

Логика и Алгоритмы

Владислав Мозговой

Факультет математики
НИУ Высшая Школа Экономики

Лекторы: Л.Д.Беклемишев, В.Б.Шехтман, А.В.Кудинов,
Д.С.Шамканов.

Весна 2021

Оглавление

1. Теория множеств ZF с Аксиомой выбора	5
1.1 Лекция 1 (01.11.2021)	5
1.2 Лекция 2 (01.12.2021)	5
1.3 Лекция 3 (01.19.2021)	5
1.4 Лекция 4 (01.25.2021)	9
1.5 Лекция 5 (01.26.2021)	11
1.6 Лекция 6 (02.02.2021)	14
1.7 Лекция 7 (02.08.2021)	17
2. Логика Предикатов	21
2.1 Лекция 8 (02.09.2021)	21
2.2 Лекция 9 (02.16.2021)	23
2.3 Лекция 10 (02.22.2021)	27
2.4 Лекция 11 (03.01.2021)	32
3. Теория Моделей	37
3.1 Лекция 12 (03.09.2021)	37
3.2 Лекция 13 (03.1.2021)	38
3.3 Лекция 14 (03.22.2021)	39
3.4 Лекция 15 (03.23.2021)	41
3.5 Лекция 16 (04.05.2021)	42
3.6 Лекция 21 (04.27.2021)	42
4. Алгоритмы	45
4.1 Лекция 22 (05.11.2021)	45
5. Дополнительно	47
Литература	49

Глава 1.

Теория множеств ZF с Аксиомой выбора

1.1. Лекция 1 (01.11.2021)

1.2. Лекция 2 (01.12.2021)

1.3. Лекция 3 (01.19.2021)

Идея: $n - \{\text{натуральные числа, меньшие } n\}$

$$0 = \emptyset, 1 = \{0\} = \{\emptyset\}, 2 = \{0, 1\} = \{\emptyset, \{\emptyset\}\}$$

Обозначения: $0 := \emptyset$. $x + 1 = S(x) := x \cup \{x\}$

Определение (Индуктивное множество). Множество Y называется индуктивным, если $0 \in Y$, $\forall x : (x \in Y \rightarrow x + 1 \in Y)$

Определение (Множество натуральных чисел). Наименьшее по включению (- наименьшее) индуктивное множество называется множеством натуральных чисел и обозначается \mathbb{N}

Утверждение такое множество существует

Теорема 1.3.1 (Принцип математической индукции). Дано некоторое множество A . Если $0 \in A$ и $\forall n \in \mathbb{N} (n \in A \rightarrow n + 1 \in A)$, то $n + 1 \in A$

Обозначение $x < y :\Leftrightarrow x \in y$

Теорема 1.3.2 (Принцип порядковой индукции). Дано некоторое множество A . Если $\forall n \in \mathbb{N} (\forall m < n m \in A \rightarrow n \in A)$, то $\mathbb{N} \subset A$

Теорема 1.3.3 (Принцип минимального элемента). Пусть A – некоторое непустое множество \mathbb{N}

Определение (Вполне упорядоченное множество). Линейно упорядоченное множество называется вполне упорядоченным, если любое его непустое подмножество Y имеет наименьший элемент (обозначается $\min Y$)

Теорема 1.3.4. Отношение $<$ на \mathbb{N} линейно упорядочивает \mathbb{N} . Более того, этот порядок является полным

Замечание

Поскольку $x < y + 1 \Leftrightarrow x < y$ или $x = y$, для любого натурального n , число $n + 1$ является непосредственно следующим за n в смысле порядка $<$

Определение (Последовательность элементов). Последовательность элементов множества A – это функция $\mathbb{N} \rightarrow A$

Теорема 1.3.5 (О рекурсии). Пусть Y – некое множество $y_0 \in Y$ и $h : Y \rightarrow Y$ – любая функция. Тогда существует единственная функция $f : \mathbb{N} \rightarrow Y$, удовлетворяющая для всех $n \in \mathbb{N}$ условию

$$\begin{cases} f(0) = y_0 \\ f(n+1) = h(f(n)) \end{cases}$$

Лемма 1.3.6.

$$\forall n \in \mathbb{N} (n = 0 \vee \exists m \in \mathbb{N} n = m + 1)$$

Доказательство. Даны множество Y , элемент $y_0 \in Y$ и функция $h : Y \rightarrow Y$. Пусть F – множество всех функций $g : m \rightarrow Y$, $m \in \mathbb{N}$, удовлетворяющих условиям на $\text{dom } g$

