория первого порядка, с дополнительным нелогическим двухместным функциональным символом $\in$, и следующими дополнительными нелогическими аксиомами и схемами аксиом.

1.2 Аксиоматика ZF, равенство, конструктивные аксиомы

def: **Равенство «по Лейбницу»**: объекты равны, если неразличимы. Если нечто ходит как утка, выглядит как утка и крякает как утка, то это утка.

def: **Принцип объёмности**: объекты равны, если состоят из одинаковых частей.

$A \subseteq B \equiv \forall x.x \in A \to x \in B$ $A = B \equiv A \subseteq B \,\&\, B \subseteq A$

def: **Аксиома равенства**: равные множества содержатся в одних и тех же множествах. $\forall x.\forall y.\forall z.x = y \,\&\, x \in z \to y \in z$.

def: **Аксиома пустого.** Существует пустое множество $\varnothing$.

$$\exists s.\forall t.\neg t \in s$$

def: **Аксиома пары.** Существует $\{a, b\}$. Каковы бы ни были два множества a и b, существует множество, состоящее в точности из них.

$$\forall a.\forall b.\exists s.a \in s \,\&\, b \in s \,\&\, \forall c.c \in s \to c = a \vee c = b$$

def: **Аксиома объединения:** существует $\cup x$. Для любого непустого множества x найдется такое множество, состоящее в точности из тех элементов, из которых состоят элементы x.

$$\forall x.(\exists y.y \in x) \to \exists p.\forall y.y \in p \leftrightarrow \exists s.y \in s \,\&\, s \in x$$

def: **Аксиома степени**: существует $\mathcal{P}(x)$. Каково бы ни было множество x, существует множество, содержащее в точности все возможные подмножества множества x.

$$\forall x.\exists p.\forall y.y \in p \leftrightarrow y \subseteq x$$

def: Схема аксиом выделения: существует $\{t \in x \mid \varphi(t)\}$. Для любого множества x и любой формулы от одного аргумента $\varphi(y)$ (b не входит свободно в φ), найдется b, в которое входят те и только те элементы из множества x, что $\varphi(y)$ истинно.

$$\forall x.\exists b.\forall y.y \in b \leftrightarrow (y \in x \,\&\, \varphi(y))$$

Теорема.

Для любого множества X существует множество $\{X\}$, содержащее в точности X.

Воспользуемся аксиомой пары: $\{X, X\}$

Теорема

Пустое множество единственно.

Доказательство:

Пусть $\forall p.\neg p \in s$ и $\forall p.\neg p \in t$. Тогда $s \subseteq t$ и $t \subseteq s$.

Q.E.D.

Теорема.

Для двух множеств s и t существует множество, являющееся их пересечением.

Доказательство:

$s \cap t = \{x \in s \mid x \in t\}$

Q.E.D.

def:Упорядоченная пара. Упорядоченной парой двух множеств a и b назовём $\{\{a\}, \{a, b\}\}$, или $\langle a, b\rangle$

Теорема. Упорядоченную пару можно построить для любых множеств.

Доказательство:

Применить аксиому пары, теорему о существовании $\{X\}$, аксиому пары.

Q.E.D.

Теорема. $\langle a, b\rangle = \langle c, d\rangle$ тогда и только тогда, когда $a = c$ и $b = d$.

1.3 Аксиома бесконечности

def: Инкремент: $x' \equiv x \cup \{x\}$

def: Аксиома бесконечности. Существует $N : \varnothing \in N \,\&\, \forall x.x \in N \to x' \in N$

В N есть всевозможные множества вида $\varnothing$, $\{\varnothing\}$, $\{\varnothing, \{\varnothing\}\}$, $\{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}\}$, $\dots$

(неформально) $\omega = \{\varnothing, \varnothing', \varnothing'', \dots\}$. Тогда $N_1 = \omega \cup \{\omega, \omega', \omega'', \dots\}$ подходит.

1. Частичный: рефлексивность ($a \preceq a$), антисимметричность ($a \preceq b \to b \preceq a \to a = b$), транзитивность ($a \preceq b \to b \preceq c \to a \preceq c$).
2. Линейный: частичный + $\forall a.\forall b.a \preceq b \vee b \preceq a$.
3. Полный: линейный + в любом непустом подмножестве есть наименьший элемент.

$\mathbb{Z}$ не вполне упорядочено: в $\mathbb{Z}$ нет наименьшего.

Отрезок $[0, 1]$ не вполне упорядочен: $(0, 1)$ не имеет наименьшего.

$\mathbb{N}$ вполне упорядочено.

1.4 Ординалы (порядковые числа)

def: Транзитивное множество X: $\forall x.\forall y.x \in y \,\&\, y \in X \to x \in X$.

def: Ординал (порядковое число) — вполне упорядоченное отношением $(\in)$ транзитивное множество.

Ординалы: $\varnothing$, $\varnothing'$, $\varnothing''$, $\dots$

def: Предельный ординал: такой x, что $x \neq \varnothing$ и нет $y : y' = x$

def: Ординал x конечный, если он сам не предельный и нет предельного, меньшего его.

Теорема.

Если x, y — ординалы, то $x = y$, или $x \in y$, или $y \in x$.

def: ω — наименьший предельный ординал.

Теорема.

ω существует.

Доказательство:

Пусть $\omega = \{x \in N \mid x \text{ конечен}\}$. Тогда:

- меньше ω предельных нет: если θ таков, что $\theta \in \omega$, тогда θ конечен.
- ω предельный: Пусть θ таков, что $\theta' = \omega$. Тогда θ конечен и θ' тоже конечен.

Q.E.D.

ω' — тоже ординал.

def: Порядковый тип множества — некоторое свойство, общее для всех множеств, изоморфных относительно биективных отображений, сохраняющих порядок.

def: Порядковый тип вполне упорядоченного множества $\langle S, (\preceq) \rangle$ — ординал A, для которого есть биективное отображение $f : S \to A$, сохраняющее порядок: $a \preceq b$ тогда и только тогда, когда $f(a) \leq f(b)$

Множество $\mathbb{Z}$ не имеет порядкового типа (в смысле определения через ординалы): оно не вполне упорядочено.

1.5 Операции над ординалами

def: $a + b$ — порядковый тип $a \uplus b$ (отмеченного объединения), причём $x_a < y_b$ при любых $x \in a$ и $y \in b$

def: $a \cdot b$ — порядковый тип $a \times b$, произведение упорядочено лексикографически: $\langle x_1, y_1 \rangle < \langle x_2, y_2 \rangle$, если $x_1 < x_2$ или $x_1 = x_2$ и $y_1 < y_2$.

$\overline{3} + \overline{4}$: порядковый тип множества $\{\overline{0}_a, \overline{1}_a, \overline{2}_a, \overline{0}_b, \overline{1}_b, \overline{2}_b, \overline{3}_b\}$, то есть $\overline{7}$

$\overline{\omega} \cdot \overline{\omega}$: порядковый тип всех натуральных точек плоскости, $\{\langle 0, 0 \rangle, \dots, \langle 0, 100 \rangle, \dots, \langle 100, 0 \rangle, \dots\}$

1.6 Операции над ординалами — как вычислять

def: upb x — верхняя грань множества ординалов, upb $x = \bigcup_{a \in x} a$.

upb $\{\varnothing', \varnothing'', \varnothing''''\} = \varnothing' \cup \varnothing'' \cup \varnothing'''' = \{\varnothing\} \cup \{\varnothing, \{\varnothing\}\} \cup \{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}, \{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}\}\} = \varnothing''''$

Теорема.

$$a + b \equiv \begin{cases} a, & b \equiv \varnothing \\ (a+c)', & b \equiv c' \\ \text{upb } \{a + c \mid c \prec b\}, & b \text{ — предельный ординал} \end{cases}$$

$\omega + 1 = \omega \cup \{\omega\}$; $1 + \omega = \text{upb } \{1 + \varnothing, 1 + 1, 1 + 2, \dots\} = \omega$

Теорема:

$$a \cdot b \equiv \begin{cases} 0, & b \equiv \varnothing \\ (a \cdot c) + a, & b \equiv c' \\ \text{upb } \{a \cdot c \mid c \prec b\}, & \text{b — предельный ординал} \end{cases}$$

def:

$$a^b \equiv \begin{cases} 1, & b \equiv \varnothing \\ (a^c) \cdot a, & b \equiv c' \\ \text{upb } \{a^c \mid c \prec b\}, & b \text{ — предельный ординал} \end{cases}$$

$\omega \cdot \omega = \text{upb } \{\omega \cdot 0, \omega \cdot 1, \omega \cdot 2, \omega \cdot 3, \dots\} = \text{upb } \{0, \omega, \omega \cdot 2, \omega \cdot 3, \dots\}$

1.7 Ординалы (порядковые числа) и порядок

- Добавить элемент перед бесконечностью: $\mathbb{N}$ и $\mathbb{N}_0$. $1 + \omega = \omega$.
- Добавить элемент после бесконечности ($+\infty$). $\omega + 1 \neq \omega$

Упорядоченные пары натуральных чисел имеют порядковый тип ω^2.