Любые две функции $g_0, g_1 \in F$ совпадают на пересечении своих областей определения. В противном случае рассмотрим минимальный $k \in \mathbb{N}$ такой, что $g_0(k) \neq g_1(k)$. Поскольку $g_0(0) = y_0 = g_1(0)$, имеем $k \neq 0$. Следовательно $k = s + 1$, причем $g_0(s) = g_1(s)$, поскольку k – минимальный. Отсюда $g_0(k) = g_0(s + 1) = h(g_0(s)) = h(g_1(s)) = g_1(s + 1) = g_1(k)$, противоречие \square

Определение (функциональное множество). Соотв $R \subset A \times B$ функционально, если $\forall a \in A \forall b_1, b_2 \in B ((a, b_1) \in R \wedge (a, b_2) \in R \Leftrightarrow b_1 = b_2)$

Каждая $g : m \rightarrow Y$ есть подмножество $m \times Y \subset \mathbb{N} \times Y$. Рассмотрим множество $f := \bigcup F \subset \mathbb{N} \times Y$ и докажем, что f является искомой функцией $\mathbb{N} \rightarrow Y$

Отношение $f = \bigcup F$ функционально, поскольку любые два элемента совпадают на общей области определения. Свойства (1) очевидно выполняются для f

Докажем тотальность, рассуждая от противного. Рассмотрим минимальное k такое, что $k \notin \text{dom } f$. Имеем $f : k \rightarrow Y$. Можно продолжить f до функции $f_0 : k + 1 \rightarrow Y$, определив $f_0(k) := y_0$, если $k = 0$ и $f_0(k) := h(f(s))$, если $k = s + 1$. Очевидно, что $f_0 \in F$, поэтому $k \in \text{dom } f$, противоречие. Тем самым доказано существование f

Единственность f , как в рассуждении выше, легко следует по принципу наименьшего числа

Теорема доказана

Определение (Сложение). Пусть $s : \mathbb{N} \rightarrow \mathbb{N}$, где $s(n) = n + 1$. Сложение $(+)$ определяется как (единственная) функция $\mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$, удовлетворяющая рекурсивным условиям для всех $n, m \in \mathbb{N}$:

$$\begin{cases} m + 0 = m \\ m + s(n) = s(m + n) \end{cases}$$

Также заметим, что

$$\begin{aligned} m + n &\neq m \oplus n \\ l = m \{k \in \mathbb{N} \mid m + k &\neq m \oplus k\} \\ l = 0 &\Leftrightarrow m + 0 = m = m \oplus 0 \\ l = s(t) = t + 1 &\Leftrightarrow m + l = m + s(t) = s(m + t) = s(m \oplus t) = m \oplus s(t) = m \oplus l \end{aligned}$$

Определение (Умножение). Умножение (\cdot) определяется как (единственная) функция $\mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$, удовлетворяющая рекурсивным условиям для всех $m, n \in \mathbb{N}$:

$$\begin{cases} m \cdot 0 = 0 \\ m \cdot s(n) = m \cdot n + m \end{cases}$$

Доказательство существования функции сложения

Рассмотрим функцию $H : \mathbb{N}^{\mathbb{N}} \rightarrow \mathbb{N}^{\mathbb{N}}$ такую, что $H(G) = s \circ G$. По теореме о рекурсии существует функция $F : \mathbb{N} \rightarrow \mathbb{N}^{\mathbb{N}}$, удовлетворяющая условиям

$$\begin{cases} F(0) = \text{id}_{\mathbb{N}} \\ F(n + 1) = H(F(n)) \end{cases}$$

Положим $m + n = F(n)(m)$, тогда

$$\begin{aligned} m + 0 &= F(0)(m) = \text{id}_{\mathbb{N}}(m) = m \\ m + s(n) &= F(s(n))(m) \\ &= F(n + 1)(m) \\ &= H(F(n))(m) \\ &= (s \circ F(n))(m) \\ &= s(F(n)(m)) \\ &= s(m + n) \end{aligned}$$

Идея: целое число можно представить разностью двух натуральных чисел $m - n$. При этом некоторые пары задают одно и то же число

Множество целых чисел \mathbb{Z} можно ввести, как фактормножество $\mathbb{Z} := (\mathbb{N} \times \mathbb{N}) \setminus \sim_{\mathbb{Z}}$, где отношение эквивалентности $\sim_{\mathbb{Z}}$ задается следующим образом:

$$(m_1, n_1) \sim_{\mathbb{Z}} (m_2, n_2) \Leftrightarrow m_1 + n_2 = n_1 + m_2$$

Идея: рациональное число $q = \frac{m}{n}$ можно рассматривать как пары (m, n) , где $m \in \mathbb{Z}$ и $n \in \mathbb{N} \setminus \{0\}$. Однако, некоторые пары задают одно и то же рациональное число.

Множество рациональных чисел \mathbb{Q} можно ввести, как фактормножество $\mathbb{Q} := (\mathbb{Z} \times (\mathbb{N} \setminus \{0\})) \setminus \sim_{\mathbb{Q}}$, где отношение эквивалентности $\sim_{\mathbb{Q}}$ задается следующим образом:

$$(m_1, n_1) \sim_{\mathbb{Q}} (m_2, n_2) \Leftrightarrow m_1 n_2 = n_1 m_2$$

Простые свойства вполне упорядоченных множеств:

- 1) всякое непустое вполне упорядоченное множество имеет наименьший элемент
- 2) всякий отличный от наибольшего элемент $x \in X$ имеет непосредственного последователя, то есть $\exists y \in X \forall z \in X (x < z \rightarrow y \leq z)$
- 3) всякое ограниченное сверху подмножество имеет точную верхнюю грань

Лемма 1.3.7. Даны вполне упорядоченное множество $(X, <)$ и функция $f : X \rightarrow X$, сохраняющая порядок. Тогда $x \leq f(x)$ для любого $x \in X$

Доказательство. Предположим, что $Y = \{x \in X \mid f(x) < x\}$ не является пустым, и рассмотрим $a = \min Y$. Имеем $f(a) < a$, поскольку $a \in Y$. Следовательно $f(f(a)) < f(a)$ по монотонности f . Тогда $f(a) \in Y$ и $f(a) < a$, что противоречит минимальности a . Заключаем, что Y пусто. \square

Определение (Начальный отрезок). Начальным отрезком множества $(X, <)$ называется такое подмножество $Y \subset X$, для которого

$$\forall x, y \in X (y < x \wedge x \in Y \Rightarrow y \in Y)$$

Обозначение

Для $a \in X$ обозначим $[0, a) = \{x \in X \mid x < a\}$ Наблюдение

Любой собственный начальный отрезок $(X, <)$ имеет вид $[0, a)$ для некоторого $a \in X$

Лемма 1.3.8. Вполне упорядоченное множество не изоморфно никакому собственному начальному отрезку

Доказательство. Допустим, что существуют собственный начальный отрезок $Y \subset X$ и изоморфизм $f : X \rightarrow Y$. Рассмотрим $a \in X \setminus Y$. Имеем $f(a) < a$, поскольку $a \notin Y$, $f(a) \in Y$ и Y – начальный отрезок X . Противоречие с предыдущей леммой. \square

Теорема 1.3.9 (Кантор). Для любых двух вполне упорядоченных множеств одно изоморфно начальному отрезку другого

Доказательство. Возьмем два вполне упорядоченных множества A, B , рассмотрим $R = \{(x, y) \in A \times B \mid [0, x)_A \cong [0, y)_B\}$. Соответствие R функционально и инъективно, то есть является биекцией из $\text{dom } R$ в $\text{ran } R$ \square

1.4. Лекция 4 (01.25.2021)

Теорема 1.4.1 (Кантор). Для любых двух вполне упорядоченных множеств одно изоморфно начальному отрезку другого

Доказательство. Возьмем два вполне упорядоченных множества A, B . Рассмотрим $R = \{(x, y) \in A \times B \mid [0, x)_A \cong [0, y)_B\}$.