$$\langle 3, 5 \rangle < \langle 4, 3 \rangle \qquad \omega \cdot 3 + 5 < \omega \cdot 4 + 3.$$

Списки натуральных чисел — порядковый тип ω^ω.

$$\langle 3, 1, 4, 1, 5, 9 \rangle \qquad \omega^5 \cdot 3 + \omega^4 \cdot 1 + \omega^3 \cdot 4 + \omega^2 \cdot 1 + \omega^1 \cdot 5 + 9$$

1.8 Дизъюнктные множества

def: Дизъюнктное (разделённое) множество — множество, элементы которого не пересекаются.

$$Dj(x) \equiv \forall y. \forall z. (y \in x \mathbin{\&} z \in x \mathbin{\&} \neg y = z) \rightarrow \neg \exists t. t \in y \mathbin{\&} t \in z$$

Дизъюнктное: $\{\{1, 2\}, \{\rightarrow\}, \{\alpha, \beta, \gamma\}\}$
Не дизъюнктное: $\{\{1, 2\}, \{\rightarrow\}, \{\alpha, \beta, \gamma, 1\}\}$

def: Прямое произведение дизъюнктного множества a — множество $\times a$ всех таких множеств b, что:

- b пересекается с каждым из элементов множества a в точности в одном элементе
- b содержит элементы только из $\cup a$.

$$\forall b. b \in \times a \leftrightarrow (b \subseteq \cup a \mathbin{\&} \forall y. y \in a \rightarrow \exists! x. x \in y \mathbin{\&} x \in b)$$

$\times\{\{\triangle, \square\}, \{1, 2, 3\}\} = \{\{\triangle, 1\}, \{\triangle, 2\}, \{\triangle, 3\}, \{\square, 1\}, \{\square, 2\}, \{\square, 3\}\}$

1.9 Аксиома выбора

def: Прямое произведение непустого дизъюнктного множества, не содержащего пустых элементов, непусто.

$$\forall t.Dj(t) \to (\forall x.x \in t \to \exists p.p \in x) \to (\exists p.p \in \times t)$$

Альтернативные варианты: любое множество можно вполне упорядочить, любая сюръективная функция имеет частичную обратную, и т.п.

def: Аксиоматика ZF + аксиома выбора = ZFC

1.10 Аксиома фундирования

def: Аксиома фундирования. В каждом непустом множестве найдется элемент, не пересекающийся с исходным множеством.

$$\forall x.x = \varnothing \lor \exists y.y \in x \,\&\, \forall z.z \in x \to z \notin y$$

Иными словами, в каждом множестве есть элемент, минимальный по отношению ($\in$).

Идея Рассела: каждому множеству припишем *тип* (тип пустого 0, тип множеств 1, тип множеств множеств 2 и т.п.). Тогда конструкция невозможна: $\{x \mid x \in x\}$. Аксиома фундирования позволяет определить функцию ранга:

$$rk(x) = \text{upb } \{rk(y) \mid y \in x\}$$

.

def: Схема аксиом подстановки. Пусть задана некоторая функция f, представимая в исчислении предикатов: то есть задана некоторая формула ϕ, такая, что $f(x) = y$ тогда и только тогда, когда $\phi(x, y) \,\&\, \exists! z.\phi(x, z)$. Тогда для любого множества S существует множество f(S) — образ множества S при отображении f.

$$\forall s.(\forall x.\forall y_1.\forall y_2.x \in s \,\&\, \phi(x, y_1) \,\&\, \phi(x, y_2) \to y_1 = y_2) \to (\exists t.\forall y.y \in t \leftrightarrow \exists x.x \in s \,\&\, \phi(x, y))$$

2 Лекция 11

2.1 Отношения

def: $A \times B := \{\langle a, b\rangle \mid a \in A, b \in B\}$

Бинарное отношение — $R \subseteq A \times B$

Функциональное бинарное отношение (функция) R — такое, что $\forall x. x \in A \to \exists! y. \langle x, y\rangle \in R$

R — инъективная функция, если $\forall x. \forall y. \langle x, t\rangle \in R \,\&\, \langle y, t\rangle \in R \to x = y$.

R — сюръективная функция, если $\forall y. y \in B \to \exists x. \langle x, y\rangle \in R$.

2.2 Равномощные множества

def:Множество A *равномощно* B ($|A| = |B|$), если существует биекция $f : A \to B$.

Множество A имеет мощность, не превышающую мощности B ($|A| \le |B|$), если существует инъекция $f : A \to B$.

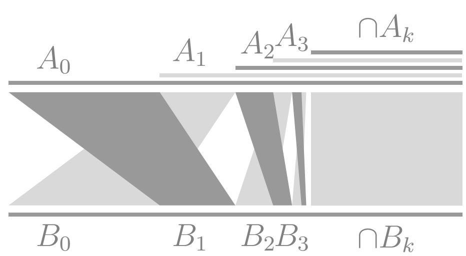
Теорема Кантора-Бернштейна

Если $|A| \le |B|$ и $|B| \le |A|$, то $|A| = |B|$.

Заметим, $f : A \to B$, $g : B \to A$ — инъекции, но не обязательно $g(f(x)) = x$.

Доказательство:

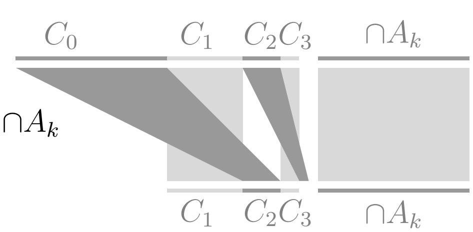
Избавимся от множества B: пусть $A_0 = A$; $A_1 = g(B)$; $A_{k+2} = g(f(A_k))$.



Тогда, если существует $h : A_0 \to A_1$ — биекция, то тогда $g^{-1} \circ h : A \to B$ — требуемая биекция.

Пусть $C_k = A_k \setminus A_{k+1}$. Тогда $g(f(C_k)) = g(f(A_k)) \setminus g(f(A_{k+1})) = A_{k+2} \setminus A_{k+3} = C_{k+2}$.

$$h(x) = \begin{cases} x, & x \in C_{2k+1} \vee x \in \cap A_k \\ g(f(x)), & x \in C_{2k} \end{cases}$$



Тогда определим $h(x)$ следующим образом:

$$h(x) = \begin{cases} x, & x \in C_{2k+1} \vee x \in \cap A_k \\ g(f(x)), & x \in C_{2k} \end{cases}$$

Q.E.D.

2.3 Кардинальные числа

def: **Кардинальное число** — наименьший ординал, не равномощный никакому меньшему:

$$\forall x.x \in c \to |x| < |c|$$

Теорема. Конечные ординалы — кардинальные числа.

def: Мощность множества ($|S|$) — равномощное ему кардинальное число.

2.4 Диагональный метод

def: $|\mathbb{R}| > |\mathbb{N}|$

Доказательство:

Рассмотрим $a \in (0,1)$ и десятичную запись: $0.a_0a_1a_2\dots$. Пусть существует биективная $f : \mathbb{N} \to (0,1)$. По функции найдём значение σ, не являющееся образом никакого натурального числа.

n	$f(n)$	$f(n)_0$	$f(n)_1$	$f(n)_2$	$f(n)_3$	$f(n)_4$	$f(n)_5$	$\dots$
n_0	0.3	3	0	0	0	0	0	$\dots$
n_1	$\pi/10$	3	1	4	1	5	9	$\dots$
n_2	$1/7$	1	4	2	8	5	7	$\dots$
	σ	8	6	7	$\dots \sigma_k = (f(n_k)_k + 5)\%10$			

Q.E.D.

Теорема Кантора

$|\mathcal{P}(S)| > |S|$

Доказательство:

Пусть $S = \{a, b, c, \dots\}$

n	$a \in f(n)$	$b \in f(n)$	$c \in f(n)$	$\dots$
a	И	Л	И	
b	Л	Л	И	
c	И	И	И	
	Л	И	Л	$y \notin f(y)$

Пусть $f : S \to \mathcal{P}(S)$ — биекция. Тогда $\sigma = \{y \in S \mid y \notin f(y)\}$. Пусть $f(x) = \sigma$. Но $x \in f(x)$ тогда и только тогда, когда $x \notin \sigma$, то есть $f(x) \neq \sigma$.

Q.E.D.

2.5 Иерархии $\aleph_n$ и $\beth_n$

def: $\aleph_0 := |\omega|$; $\aleph_{k+1} := \min\{a \mid a - \text{ординал}, \aleph_k < |a|\}$

def: $\beth_0 := |\omega|$; $\beth_{k+1} := |\mathcal{P}(\beth_k)|$

Континуум-гипотеза (Г.Кантор, 1877): $\aleph_1 = \beth_1$ (не существует мощности, промежуточной между счётной и континуумом).

Обобщённая континуум-гипотеза: $\aleph_n = \beth_n$ при всех n.

def: Утверждение α противоречит аксиоматике: $\vdash \alpha$ ведёт к противоречию.

def: Утверждение α не зависит от аксиоматики: $\nvdash \alpha$ и $\nvdash \neg\alpha$.

Теорема о независимости континуум-гипотезы

Утверждение $\aleph_1 = \beth_1$ не зависит от аксиоматики ZFC.