Проверим инъективность соответствия R , если $(x_1, y), (x_2, y) \in R$ то $[0, x_1)_A \cong [0, y)_B \cong [0, x_2)_A$. Так как ни одно из множеств не может являться собственным начальным отрезком другого, то $x_1 \not<_A x_2$, $x_2 \not<_A x_1$, откуда $x_1 = x_2$

Аналогично проверяется функциональность соответствия R

Множество $\text{dom } R$ является начальным отрезком A . Действительно, если $x <_A x'$ и $x' \in \text{dom } R$, то $[0, x)_A \subset [0, x')_A$ и существует изоморфизм $g : [0, x')_A \rightarrow [0, y')_B$. Ограничение изоморфизма g на $[0, x)_A - [0, x)_A \cong [0, g(x))_B$, тогда $(x, g(x)) \in R$ и $x \in \text{dom } R$

Соответствие R сохраняет порядок, так как если $x <_A x'$, $(x, y) \in R$, $(x', y') \in R$, $y <_B y'$, иначе $[0, x')_A$ изоморфен своему начальному отрезку

Аналогично $\text{ran } R = \{y \in B \mid \exists x \in A (x, y) \in R\}$ является начальным отрезком в B , и отношение R^{-1} сохраняет порядок

Получается что R – изоморфизм из $\text{dom } R$ в $\text{ran } R$, проверим что $\text{dom } R = A$, $\text{ran } R = B$ Если это не так, рассмотрим $x_0 = \min(A \setminus \text{dom } R)$ и $y_0 = \min(B \setminus \text{ran } R)$, тогда $\text{dom } R = [0, x_0)_A$, $\text{ran } R = [0, y_0)_B$ и $(x_0, y_0) \in R$ – противоречие \square

Идея: трансфинитно продолжим ряд натуральных чисел так, чтобы всякий член ряда был равен множеству предшествующих членов ряда

Обозначение: $x + 1 := x \cup \{x\}$

Определение. Множество T называется транзитивным, если $\bigcup T \subset T$, или эквивалентно $\forall x, y (x \in y \in T \rightarrow x \in T)$

Ординал – транзитивное множество, все элементы которого также транзитивны

Лемма 1.4.2. Всякий элемент ординала – ординал

Доказательство. Пусть α – ординал, то есть транзитивное множество, каждый элемент которого транзитивен

Тогда $\beta \subset \alpha$ в силу транзитивности, тогда каждый элемент β транзитивен и сам тоже транзитивен, а следовательно он ординал \square

Лемма 1.4.3. Для любых ординалов α, β, γ имеем $\alpha \notin \alpha$, $\alpha \in \gamma$ если $\alpha \in \beta$, $\beta \in \gamma$

Доказательство. Предположим что $\alpha \in \alpha$ и рассмотрим $\{\alpha\}$. В нем по аксиоме регулярности должен найтись элемент без α , но такого нет

Рассмотрим ординалы α, β, γ , тогда $\alpha \in \beta \in \gamma$ и по транзитивности $\alpha \in \gamma$ □

Лемма 1.4.4. всякое непустое множество ординалов X содержит \in -минимальный элемент

Доказательство. Через аксиому регулярности □

Лемма 1.4.5. Для любых ординалов α, β верно, что $\alpha \in \beta$, или $\alpha = \beta$, или $\beta \in \alpha$

Доказательство. Допустим, что это не так, то есть существует ординал α , который несравним с некоторым ординалом.

Рассмотрим ординал $\alpha + 1 = \alpha \cup \{\alpha\}$ и его подмножество X , состоящее из тех элементов, которые несравнимы с некоторым ординалом. По предыдущей лемме множество X содержит минимальный α_0 элемент

Пусть β – некоторый ординал, с которым несравним α_0 , рассмотрим $\beta + 1 = \beta \cup \{\beta\}$ и его подмножество Y , состоящее из тех элементов, которые насравнимы с ординалом α_0 . По лемме Y содержит минимальный β_0 , проверим что $\alpha_0 = \beta_0$

Установим вкючение α_0 в β_0 , если $\gamma \in \alpha_0$, $\gamma \in \alpha + 1$ и $\gamma \notin X$, тогда так как α_0 минимальный, то γ сравним со всеми ординалами, а тогда $\gamma \in \beta_0$, так как иначе $\beta_0 \in \alpha_0$, и это противоречие

Установим включение β_0 в α_0 . Если $\delta \in \beta_0$, то $\delta \in \beta + 1$, тогда δ сравним с α_0 и $\delta \in \alpha_0$, так как иначе будет противоречие с несравнимостью α_0 и β_0 □

Обозначение $x < y :\Leftrightarrow x \in y$

Теорема 1.4.6. Класс всех ординалов линейно упорядочен через $<$, а также всякое непустое множество содержит $<$ -наименьший элемент

Следствие 1.4.6.1. Любой ординал α сам как множество вполне упорядочен с помощью $<$ и является начальным отрезком в классе всех ординалов

Теорема 1.4.7 (Трансфинитная индукция). Пусть φ – некоторое свойство множеств. Допустим что для всякого ординала α имеет место $\forall \beta < \alpha \varphi(\beta) \rightarrow \varphi(\alpha)$. Тогда для всех ординалов γ верно $\varphi(\gamma)$

Доказательство. Допустим, что $\varphi(\gamma)$ не выполнено для некоторого ординала γ . Рассмотрим подмножество X множества $\gamma + 1 = \gamma \cup \{\gamma\}$, состоящее из ординалов, которые не удовлетворяют свойству φ . Поскольку множество X непусто, оно содержит $<$ -минимальный элемент α . Получаем, что $\varphi(\alpha)$ верно, поскольку $\varphi(\beta)$ верно для любого $\beta < \alpha$, противоречие □

Теорема 1.4.8 (парадокс Бурали-Форти 1897). Класс всех ординалов не является множеством

Доказательство. Допустим, что существует O , которое в точности содержит все ординалы Тогда O является транзитивным множеством транзитивных множеств, то есть ординалом Следовательно множество $O \in O$, что противоречит иррефлексивности \in . □

Утверждение

Каждое натуральное число и все множество \mathbb{N} – ординалы

Схема аксиом подстановки

Пусть свойство $\varphi(x, y)$ – такое, что для любого множества x найдется не более одного множества y , для которого $\varphi(x, y)$. Тогда для любого X найдется множество $Y = \{y \mid \exists x \in X \varphi(x, y)\}$

Теорема 1.4.9 (Кантор). Пусть $(X, <)$ – вполне упорядоченное множество. Тогда существует единственный ординал α , изоморфный множеству $(X, <)$

Доказательство. Рассмотрим свойство $\varphi(x, y) : x \in X, y$ – ординал, и $[0, x)_X \cong y$.

Видим, что для любого множества x найдется не более одного множества y , для которого имеет место $\varphi(x, y)$.

По аксиоме подстановки найдется множество $Y = \{y \mid \exists x \in X \varphi(x, y)\}$, содержащее те и только те ординалы, которые изоморфны собственным начальным отрезкам $(X, <)$.

Поскольку не существует множества всех ординалов, то найдется ординал α , не лежащий в Y

По теореме Кантора о сравнении вполне упорядоченных множеств, множество $(X, <)$ изоморфно некоторому начальному отрезку α . Поскольку α и все его собственные начальные отрезки являются ординалами, получаем, что $(X, <)$ изоморфно ординалу

Единственность следует из того, что для двух различных ординалов, один является собственным начальным отрезком другого. Следовательно разные ординалы неизоморфны как вполне упорядоченные множества. \square

Определение. Ординал α называется порядковым типом вполне упорядоченного множества $(X, <)$, если он изоморфен $(X, <)$.

Лемма 1.4.10. Всякий ординал α либо имеет вид $\beta + 1$ для некоторого ординала β , либо равен объединению всех предшествующих ординалов $\bigcup \alpha$

Замечание: ординалы вида $\beta + 1$ называются ординалами-последвателями; все остальные ординалы, кроме 0, называются предельными.

1.5. Лекция 5 (01.26.2021)

Определение. Ординал – транзитивное множество, все элементы которого транзитивны

Обозначение: $x < y \Leftrightarrow x \in y$

Теорема 1.5.1. Класс всех ординалов линейно упорядочен с помощью $<$. Более того, всякое множество содержит $<$ -наименьший элемент

Теорема 1.5.2 (Парадокс Бурали-Форти 1897). Не существует множества, состоящего в точности из всех ординалов

Определение. Ординалы вида $\beta + 1$ называются ординалами-последователями. Все остальные ординалы, кроме 0, называются предельными

Замечание: Не существует ординала γ такого, что $\alpha < \gamma < \alpha + 1$

Определение. Пусть ζ – некоторый ординал. Множество g называется ζ -последовательностью, если $g : \zeta \rightarrow X$ для некоторого X .