2.6 Примеры мощностей множеств

Пример	мощность
ω	$\aleph_0$
ω^2, ω^ω	$\aleph_0$
$\mathbb{R}$	$\beth_1$
все непрерывные функции $\mathbb{R} \to \mathbb{R}$	$\beth_1$
все функции $\mathbb{R} \to \mathbb{R}$	$\beth_2$

2.7 Арифметика для кардинальных чисел

def: Если α и β — кардинальные числа, то $\alpha + \beta := |\alpha \uplus \beta|$, $\alpha \cdot \beta := |\alpha \times \beta|$, α^β — мощность множества всех функций из β в α

Теорема. Если α — некоторое бесконечное кардинальное число, то $\alpha \cdot \alpha = \alpha$

Теорема. Если $0 < \beta \le \alpha$ и α бесконечное, то $\alpha \cdot \beta = \alpha$

Доказательство:

- $\alpha \cdot \beta \ge \alpha$: фиксируем $b_0 \in \beta$ (т.к. $\beta > 0$), тогда в качестве $f : \alpha \to \alpha \times \beta$ возьмём $f(a) = \langle a, b_0 \rangle$.
- $\alpha \cdot \beta \le \alpha \cdot \alpha = \alpha$.

Q.E.D.

2.8 Как пересчитать вещественные числа (неформально)?

1. Номер вещественного числа — первое упоминание в литературе, т.е. $\langle j, y, n, p, r, c \rangle$:
   j — гёделев номер названия научного журнала (книги);
   y — год издания;
   n — номер;
   p — страница;
   r — строка;
   c — позиция

2. Попробуете предъявить число x, не имеющее номера? Это рассуждение сразу даст номер.

2.9 Мощность модели и аксиоматизации

def: Пусть задана модель $\langle D, F_n, P_n\rangle$ для некоторой теории первого порядка. Её мощностью будем считать мощность D.

def: Пусть задана формальная теория с аксиомами α_n. Её мощность — мощность множества $\{\alpha_n\}$.

Формальная арифметика, исчисление предикатов, исчисление высказываний — счётно-аксиоматизируемые

2.10 Элементарная подмодель

def: $\mathcal{M}' = \langle D', F'_n, P'_n\rangle$ — элементарная подмодель $\mathcal{M} = \langle D, F_n, P_n\rangle$, если:

1. $D' \subseteq D$, F'_n, P'_n — сужение F_n, P_n (замкнутое на D').
2. $\mathcal{M} \models \varphi(x_1, \ldots, x_n)$ тогда и только тогда, когда $\mathcal{M}' \models \varphi(x_1, \ldots, x_n)$ при $x_i \in D'$.

Теорема Лёвенгейма-Сколема

Пусть T — множество всех формул теории первого порядка. Пусть теория имеет некоторую модель $\mathcal{M}$. Тогда найдётся элементарная подмодель $\mathcal{M}'$, причём $|\mathcal{M}'| \leq \max(\aleph_0, |T|)$.

Доказательство(схема)

1. Построим D_0 — множество всех значений, которые упомянуты в языке теории.
2. Будем последовательно пополнять D_i: $D_0 \subseteq D_1 \subseteq D_2 \ldots$, следя за мощностью. $D' = \cup D_i$.
3. Покажем, что $\langle D', F_n, P_n\rangle$ — требуемая подмодель.

Пусть $\{f^0_k\}$ — все 0-местные функциональные символы теории.

1. $D_0 = \{[\![f^0_k]\!]\}$, если есть хотя бы один f^0_k.
2. Если таких f^0_k нет, возьмём какое-нибудь одно значение из D.

Очевидно, $|D_0| \leq |T|$.

Фиксируем некоторый D_k. Напомним, T — множество всех формул теории. Рассмотрим $\varphi \in T$.

1. φ не имеет свободных переменных — пропустим.
2. φ имеет хотя бы одну свободную переменную y.
   (a) $\varphi(y, x_1, \ldots, x_n)$ при $y, x_i \in D_k$ бывает истинным и ложным — ничего не меняем
   (b) $\varphi(y, x_1, \ldots, x_n)$ при $y \in D$ и $x_i \in D_k$ либо всегда истинен, либо всегда ложен — ничего не меняем
   (c) $\varphi(y, x_1, \ldots, x_n)$ при $y, x_i \in D_k$ тождественно истинен или ложен, но при $y' \in D \setminus D_k$ отличается — добавим y' к D_{k+1}. Вместе добавим всевозможные $[\![\theta(y')]\!]$.

1. Всего добавили не больше $|T| \cdot |T|$ (для каждой формулы φ, возможно, будет добавлен y — и всевозможные выражения $\theta(y)$, допустимые в языке), и $|D_0| \leq |T| \leq |T| \cdot |T|$, отсюда $|D_k| \leq |T| \cdot |T|$.

2. $|D'| = |\bigcup D_i| \le |T| \cdot |T| \cdot \aleph_0$.
3. Тогда $|T| \cdot |T| \cdot \aleph_0 = \max(|T|, \aleph_0)$. Разберём случаи:
   (a) Если $|T| < \aleph_0$, тогда $(|T| \cdot |T|) \cdot \aleph_0 = \aleph_0$
   (b) Если $|T| \ge \aleph_0$, тогда $(|T| \cdot |T|) \cdot \aleph_0 = |T| \cdot \aleph_0 = |T|$.
4. Итого, $|D'| \le \max(|T|, \aleph_0)$.

Докажем, что $\mathcal{M}'$ — элементарная подмодель

Индукцией по структуре формул $\tau \in T$ покажем, что все формулы можно вычислить, и что $[\![\varphi]\!]_{\mathcal{M}'} = [\![\varphi]\!]_{\mathcal{M}}$.

1. База, 0 связок. $\tau \equiv P(f_1(x_1, \dots, x_n), \dots, f_n(x_1, \dots, x_n))$. Если $x_i \in D'$, то значит, добавлены на некоторых шагах (максимальный пусть t). Поэтому в D_{t+1} можно вычислить формулу, и её значение сохранилось.
2. Переход. Пусть формулы из k связок сохраняют значения. Рассмотрим τ с $k+1$ связкой.
   (a) $\tau \equiv \rho \star \sigma$ — очевидно.
   (b) $\tau \equiv \forall y.\varphi(y, x_1, \dots, x_n)$. Каждый x_i добавлен на каком-то шаге — максимум t. Если $\varphi(y, x_1, \dots, x_n)$ бывает истинен и ложен при $y_t, y_f \in D$, то $y_t, y_f \in D_{t+1}$ (по построению). Поэтому, если $\mathcal{M} \not\models \forall y.\varphi(y, x_1, \dots, x_n)$, то и $\mathcal{M}' \not\models \forall y.\varphi(y, x_1, \dots, x_n)$. Если же $\varphi(y, x_1, \dots, x_n)$ не меняется от y, то тем более $[\![\varphi]\!]_{\mathcal{M}'} = [\![\varphi]\!]_{\mathcal{M}}$.
   (c) $\tau \equiv \exists y.\varphi(y, x_1, \dots, x_n)$ — аналогично.

2.11 «Парадокс» Сколема

1. Как известно, $|\mathbb{R}| = |\mathcal{P}(\mathbb{N})| > |\mathbb{N}| = \aleph_0$. Однако, ZFC — теория со счётным количеством формул. Значит, существует счётная модель ZFC, то есть $|\mathbb{R}| = \aleph_0$. В чём ошибка?
2. У равенств разный смысл, первое — в предметном языке, второе — в метаязыке.

3 Лекция 12.

3.1 Аксиома выбора

def: Аксиома выбора:

Из любого семейства дизъюнктных непустых множеств $\mathcal{A}$ можно выбрать непустую трансверсаль — множество S, что $|S \cap A| = 1$ для каждого $A \in \mathcal{A}$. Иначе, $S \in \times\mathcal{A}$.

Теорема: функциональный вариант аксиомы выбора Пусть $\mathcal{A}$ — семейство непустых множеств. Тогда существует $f : \mathcal{A} \to \cup\mathcal{A}$, причём $\forall a.a \in \mathcal{A} \to f(a) \in a$

Доказательство:

Пусть $X(A) = \{\langle A, a\rangle \mid a \in A\}$, по семейству $\mathcal{A}$ рассмотрим $\{X(A) \mid A \in \mathcal{A}\}$

- непустых: если $A \in \mathcal{A}$, $A \neq \varnothing$, то $X(A) \neq \varnothing$;
- дизъюнктное: если $A_0, A_1 \in \mathcal{A}$, $A_0 \neq A_1$, то $X(A_0) \cap X(A_1) = \varnothing$

тогда по аксиоме выбора $\exists f.f \in \times\mathcal{A}$.

Q.E.D.

Обратное утверждение также легко показать.

Теорема. Лемма Цорна

Если задано $\langle M, (\preceq)\rangle$ и для всякого линейно упорядоченного $S \subseteq M$ выполнено $\mathrm{upb}_M S \neq \varnothing$, то в M существует максимальный элемент.

Теорема Цермело

На любом множестве можно задать полный порядок.

Теорема:

У любой сюръективной функции существует частичная обратная.