Такие последовательности также обозначают $(X_\nu)_{\nu < \zeta}$

Определение. Пусть $\varphi(x, y)$ – некоторое свойство множеств, причем для любой трансинитной последовательности x существует не более одного множества y , удовлетворяющего $\varphi(x, y)$. Будем говорить, что трансинитная последовательность g (длины ζ) удовлетворяет рекурсивному условию, заданному φ , если для всякого ординала $\nu < \zeta$ имеет место $\varphi(g \upharpoonright_\nu, g(\nu))$

Теорема 1.5.3. Пусть $\varphi(x, y)$ – некоторое свойство множеств, причем для любой трансинитной последовательности x существует не более одного множества y , удовлетворяющего $\varphi(x, y)$. Тогда выполнено следующее:

- 1) либо для любого ординала α существует единственная α -последовательность, удовлетворяющая рекурсивному условию, заданному φ
- 2) либо существует единственная трансфинитная последовательность g , удовлетворяющая рекурсивному условию, заданному φ , для которой не существует такого y , что $\varphi(g, y)$

Доказательство. Будем говорить, что трансинитная последовательность g (длины ζ) удовлетворяет рекурсивному условию, если для всякого ординала $\nu < \zeta$ имеет место $\varphi(g \upharpoonright_\nu, g(\nu))$

Любые две трансинитные последовательности g_1, g_2 удовлетворяющие рекурсивному условию, совпадают на пересечении своих областей определения. В противном случае рассмотрим \in -минимальный ординал λ такой, что $g_1(\lambda) \neq g_2(\lambda)$. В силу минимальности λ получаем, что $g \upharpoonright_\lambda$

Предположим, что не для всякого ординала α существует α -последовательность, удовлетворяющая рекурсивному условию. Рассмотрим минимальный ординал λ , для которого не существует соответствующей λ -последовательности

Видим, что $\lambda \neq 0$. Проверим, что λ не является предельным ординалом. Рассмотрим условие $\psi(u, v)$: u – ординал, v – u -последовательность, удовлетворяющая рекурсивному условию.

Для всякого u существует не более одного v такого, что верно $\psi(u, v)$. По аксиоме подстановки существует множество $V = \{v \mid \exists u \in \lambda \psi(u, v)\}$. Тогда $\bigcup V$ – λ -последовательность, удовлетворяющая рекурсивному условию. Противоречие.

Следовательно $\lambda = \lambda_0 + 1$ для некоторого ординала λ_0 . По минимальности λ , найдется λ_0 -последовательность g , удовлетворяющая рекурсивному условию. Видим, что не существует такого y , что $\varphi(g, y)$ □

Теорема 1.5.4 (Цермело). Для всякого множества X существует бинарное отношение $<$ на X такое, что $(X, <)$ – вполне упорядоченное множество

Доказательство. Пусть f – функция выбора на семействе всех непустых подмножеств X . Такая функция существует по аксиоме выбора.

Назовем трансфинитную последовательность g хорошей, если $\text{ran } g \subset X$ и $g(a) \neq g(b)$ для любых $a \neq b$ из $\text{dom } g$. Другими словами, хорошая последовательность – трансфинитная последовательность из различных элементов X .

Рассмотрим условие $\varphi(x, y)$: x – хорошая трансфинитная последовательность, для которой $X \setminus \text{ran } x \neq \emptyset$ и $y = f(X \setminus \text{ran } x)$

Видим, что для любой трансфинитной последовательности x существует не более одного множества y , удовлетворяющего $\varphi(x, y)$

Мы находимся в условиях теоремы о трансфинитной рекурсии. Заметим, что любая трансфинитная последовательность, удовлетворяющая рекурсивному условию, заданному φ , является хорошей

Допустим, что для любого ординала α существует единственная α -последовательность, удовлетворяющая рекурсивному условию, заданному φ .

Придем к противоречию, рассмотрев условие $\psi(c, d) : c \in X, d$ – ординал, и для некоторой трансфинитной последовательности g , удовлетворяющей рекурсивному условию, $g(d) = c$

Видим, что для любого множества c существует не более одного множества d , удовлетворяющего условию $\psi(c, d)$. По аксиоме подстановки существует множество $D = \{d \mid \exists c \in X \psi(c, d)\}$. В нашем предположении D является множеством всех ординалов, но такое множество не существует.

Следовательно, существует трансфинитная последовательность g , удовлетворяющая рекурсивному условию, заданному φ , которую нельзя продолжить, то есть не существует такого y , что $\varphi(g, y)$

Поскольку g является хорошей и ее нельзя продолжить, то $X \setminus \text{ran } g = \emptyset$. Другими словами, g является биекцией из некоторого ординала α в X . Тогда полный порядок на X определяется как $\{(a, b) \in X \times X \mid g^{-1}(a) \in g^{-1}(b)\}$ \square

Определение. Кардинал – это такой ординал, который неравномошен никакому меньшему ординалу

Лемма 1.5.5. Для любого множества A существует единственный кардинал, который равномошен A .