Теорема

Аксиома выбора $\Rightarrow$ лемма Цорна: без доказательства.

3.2 Начальный отрезок

def:

Назовём (для данного раздела) упорядоченным множеством пару $\langle S, (\prec_S)\rangle$. Отношение порядка $(\prec_S)$ может быть как строгим, так и нестрогим. Будем говорить, что $\langle S, (\prec_S)\rangle$ — начальный отрезок $\langle T, (\prec_T)\rangle$, если:

- $S \subseteq T$;
- если $a, b \in S$, то $a \prec_S b$ тогда и только тогда, когда $a \prec_T b$;
- если $a \in S$, $b \in T \setminus S$, то $a \prec_T b$.

Будем обозначать это как $\langle S, (\prec_S)\rangle \sqsubseteq \langle T, (\prec_T)\rangle$ или как $S \sqsubseteq T$, если порядок на множествах понятен из контекста.

Теорема.

Отношение «быть начальным отрезком» является отношением нестрогого порядка.

Теорема о верхней грани Если семейство упорядоченных множеств X линейно упорядочено отношением «быть начальным отрезком», то у него есть верхняя грань.

Доказательство:

Пусть $M = \cup\{T | \langle T, (\prec)\rangle \in X\}$ и $(\prec)_M = \cup\{(\prec) | \langle T, (\prec)\rangle \in X\}$.

Покажем, что если $\langle A, (\prec_A)\rangle \in X$, то $A \sqsubseteq M$. Рассмотрим определение:

- $A \subseteq M$ — выполнено по построению M;
- если $a, b \in A$, то $a \prec_A b$ влечёт $a \prec_M b$ (по построению M). Если же $a \prec_M b$, но $a \not\prec_A b$, то существует A', что $a, b \in A'$ и $a \prec_{A'} b$. Тогда $A \not\sqsubseteq A'$ и $A' \not\sqsubseteq A$, что невозможно по линейности порядка;
- если $a \in A$, $b \in M \setminus A$, то найдётся B, что $b \in B$, отчего $a \prec_B b$ (так как $A \sqsubseteq B$) и $a \prec_M b$ (по построению M).

Тогда $\langle M, (\prec_M)\rangle$ — требуемая верхняя грань.

Q.E.D.

Теорема.

Лемма Цорна $\Rightarrow$ теорема Цермело

Пусть выполнена лемма Цорна и дано некоторое X. Покажем, что на нём можно ввести полный порядок.

- Пусть $S = \{\langle P, (\prec)\rangle \mid P \subseteq X, (\prec) — \text{полный порядок}\}$. Например, для $X = \{0, 1\}$ множество $S = \{\langle\varnothing, \varnothing\rangle, \langle\{0\}, \varnothing\rangle, \langle\{1\}, \varnothing\rangle, \langle X, 0 \prec 1\rangle, \langle X, 1 \prec 0\rangle\}$
- Введём порядок на S как $(\sqsubseteq)$. Заметим, что это — частичный, но не линейный порядок. Например, $\langle X, 0 \prec 1\rangle$ несравним с $\langle X, 1 \prec 0\rangle$.
- По теореме о верхней грани любое линейно упорядоченное подмножество $\langle T, (\sqsubseteq)\rangle$ (где $T \subseteq S$) имеет верхнюю грань.

  Например, для $\{\langle\varnothing, \varnothing\rangle, \langle\{0\}, \varnothing\rangle, \langle X, 0 \prec 1\rangle\}$ это $\langle X, 0 \prec 1\rangle$.
- По лемме Цорна тогда есть $\langle R, (\sqsubseteq_R)\rangle = \max S$. Заметим, что $R = X$, потому что иначе пусть $a \in X \setminus R$. Тогда положив $M = \langle R \cup \{a\}, (\sqsubseteq_R) \cup \{x \prec a \mid x \in R\}\rangle$ получим, что M тоже вполне упорядоченное (и потому $M \in S$), значит, R не максимальное.

Теорема Цермело $\Rightarrow$ существование обратной $\Rightarrow$ аксиома выбора

Теорема Цермело $\Rightarrow$ у сюръективных функций существует частичная обратная.

Доказательство:

Рассмотрим сюръективную $f : A \to B$. Рассмотрим семейство $R_b = \{a \in A \mid f(a) = b\}$. Построим полный порядок на каждом из R_b. Тогда $f^{-1}(b) = \min R_b$.

Теорема.

Существует частичная обратная у сюръективных функций $\Rightarrow$ существует трансверсаль у семейства непустых дизъюнктных множеств.

Доказательство:

Пусть дано семейство непустых дизъюнктных множеств $\mathcal{A}$. Рассмотрим $f : \cup\mathcal{A} \to \mathcal{A}$, что $f(a) = \cup\{A \in \mathcal{A} \mid a \in A\}$. Поскольку элементы $\mathcal{A}$ дизъюнктны, $f(a) \in \mathcal{A}$ при всех a. Тогда существует $f^{-1} : \mathcal{A} \to \cup\mathcal{A}$. Тогда $\{f^{-1}(A) \mid A \in \mathcal{A}\} \in \times\mathcal{A}$.

Q.E.D

3.3 Равенство и функции

Пусть $A_0 = \{0, 1, 3, 5\}$ и $A_1 = \{3, 5, 1, 0, 0, 5, 3\}$. Верно ли, что $A_0 = A_1$?

Да, так как $\forall x.x \in \{0, 1, 3, 5\} \leftrightarrow x \in \{3, 5, 1, 0, 0, 5, 3\}$.

Конгруэнтность

Если $f : A \to B$, также $a, b \in A$ и $a = b$, то $f(a) = f(b)$.

Доказательство:

Пусть $F \subseteq A \times B$ — график функции f.

По определению функции, $\forall x.\forall y_1.\forall y_2.\langle x, y_1\rangle \in F \,\&\, \langle x, y_2\rangle \in F \to y_1 = y_2$.
Также, если $f(a) = y_1$, $f(b) = y_2$, то $\langle a, y_1\rangle \in F$ и $\langle b, y_2\rangle \in F$.
Тогда: $\langle a, y_1\rangle = \langle b, y_1\rangle = \langle b, y_2\rangle = \langle a, y_2\rangle$, то есть $f(a) = y_2 = f(b)$.

Q.E.D.

3.4 Теорема Диаконеску

Если рассмотреть ИИП с ZFC, то для любого P выполнено $\vdash P \vee \neg P$.

Доказательство:

Рассмотрим $\mathcal{B} = \{0, 1\}$, $A_0 = \{x \in \mathcal{B} | x = 0 \vee P\}$ и $A_1 = \{x \in \mathcal{B} | x = 1 \vee P\}$. $\{A_0, A_1\}$ — семейство непустых множеств, и по акс. выбора существует $f : \{A_0, A_1\} \to \cup A_i$, что $f(A_i) \in A_i$. (Если P, то $A_0 = A_1$ и $\{A_0, A_1\} = \{\mathcal{B}\}$).

$\vdash f(A_0) \in A_0 \,\&\, f(A_1) \in A_1$	а.выбора: $f(A_i) \in A_i$
$\vdash f(A_0) \in \mathcal{B} \,\&\, (f(A_0) = 0 \vee P) \,\&\, f(A_1) \in \mathcal{B} \,\&\, (f(A_1) = 1 \vee P)$	а.выделения
$\vdash (f(A_0) = 0 \,\&\, f(A_1) = 1) \vee P$	Удал. (&) + дистр.
$\vdash P \vee f(A_0) \neq f(A_1)$	$0 \neq 1$ и транз.
$\vdash P \to A_0 = A_1$	Определение A_i
$\vdash A_0 = A_1 \to f(A_0) = f(A_1)$	Конгруэнтность
$\vdash f(A_0) \neq f(A_1) \to \neg P$	Контрапозиция
$\vdash P \vee \neg P$	Подставили

3.5 Слабые варианты аксиомы выбора

Теорема конечного выбора

Если $X_1 \neq \varnothing, \dots, X_n \neq \varnothing$, $X_i \cap X_j = \varnothing$ при $i \neq j$, то $\times\{X_1, \dots, X_n\} \neq \varnothing$.

Доказательство:

- База: $n = 1$. Тогда $\exists x_1.x_1 \in X_1$, поэтому $\exists x_1.\{x_1\} \in \times\{X_1\}$.
- Переход: $\exists v.v \in \times\{X_{1,n}\} \to \exists x_{n+1}.x_{n+1} \in X_{n+1} \to v \cup \{x_{n+1}\} \in \times(X_{1,n} \cup \{X_{n+1}\})$

Аксиома счётного выбора

Для счётного семейства непустых множеств существует функция, каждому из которых сопоставляющая один из своих элементов

Аксиома зависимого выбора

Если $\forall x \in E.\exists y \in E.xRy$, то существует последовательность $x_n : \forall n.x_n R x_{n+1}$

Заметим, что семейство $\{A_0, A_1\}$ из теоремы Диаконеску в ИИП не является конечным (равно как и бесконечным). **def:** Конечное множество — равномощное некоторому конечному кардинальному числу.

- Какова мощность семейства?
- 1, если P, и 2, если $\neg P$.
- Но поскольку $P \vee \neg P$ не выполнено в ИИП, мы не можем доказать, что мощность семейства 1 или 2.
- Поэтому мы не можем воспользоваться теоремой конечного выбора.

3.6 Наследственные фундированные множества

def: **Наследственным свойством множества** назовём такое свойство, которым обладает как само множество, так и все его подмножества.

def: **Фундированным множеством** назовём такое, которое не пересекается хотя бы с одним своим элементом.

3.7 Каковы возможные модели для теории множеств?

def: *Универсум фон Неймана* V — все наследственные фундированные множества.

При наличии аксиомы фундирования можно показать, что $V = \cup_a V_a$, где:

$$V_a = \begin{cases} \varnothing, & a = 0 \\ \mathcal{P}(V_b), & a = b' \\ \bigcup_{b<a}(V_b), & a \text{ — предельный} \end{cases}$$

def: *Конструктивный универсум* $L = \cup_a L_a$, где:

$$L_a = \begin{cases} \varnothing, & a = 0 \\ \{\{x \in L_b \mid \varphi(x, t_1, \dots, t_k)\} \mid \varphi \text{ — формула}, t_i \in L_b\}, & a = b' \\ \bigcup_{b<a}(L_b), & a \text{ — пред.} \end{cases}$$

3.8 Усиление аксиомы выбора

def: Аксиома конструктивности: $V = L$, то есть допустимы только те фундированные множества, которые задаются формулами.

Теорема. Аксиома выбора и континуум-гипотеза следуют из аксиомы конструктивности

Для некоторых теорий аксиома слишком сильна.

3.9 Заключительный обзор

Конструктивность теории — насколько легко строить сложные объекты в ней:

1. Неконструктивные теории допускают доказательства чистого существования произвольных по сложности объектов.
2. Конструктивные теории: требуют процесс построения (желательно конечный или хотя бы счётный), состоящий из интуитивно понятных шагов.

Аксиома выбора и её рассмотренные варианты влияют на её конструктивность:

1. КИП + ЦФ + Акс. выбора: менее конструктивна. Например, возможно показать существование разбиения шара на 5 частей, из которых можно составить два шара, равных исходному (теорема Банаха-Тарского). Интуитивно нарушается аддитивность объёма (формального парадокса нет).
2. КИП + ЦФ
3. ИИП + ЦФ: более конструктивна. Она проще формализуется с помощью компьютера, но мат. анализ в ней сложнее и довольно сильно отличается от классического.

4 Лекция 13.

4.1 Два вида норм индукции

def: Принцип математической индукции

Какое бы ни было $\varphi(x)$, если $\varphi(0)$ и при всех x выполнено $\varphi(x) \to \varphi(x')$, то при всех x выполнено и само $\varphi(x)$.

def: Принцип полной математической индукции

Какое бы ни было $\psi(x)$, если $\psi(0)$ и при всех x выполнено $(\forall t.t \le x \to \psi(t)) \to \psi(x')$, то при всех x выполнено и само $\psi(x)$.

Теорема. Принципы математической индукции эквивалентны

Доказательство:

$(\Rightarrow)$ взяв $\varphi := \psi$, имеем выполненность $\varphi(x) \to \varphi(x')$, значит, $\forall x.\psi(x)$.

$(\Leftarrow)$ возьмём $\psi(x) := \forall t.t \le x \to \varphi(t)$.

4.2 Наследственные подмножества

def: Назовём **вполне упорядоченное отношением** $(\in)$ множество S наследственным подмножеством A, если $\forall x.x \in A \to (\forall t.t \in x \to t \in S) \to x \in S$.

Теорема. Единственным наследственным подмножеством вполне упорядоченного множества является оно само.

Доказательство:

Пусть $B \subseteq A$ — наследственное и $B \ne A$. Тогда существует $a = \min(A \setminus B)$. Тогда $(\forall t.t \in a \to t \in B) \to a \in B$ по наследственности B, и выполнено $\forall t.t \in a \to t \in B$ (по минимальности a). Значит, $a \in B$.

Q.E.D.

4.3 Трансфинитная индукция

Теорема.Ограниченная трансфинитная индукция Если для $\varphi(x)$ (некоторого утверждения теории множеств) и некоторого ординала ε (ограничения) выполнено $\forall x.x \in \varepsilon \to (\forall t.t \in x \to \varphi(t)) \to \varphi(x)$, то $\forall x.x \in \varepsilon \to \varphi(x)$.

Доказательство:

Рассмотрим $S = \{x \in \varepsilon \mid \varphi(x)\}$. Тогда $x \in S$ равносильно $x \in \varepsilon \,\&\, \varphi(x)$. Тогда перепишем: $\forall e.e \in \varepsilon \to (\forall x.x \in e \to x \in S) \to e \in S$. Отсюда по теореме о наследственных множествах $S = \varepsilon$.

Q.E.D.

Теорема. Неограниченная трансфинитная индукция

Если для $\varphi(x)$ (некоторого утверждения теории множеств) выполнено $\forall x.\text{ординал}(x) \to (\forall t.t \in x \to \varphi(t)) \to \varphi(x)$, то $\forall x.\text{ординал}(x) \to \varphi(x)$.

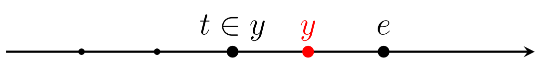
Теорема. Альтернативная формулировка.

Для ординала ε подмножество $S \in \varepsilon$ — наследственное, если и только если одновременно:
Если $x \in \varepsilon$ и $x = \varnothing$, то $x \in S$;
Если $x \in \varepsilon$ и существует y: $y' = x$, то $y \in S \to x \in S$;
Если $x \in \varepsilon$ и x — предельный, то $(\forall t.t \in x \to t \in S) \to (x \in S)$.

Доказательство:

$(\Rightarrow)$ очевидно. Докажем $(\Leftarrow)$: пусть S не наследственное: $E := \{e \in \varepsilon \mid (\forall t.t \in e \to t \in S) \& e \notin S\}$ и $E \neq \varnothing$. Тогда пусть $e = \min E$.

1. $e = \varnothing$ или предельный. Тогда $(\forall t.t \in e \to t \in S) \to (e \in S)$.
2. $e = y'$. Тогда $y \in \varepsilon$ (ε — ординал) и $(\forall t.t \in y \to t \in S) \to (y \in S)$ (так как e минимальный, для которого S не наследственное). По условию, $(y \in S) \to (e \in S)$, отсюда $(\forall t.t \in e \to t \in S) \to (e \in S)$.



Q.E.D.

Пример применения: $\alpha \cdot \alpha = \alpha$ при $\alpha \geq \aleph_0$

Теорема. Если α — кардинальное число, $\alpha \geq \aleph_0$, то $\alpha \cdot \alpha = \alpha$.

Доказательство:

Трансфинитная индукция: $\varphi(x) := x < \omega \lor x \cdot x = x$

1. База: $x = \varnothing$. Тогда $\varphi(\varnothing) \equiv \varnothing < \omega \lor |\varnothing \times \varnothing| = \varnothing$, что доказуемо.
2. Переход: $\forall y.y < x \to \varphi(y)$, тогда $\varphi(x)$. Три случая:
   (a) $x < \omega$. Тогда $\varphi(x)$ истинно (аналогично базе).
   (b) $x = \omega$. Счётный случай (рассмотрим отдельно).
   (c) $x > \omega$. Общий случай (рассмотрим отдельно).

Счётный случай: $\omega < \omega \lor |\omega \cdot \omega| = \omega$

Тогда $\omega \times \omega$ упорядочим так: $\langle p, q\rangle \prec \langle s, t\rangle$, если

1. $\max(p, q) < \max(s, t)$
2. $\max(p, q) = \max(s, t)$ и $q < t$
3. $\max(p, q) = \max(s, t)$, $q = t$ и $p < s$

Очевидно, можно построить биекцию между так упорядоченными значениями и ω.

12 $\langle 0, 3\rangle$	13 $\langle 1, 3\rangle$	14 $\langle 2, 3\rangle$	15 $\langle 3, 3\rangle$
6 $\langle 0, 2\rangle$	7 $\langle 1, 2\rangle$	8 $\langle 2, 2\rangle$	11 $\langle 3, 2\rangle$
2 $\langle 0, 1\rangle$	3 $\langle 1, 1\rangle$	5 $\langle 2, 1\rangle$	10 $\langle 3, 1\rangle$
0 $\langle 0, 0\rangle$	1 $\langle 1, 0\rangle$	4 $\langle 2, 0\rangle$	9 $\langle 3, 0\rangle$

Общий случай: $|\alpha \cdot \alpha| = \alpha$

Аналогично счётному случаю, $\alpha \times \alpha$ упорядочим так: $\langle p, q\rangle \prec \langle s, t\rangle$, если

1. $p \cup q < s \cup t$
2. $p \cup q = s \cup t$ и $q < t$
3. $p \cup q = s \cup t$, $q = t$ и $p < s$

- Легко заметить, что это — линейный порядок (показав, что $p \not\prec q$ и $q \not\prec p$ влечёт $p = q$)
- ... и полный порядок. Найти наименьший в $S \neq \varnothing$ возможно, рассмотрев $m_1 := \min\{p \cup q \mid \langle p, q\rangle \in S\}$ и $M_1 := \{\langle p, q\rangle \mid \langle p, q\rangle \in S, p \cup q = m_1\}$, затем $m_2 := \min\{q \mid \langle p, q\rangle \in M_1\}$, $M_2 := \{\langle p, q\rangle \mid \langle p, q\rangle \in M_1, q = m_2\}$. Тогда требуемым наименьшим в S будет $\min\{p \mid \langle p, q\rangle \in M_2\}$
- Тогда $\langle \alpha \times \alpha, (\prec)\rangle$ соответствует какой-то ординал τ и сохраняющая порядок биекция $t : \tau \to \alpha \times \alpha$.
- Заметим, что $x < \omega$ тогда и только тогда, когда $\cup(\cup t(x)) < \omega$ (очевидно из того, что $|\{z \mid \text{ординал}(z), z < x\}| = |\{p \mid p \prec t(x)\}|$).
- Покажем, что $|\tau| = \alpha$.