Доказательство. $(A, <) \cong \alpha$, рассмотрим ординалы, равномошные $\alpha : K = \min\{\beta \leq \alpha \mid \beta \sim \alpha \sim A\}$ (тогда K – кардинал и он единственен по определению). \square

Определение. Кардинал k называется мощностью множества A , если он равномошен A

Лемма 1.5.6. Любые два множества A, B сравнимы по мощности, то есть $A \lesssim B$ или $B \lesssim A$

1.6. Лекция 6 (02.02.2021)

Определение. Множество g называется трансфинитной последовательностью, если $g : \zeta \rightarrow X$ для некоторого ординала ζ и некоторого множества X

Теорема 1.6.1. Пусть $\varphi(x, y)$ – некоторое свойство множеств, причем для любой трансфинитной последовательности x существует не более одного y , удовлетворяющего $\varphi(x, y)$

Тогда выполнено следующее: 1) либо для любого ординала

Теорема 1.6.2 (Цорн). Пусть $(P, <)$ – частично упорядоченное множество, в котором всякая цепь имеет верхнюю грань. Тогда $(P, <)$ содержит максимальный элемент

Доказательство. Пусть f – функция выбора на семействе всех непустых подмножеств P , она существует по аксиоме выбора

Назовем трансфинитную последовательность g хорошей, если $\text{ran } g \subset P$ и $g(a) < g(b)$ для любых $a < b \in \text{dom } g$

Определение. Назовем строгой верхней гранью множества $A \subset P$ такой элемент $z \in P$, что $a < z$ для любого $a \in A$. Через $b(A)$ обозначим множество всех строгих верхних граней A

Рассмотрим условие $\varphi(x, y) : x$ – хорошая трансфинитная последовательность, для которой $b(\text{ran } x) \neq \emptyset$, и $y = f(b(\text{ran } x))$

Видим, что для любой трансфинитной последовательности x существует не более одного множества y , удовлетворяющего $\varphi(x, y)$

Допустим, что для любого ординала α существует единственная α -последовательность, удовлетворяющая φ

Придем к противоречию, рассмотрев условие $\psi(c, d) : c \in P, d$ – ординал, и для некоторой трансфинитной последовательности g , удовлетворяющей рекурсивному условию, $g(d) = c$

Видим, что для любого множества c существуют не более одного множества d , удовлетворяющего $\psi(c, d)$. По аксиоме подстановки существует множество $D = \{d \mid \exists c \in P \psi(c, d)\}$. В нашем предположении D является множеством всех ординалов, противоречие.

Следовательно существует такая последовательность g , удовлетворяющая φ , которую нельзя продолжить, то есть нет такого y , что $\varphi(g, y)$

Поскольку g является хорошей и g нельзя продолжить, получаем, что $b(\text{ran } g) = \emptyset$. Кроме того, $\text{ran } g$ является цепью в P . Замечаем, что a (верхняя грань для $\text{ran } g$) – искомый максимальный элемент P , поскольку иначе $b(\text{ran } g) \neq \emptyset$ и g можно было бы продолжить \square

Теорема 1.6.3 (Кантора-Бернштейна). Если $A \lesssim B$ и $B \lesssim A$, то $A \sim B$

Следствие 1.6.3.1. 1) Всякое бесконечное множество содержит счетное подмножество
2) Мощность бесконечного множества не меняется при объединении с конечным

3) $\mathbb{N} \sim \mathbb{N} \times \{0, 1\} \sim \mathbb{N} \times \mathbb{N}$

$$(m_1, m_2) < (n_1, n_2) \Leftrightarrow \begin{cases} \max\{m_1, m_2\} < \max\{n_1, n_2\} \\ \max\{m_1, m_2\} = \max\{n_1, n_2\} \text{ и } m_1 < n_1 \\ \max\{m_1, m_2\} = \max\{n_1, n_2\} \text{ и } m_1 = n_1, m_2 < n_2 \end{cases}$$

Лемма 1.6.4. Если множество A бесконечно, то $A \sim A \times \{0, 1\}$

Доказательство. Рассмотрим P , состоящее из пар вида (B, f) , где B – бесконечное подмножество, $f : B \rightarrow B \times 2$ – биекция. Зададим на P частичный порядок

$$(B_1, f_1) \leq (B_2, f_2) \Leftrightarrow B_1 \subset B_2, f_1 = f_2 \upharpoonright_{B_1}$$

Пусть C – произвольная цепь в P является верхней гранью C . Проверим, что P непусто. Бесконечное множество A содержит счетное подмножество D . Поскольку D счетно, ято существует биекция $g : D \rightarrow D \times 2$. Получаем, что пара $(D, g) \in P$ и является верхней гранью C .