Докажем $\tau = \alpha$

Очевидно, что $\tau \geq \alpha$ (так как $|\tau| = |\alpha \times \alpha| \geq \alpha$). Но пусть $\tau > \alpha$.

- Тогда $t(\alpha) = \langle \zeta, \eta\rangle$ определено (у α есть образ).
- Пусть $\sigma := \zeta \cup \eta$. Очевидно, $\langle \zeta, \eta\rangle \preceq \langle \sigma, \sigma\rangle$ и $\sigma \in \alpha$.
- Каков образ t на этом начальном отрезке? $\{t(x) \mid x < \alpha\} \subseteq \{\langle p, q\rangle \mid p, q \leq \sigma\}$. Поэтому $\alpha \leq |(\sigma + 1) \times (\sigma + 1)|$.
- С другой стороны, $\sigma < \alpha$. Поскольку α — кардинал (т.е., в частности, предельный ординал), то $\sigma + 1 < \alpha$ и $|\sigma + 1| < \alpha$.
- По предположению индукции, $|\sigma + 1| < \omega \vee |\sigma + 1| = |\sigma + 1| \cdot |\sigma + 1|$, по свойствам $(\prec)$ имеем $\sigma \geq \omega$.
- Отсюда $\alpha \leq |(\sigma + 1) \times (\sigma + 1)| = |\sigma + 1| < \alpha$, что невозможно.

Q.E.D.

4.4 Теорема о непротиворечивости формальной арифметики

def: Введем исчисление S_∞

1. Язык: связки $\neg$, $\vee$, $\forall$, $=$; нелогические символы: $(+)$,$(\cdot)$,$(')$,0; переменные: x.
2. Аксиомы: все истинные формулы вида $\theta_1 = \theta_2$; все истинные отрицания формул вида $\neg\theta_1 = \theta_2$ (θ_i — термы без переменных).
3. Структурные (слабые) правила:

$$\frac{\zeta \vee \alpha \vee \beta \vee \delta}{\zeta \vee \beta \vee \alpha \vee \delta} \qquad \frac{\alpha \vee \alpha \vee \delta}{\alpha \vee \delta}$$

Сильные правила

$$\frac{\beta}{\alpha \vee \beta} \quad \frac{\neg\alpha \vee \delta \quad \neg\beta \vee \delta}{\neg(\alpha \vee \beta) \vee \delta} \quad \frac{\alpha \vee \delta}{\neg\neg\alpha \vee \delta} \quad \frac{\neg\alpha[x := \theta] \vee \delta}{(\neg\forall x.\alpha) \vee \delta}$$

Формулы в правилах, обозначенные буквами ζ и δ, называются боковыми и могут отсутствовать.

4. Бесконечная индукция:

$$\frac{\alpha[x := \overline{0}] \vee \delta \quad \alpha[x := \overline{1}] \vee \delta \quad \alpha[x := \overline{2}] \vee \delta \quad \dots}{(\forall x.\alpha) \vee \delta}$$

5. Сечение:

$$\frac{\zeta \vee \alpha \qquad \neg\alpha \vee \delta}{\zeta \vee \delta}$$

Здесь α — секущая формула, число связок в $\neg\alpha$ — степень сечения.
В отличие от других правил, в правиле сечения хотя бы одна из боковых формул ζ или δ должна присутствовать.

1. Доказательства образуют деревья.
2. Каждой формуле в дереве сопоставим порядковое число (ординал).
3. Порядковое число заключения любого неструктурного правила строго больше порядкового числа его посылок (больше или равно в случае структурного правила).

$$\cfrac{\cfrac{(\neg 1 = 0)_1 \quad (\neg 2 = 0)_2 \quad (\neg 3 = 0)_4 \quad (\neg 4 = 0)_8 \dots}{(\forall x.\neg x' = 0)_\omega}}{(\neg\neg\forall x.\neg x' = 0)_{\omega+1}}$$

4. Существует конечная максимальная степень сечения в дереве (назовём её степенью вывода).

Теорема. Если $\vdash_{\text{фа}} \alpha$, то $\vdash_\infty |\alpha|_\infty$

Обратное неверно:

$$\frac{\neg\omega_1(\overline{0}, \overline{\ulcorner\sigma\urcorner}) \qquad \neg\omega_1(\overline{1}, \overline{\ulcorner\sigma\urcorner}) \qquad \neg\omega_1(\overline{2}, \overline{\ulcorner\sigma\urcorner}) \qquad \dots}{\forall x.\neg\omega_1(x, \overline{\ulcorner\sigma\urcorner})}$$

Теорема Если Ф.А. противоречива, то противоречива и S_∞

4.5 Обратимость правил де Моргана, отрицания, бесконечной индукции

$$\frac{\neg(\alpha \vee \beta) \vee \delta}{\neg\alpha \vee \delta \quad \neg\beta \vee \delta} \quad \frac{\neg\neg\alpha \vee \delta}{\alpha \vee \delta} \quad \frac{(\forall x.\alpha) \vee \delta}{\alpha[x := \overline{0}] \vee \delta \quad \alpha[x := \overline{1}] \vee \delta \quad \alpha[x := \overline{2}] \vee \delta \quad \dots}$$

Доказательство:

Например, формула вида $\neg\neg\alpha \vee \delta$.

Проследим историю $\neg\neg\alpha$; она могла быть получена:

1. ослаблением — заменим $\neg\neg\alpha$ на α в этом узле и последующих.
2. отрицанием — выбросим правило, заменим $\neg\neg\alpha$ на α в последующих.

Изменённый вывод — доказательство требуемого.

$$\begin{tikzcd}
\delta(0) \arrow[d] & \alpha \vee \delta(2) \arrow[d] \arrow[dd, bend right] & \\
\neg\neg\alpha \vee \delta(0) \arrow[dr] & \neg\neg\alpha \vee \delta(2) \arrow[d] & \dots \arrow[dl] \\
& \neg\neg\alpha \vee \forall x.\delta(x) &
\end{tikzcd}$$

Q.E.D.

4.6 Устранение сечений

Теорема Если α имеет вывод степени $m > 0$ порядка t, то можно найти вывод степени строго меньшей m с порядком 2^t.

Доказательство:

Трансфинитная индукция. Пусть для всех деревьев порядка $t_1 < t$ условие выполнено. Покажем, что оно выполнено для порядка t. Рассмотрим заключительное правило. Это может быть...

1. Не сечение.
2. Сечение, секущая формула — элементарная.
3. Сечение, секущая формула — $\neg\alpha$.
4. Сечение, секущая формула — $\alpha \vee \beta$.
5. Сечение, секущая формула — $\forall x.\alpha$.

4.6.1 Случай 1. Не сечение

$$\frac{(\pi_0)_{t_0} \quad (\pi_1)_{t_1} \quad (\pi_2)_{t_2} \quad \dots}{(\alpha)_t}$$

Заменим доказательства посылок $(\pi_i)_{t_i}$ на $(\pi'_i)_{2^{t_i}}$ по индукционному предположению.

1. Поскольку степени посылок $m'_i < m_i$, то $\max m'_i < \max m_i$.
2. Поскольку $t_i \leq t$, то $2^{t_i} \leq 2^t$.

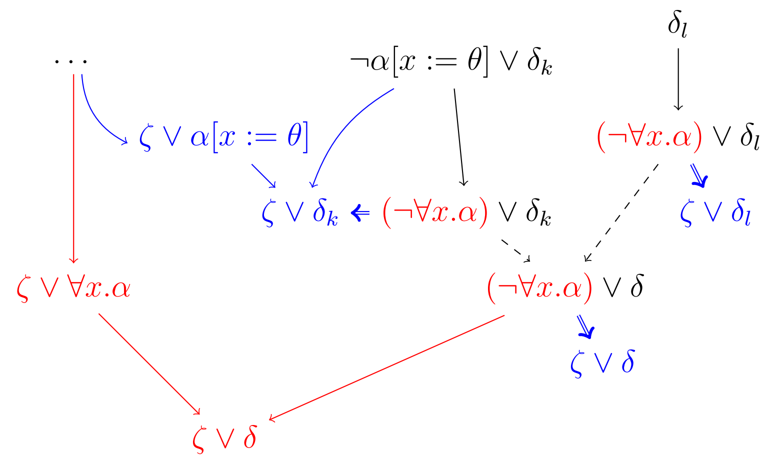
4.6.2 Случай 5. Сечение с формулой вида $\forall x.\alpha$

$$\frac{\zeta \vee \forall x.\alpha \qquad (\neg\forall x.\alpha) \vee \delta}{\zeta \vee \delta}$$

Причём степень и порядок выводов компонент, соответственно, (m_1, t_1) и (m_2, t_2).

1. По индукции, вывод $\zeta \vee \forall x.\alpha$ можно упростить до $(m_1', 2^{t_1})$.
2. По обратимости, можно построить вывод $\zeta \vee \alpha[x := \theta]$ за $(m_1', 2^{t_1})$.
3. В формуле $(\neg\forall x.\alpha) \vee \delta$ формула $\neg\forall x.\alpha$ получена либо ослаблением, либо квантификацией из $\neg\alpha[x := \theta_k] \vee \delta_k$.
   (a) Каждое правило квантификации заменим на:
   $$\frac{\zeta \vee \alpha[x := \theta_k] \qquad (\neg\alpha[x := \theta_k]) \vee \delta_k}{\zeta \vee \delta_k}$$
   (b) Остальные вхождения $\neg\forall x.\alpha$ заменим на ζ (в правилах ослабления).
4. В получившемся дереве меньше степень — так как в $\neg\alpha[x := \theta]$ меньше связок, чем в $\neg\forall x.\alpha$.

4.6.3 Случай 5. Как перестроим доказательство



4.7 Теорема об устранении сечений

def: Итерационная экспонента

$$(a\uparrow)^m(t) = \begin{cases} t, & m = 0 \\ a^{(a\uparrow)^{m-1}(t)}, & m > 0 \end{cases}$$

Теорема. Если $\vdash_\infty \sigma$ степени m порядка t, то найдётся доказательство без сечений порядка $(2\uparrow)^m(t)$

Доказательство: В силу конечности m воспользуемся индукцией по m и теоремой об уменьшении степени.

4.8 Порядок трансфинитной индукции

def: ε_0 — неподвижная точка $\varepsilon_0 = \omega^{\varepsilon_0}$

Иначе говоря, $\varepsilon_0 = \{\omega, \omega^\omega, \omega^{\omega^\omega}, (\omega\uparrow)^3(\omega), (\omega\uparrow)^4(\omega), \dots\}$.

Очевидно, что теорема об устранении сечений может быть доказана трансфинитной индукцией до ординала ε_0 (максимальный порядок дерева вывода, при правильной нумерации вершин).

4.9 Непротиворечивость формальной арифметики

Лемма. Если $\vdash_\infty \alpha$ и $\vdash_\infty \neg\alpha$, тогда $\vdash_\infty \neg 0 = 0$.

Теорема. $\nvdash_\infty \neg 0 = 0$

Доказательство:

Пусть $\vdash_\infty \neg 0 = 0$, устраним сечения и рассмотрим заключительное правило.

1. Правило де Моргана? Нет отрицаний дизъюнкции $(\neg(\alpha \vee \beta) \vee \delta)$.
2. Отрицание? Нет двойного отрицания $(\neg\neg\alpha \vee \delta)$.
3. Бесконечная индукция или квантификация? Нет квантора.
4. Ослабление? Нет дизъюнкции $(\alpha \vee \beta)$, хотя β обязана присутствовать.
5. Сечение? Исключено по условию.

То есть, неизбежно, $\neg 0 = 0$ — аксиома, что также неверно.

5 Лекция 14.

5.1 Метод резолюции

Дана формула α.

1. Упростим формулу — поверхностные кванторы всеобщности, сколемизация.

   Умеем строить формулу β:

$$\beta := \forall x_1.\forall x_2.\forall x_k.\delta_1(x_1, \dots, x_k) \& \dots \& \delta_n(x_1, \dots, x_k)$$

   α доказуема тогда и только тогда, когда при всех оценках предикатных и функциональных символов найдётся значение сколемовских функций e_k, при которых β всегда истинна (слоёный пирог из кванторов).

2. Упрощаем предметное множество — заменили произвольный D на эрбранов универсум H. Выполнимость формулы эквивалентна выполнимости на эрбрановом универсуме.

3. Осталось избавиться от кванторов всеобщности и организовать правильный перебор (эрбранов универсум может быть бесконечным).

def: Эрбранов универсум H_φ — всевозможные комбинации функциональных символов из формулы φ. Если в формуле нет нульместных функциональных символов, к множеству символов формулы добавляется свежий нульместный функциональный символ a и все комбинации с его участием.

Например, для $P(0) \vee (P(x) \rightarrow P(x'))$ эрбрановым универсумом будет $\{0, 0', 0'', 0''', \dots\}$, для $P(x')$ это будет $\{a, a', a'', a''', \dots\}$.

def: Если φ — бескванторная формула, то её эрбранова оценка задаётся как $\langle H_\varphi, F, P, E\rangle$, функции F определяются как текстовые подстановки $[\![f(\theta)]\!] = “f(“ + +[\![\theta]\!] + +“)“$, предикаты P задаются перечислением истинных.

Например, для $P(0) \vee (P(x) \rightarrow P(x'))$ эрбранова оценка при истинных предикатах $\{P(0'), P(0''), P(0'''')\}$ такова: $[\![\varphi]\!]^{x:=0} =$ И и $[\![\varphi]\!]^{x:=0''} =$ Л.

5.2 Противоречивые системы дизъюнктов

Теорема о выполнимости.

Формула выполнима тогда и только тогда, когда она выполнима в какой-то эрбрановой оценке.

Доказательство:

Доказано на предыдущей лекции.

def: Система дизъюнктов $S = \{\delta_1, \dots, \delta_n\}$ противоречива, если для каждой оценки $M = \langle D, P, F, E\rangle$ найдётся δ_t и такой набор $\overline{d} \in D$, что $[\![\delta_t]\!]^{\overline{x}:=\overline{d}} =$ Л.

Теорема. Система дизъюнктов противоречива, если она невыполнима в эрбрановых оценках.

5.3 Основные примеры

Рассмотрим сколемизированную формулу β в КНФ. Заметим, что если $\beta = \forall x_1. \dots .\forall x_k.\delta_1 \mathbin{\&} \delta_2 \mathbin{\&} \dots \mathbin{\&} \delta_n$, то

$$\vdash \beta \leftrightarrow (\forall x_1. \dots .\forall x_k.\delta_1) \mathbin{\&} \dots \mathbin{\&} (\forall x_1. \dots .\forall x_k.\delta_n)$$

def: Дизъюнкт с подставленными значениями из эрбранового универсума H_β вместо переменных называется основным примером формулы β.

def: Система основных примеров — все основные примеры, опровергаемые хоть при какой-то эрбрановой оценке $\mathcal{M}$:

$$\mathcal{E}_S = \{\delta_t[\overline{x} := \overline{d}] \mid \text{существует } \mathcal{M}\text{, что } [\![\delta_t[\overline{x} := \overline{d}]]\!]_\mathcal{M} = \text{Л}; \quad d_i \in H_\beta\}$$

5.4 Противоречивые множества основных примеров

def: Система основных примеров E противоречива в эрбрановой оценке (интерпретации), если для любой эрбрановой оценки M найдётся такой $\varepsilon \in E$, что $[\![\varepsilon]\!]_M = \text{Л}$.

Теорема.

Система дизъюнктов S противоречива тогда и только тогда, когда система её всевозможных основных примеров $\mathcal{E}_S$ противоречива в эрбрановой интерпретации.

5.5 Теорема Эрбрана

Теорема Гёделя о компактности

Если Γ — некоторое семейство бескванторных формул, то Γ имеет модель тогда и только тогда, когда любое его конечное подмножество имеет модель.

Теорема Эрбрана

Система дизъюнктов S противоречива тогда и только тогда, когда у $\mathcal{E}_S$ существует конечное противоречивое в эрбрановой интерпретации подмножество.

Доказательство:

($\Leftarrow$) Пусть $\{\varepsilon_1, \dots, \varepsilon_t\} \subseteq \mathcal{E}_S$ противоречиво, $\varepsilon_i = \delta_{m_i}[\overline{x} := \overline{d_i}]$, где $\overline{d_i}$ — набор значений из H. То есть, для любой эрбрановой оценки M существует ε_p, что $[\![\varepsilon_p]\!]_M = \text{Л}$. Отсюда, по теореме о выполнимости S тоже противоречива.

($\Rightarrow$) Если S противоречива, то $\mathcal{E}_S$ противоречива. Тогда у неё нет модели. Тогда у неё найдётся конечное противоречивое подмножество (компактность). Возможно убедиться в невыполнимости за конечное время.

Общая схема алгоритма

Цель алгоритма: убедиться, что α доказуемо.

1. По формуле α строим её отрицание $\neg\alpha$.
2. Приводим к виду с поверхностными кванторами, проводим сколемизацию, находим КНФ: $\beta = \forall x_1. \dots .\forall x_k.\delta_1 \mathbin{\&} \dots \mathbin{\&} \delta_n$.

3. Убедимся, что при любом D и значениях функциональных и предикатных символов и сколемовских функций e_k найдутся $d_i \in D$, что один из дизъюнктов δ_t при подстановке $\overline{x} := \overline{d}$ ложный.
4. Для этого строим универсум Эрбрана H, и систему основных примеров $\mathcal{E}_S$, её противоречивость эквивалентна невыполнимости β.
5. Конечное противоречивое подмножество обязательно находится в каком-то начальном отрезке $\{\varepsilon_1, \dots, \varepsilon_t\} \subseteq \mathcal{E}_S$ (если оно есть).

Пример: как проверяем выполнимость формулы?

Допустим, формула: $(\forall x.P(x) \,\&\, P(x')) \,\&\, \exists x.\neg P(x'''')$

1. Поверхностные кванторы, сколемизация, КНФ: $(\forall x.P(x)) \,\&\, (\forall x.P(x')) \,\&\, (\neg P(e''''))$
2. Строим эрбранов универсум: $H = \{e, e', e'', e''', \dots\}$
3. Если есть противоречие, то среди основных примеров:

$$\mathcal{E} = \{P(e), P(e'), P(e''), P(e'''), P(e''''), \neg P(e''''), \dots\}$$

Либо есть $\mathcal{M}$, что $[\![\& \,\mathcal{E}]\!]_{\mathcal{M}} = \text{И}$, либо есть $\{\varepsilon_1, \dots, \varepsilon_n\} \subseteq \mathcal{E}$, что $[\![\varepsilon_t]\!]_{\mathcal{M}} = \text{Л}$ для какого-то t при каждой эрбрановой оценке $\mathcal{M}$.

Подмножество $\mathcal{E}$	выполнено в оценке	количество оценок
$\{P(e)\}$	$[\![P(e)]\!] = \text{И}$	2 варианта
$\{P(e), P(e')\}$	$[\![P(e)]\!] = [\![P(e')]\!] = \text{И}$	4 варианта
$\dots$		
$\{P(e), \dots, P(e''''), \neg P(e'''')\}$	невыполнимо	32 варианта

5.6 Правило резолюции (исчисление высказываний)

Пусть даны два дизъюнкта, $\alpha_1 \vee \beta$ и $\alpha_2 \vee \neg\beta$. Тогда следующее правило вывода называется правилом резолюции:

$$\frac{\alpha_1 \vee \beta \qquad \alpha_2 \vee \neg\beta}{\alpha_1 \vee \alpha_2}$$

Теорема.

Система дизъюнктов противоречива, если в процессе всевозможного применения правила резолюции будет построено явное противоречие, т.е. найдено два противоречивых дизъюнкта: β и $\neg\beta$.

5.7 Расширение правила резолюции на исчисление предикатов

Заметим, что правило резолюции для исчисления высказываний не подойдёт для исчисления предикатов.

$$S = \{P(x), \neg P(0)\}$$

Здесь $P(x)$ противоречит $\neg P(0)$, но правило резолюции для исчисления высказываний здесь неприменимо, потому что x можно заменять, это не константа:

$$\frac{P(x) \qquad \neg P(0)}{???}$$

Нужно заменять $P(x)$ на основные примеры, и искать среди них. Модифицируем правило резолюции для этого.

5.8 Алгебраические термы

def: Алгебраический терм

$$\theta := x \mid (f(\theta_1, \ldots, \theta_n))$$

где $x-$переменная, $f(\theta_1, \ldots, \theta_n)-$применение функции. Напомним, что константы — нульместные функциональные символы, собственно переменные будем обозначать последними буквами латинского алфавита.

def: Система уравнений в алгебраических термах $\begin{cases} \theta_1 = \sigma_1 \\ \vdots \\ \theta_n = \sigma_n \end{cases}$

где θ_i и σ_i – термы

5.9 Уравнение в алгебраических термах

def: $\{x_i\} = X-$множество переменных, $\{\theta_i\} = T-$множество термов.

def: Подстановка–отображение вида: $\pi_0 : X \to T$, тождественное почти везде (за исключением конечного числа переменных).

$\pi_0(x)$ может быть либо $\pi_0(x) = \theta_i$, либо $\pi_0(x) = x$.

Доопределим $\pi : T \to T$, где

1. $\pi(x) = \pi_0(x)$
2. $\pi(f(\theta_1, \ldots, \theta_k)) = f(\pi(\theta_1), \ldots, \pi(\theta_k))$

Доказательство:

Решить уравнение в алгебраических термах–найти такую наиболее общую подстановку π, что $\pi(\theta_1) = \pi(\theta_2)$. Наиболее общая подстановка — такая, для которой другие подстановки являются её частными случаями.

5.10 Задача унификации

deffdef:

Пусть даны формулы α и β. Тогда решением задачи унификации будет такая наиболее общая подстановка $\pi = \mathcal{U}[\alpha, \beta]$, что $\pi(\alpha) = \pi(\beta)$.

Также, η назовём наиболее общим унификатором.

- Формулы $P(a, g(b))$ и $P(c, d)$ не имеют унификатора (мы считаем, что a, b, c, d — нульместные функции, а g — одноместная функция).
- Проверим формулу на соответствие 11 схеме аксиом:

$$(\forall x.P(x)) \to P(f(t, g(t), y))$$

Пусть $\pi = \mathcal{U}\big[P(x), P(f(t, g(t), y))\big]$, тогда $\pi(x) = f(t, g(t), y)$.

5.11 Правило резолюции для исчисления предикатов

def:

Пусть σ_1 и σ_2 — подстановки, заменяющие переменные в формуле на свежие. Тогда правило резолюции выглядит так:

$$\frac{\alpha_1 \vee \beta_1 \qquad \alpha_2 \vee \neg\beta_2}{\pi(\sigma_1(\alpha_1) \vee \sigma_2(\alpha_2))}\ \pi = \mathcal{U}\big[\sigma_1(\beta_1), \sigma_2(\beta_2)\big]$$

σ_1 и σ_2 разделяют переменные у дизъюнктов, чтобы π не осуществила лишние замены, ведь $\vdash (\forall x.P(x) \& Q(x)) \leftrightarrow (\forall x.P(x)) \& (\forall x.Q(x))$, но $\not\vdash (\forall x.P(x) \vee Q(x)) \to (\forall x.P(x)) \vee (\forall x.Q(x))$.

$$\frac{Q(x) \vee P(x) \quad \neg P(a) \vee T(x)}{Q(a) \vee T(x'')}\ \text{подстановки: } \sigma_1(x) = x', \sigma_2(x) = x'', \pi(x') = a$$

5.12 Метод резолюции

Ищем $\vdash \alpha$.

1. будем искать опровержение $\neg\alpha$.
2. перестроим $\neg\alpha$ в КНФ.
3. будем применять правило резолюции, пока получаем новые дизъюнкты и пока не найдём явное противоречие (дизъюнкты вида β и $\neg\beta$).

Если противоречие нашлось, значит, $\vdash \neg\neg\alpha$. Если нет — значит, $\vdash \neg\alpha$. Процесс может не закончиться.

5.13 SMT-решатели

Обычно требуется не логическое исчисление само по себе, а теория первого порядка. То есть, «Satisfability Modulo Theory», «выполнимость в теории» — вместо SAT, выполнимости.

- Иногда можно вложить теорию в логическое исчисление, даже в исчисление высказываний: $\overline{S_2 S_1 S_0} = \overline{A_1 A_0} + \overline{B_1 B_0}$

$$\begin{array}{ll} S_0 = A_0 \oplus B_0 & C_0 = A_0 \& B_0 \\ S_1 = A_1 \oplus B_1 \oplus C_0 & C_1 = (A_1 \& B_1) \vee (A_1 \& C_0) \vee (B_1 \& C_0) \\ S_2 = C_1 & \end{array}$$

- А можно что-то добавить прямо на уровень унификации / резолюции: Например, можем зафиксировать арифметические функции — и производить вычисления в правиле резолюции вместе с унификацией.

  Тогда противоречие в $\{x = 1 + 3 + 1, \neg x = 5\}$ можно найти за один шаг.

5.14 Уточнённые типы (Refinement types), LiquidHaskell

def: Уточнённый тип — тип вида $\{\tau(x) \mid P(x)\}$, где P — некоторый предикат.

Пример на LiquidHaskell:

```
data [a] <p :: a -> a -> Prop> where
   | []  :: [a] <p>
   | (:) :: h:a -> [a<p h>]<p> -> [a]<p>
```

- `h:a` — голова (h) имеет тип a

- `[a<p h>]<p>` — хвост состоит из значений типа a, уточнённых p — $\{t : a \mid p\ h\ t\}$ (карринг: `a <p h>`).

```
{-@ type IncrList a = [a] <{\xi xj -> xi <= xj}> @-}
{-@ insertSort    :: (Ord a) => xs:[a] -> (IncrList a) @-}
insertSort []     = []
insertSort (x:xs) = insert x (insertSort xs)
```

6 Информация о курсе.

Поток — y2024.
Группы M3232-M3239.
Преподаватель — Штукенберг Дмитрий Григорьевич.

Нам пизда, ребятки.