Предположим что $C \neq \emptyset$

Рассмотрим $D = \bigcup \{B \mid \exists f (B, f) \in C\}$, то есть объединение всех первых компонент элементов C , и $g = \bigcup \{f \mid \exists B (B, f) \in C\}$, то есть объединение всех вторых компонент

Соответствие $g \subset D \times (D \times 2)$ функционально в силу того, что все вторын компоненты элеметов C попарно совпадают на общих областях определения. Очевидно, что g тотально, а следовательно g – функция.

Функция g инъективна: для различных $d_1, d_2 \in D$ возьмем большее из множеств, которым принадлежат d_1 и d_2 . На нем g является инъекцией по предположению

Кроме того, g – сюръекция, для любой пары возьмем $(d, i) \in D \times 2$ возьмем множество B из которого произошло d и вспомним, что мы имели взаимно однозначное соответствие между ним и $B \times 2$

Мы нахлдимся в условиях леммы Цорна и знаем, что P содержит максимальный элемент (E, h)

Рассмотрим дополнение E до A . Если множество $A \setminus E$ конечно, то $A = (A \setminus E) \cup E \sim E$. Получим $A \sim E \sim E \times 2 \sim A \times 2$, все доказано.

Если множество $A \setminus E$ бесконечно, то оно содержит счетное подмножество E' . Кроме того, существует биекция $h' : E' \rightarrow E' \times 2$

Тогда $h \cup h'$ – биекция из $E \cup E'$ в $(E \cup E') \times 2 = E \times 2 \cup E' \times 2$. Полчим пару $(E \cup E', h \cup h')$ из P , которая больше пары (E, h) , что противоречит максимальнойности (E, h) , этот случай невозможен. \square

Теорема 1.6.5. Объединение двух бесконечных множеств A и B равномощно большему из них

Доказательство. Поскольку любые два множества сравнимы по мощности, можно считать без ограничения общности, что $A \lesssim B$. Тогда $B \lesssim A \cup B \lesssim B \times \{0, 1\} \sim B$. По теореме кантора-Бернштейна получаем что $B \sim A \cup B$ \square

Лемма 1.6.6. Если A бесконечно, то $A \sim A \times A$

Доказательство. Рассмотрим множество P , состоящее из пар вида (B, f) , где B – бесконечное подмножество A , $f : B \rightarrow B \times B$ – биекция. Зададим на P частичный порядок

$$(B_1, f_1) \leq (B_2, f_2) \Leftrightarrow B_1 \subset B_2, f_1 = f_2 \upharpoonright_{B_1}$$

Пусть C – произвольная цепь в P . Убедимся что C имеет верхнюю грань (D, g)

Если $C = \emptyset$, то любой элемент P является верхней гранью C . Проверим, что P непусто. Бесконечное множество A содержит счетное подмножество D . Поскольку D счетно, существует биекция $g : D \rightarrow D \times D$. Получаем, что пара $(D, g) \in P$ и является верхней гранью C .

Теперь предположим, что $C \neq \emptyset$

Рассмотрим $D = \bigcup \{B \mid \exists f (B, f) \in C\}$, то есть объединение всех первых компонент элементов C , и $g = \bigcup \{f \mid \exists B (B, f) \in C\}$, то есть объединение всех вторых компонент.

Как и предыдущем доказательстве, замечаем, что соответствие $g \subset D \times (D \times D)$ является функцией.

Функция g инъективна: для различных $d_1, d_2 \in D$ возьмем большее из множеств, которым принадлежат d_1, d_2 , на нем g является индукцией по предположению

Кроме того, g является сюръекцией: для любой пары $(d_1, d_2) \in D \times D$ возьмем множества B_1, B_2 , из которых произошли d_1, d_2 выберем из этих множеств большее и вспомним, что мы имели взаимно однозначное соответствие между ним и его квадратом

Мы находимся в условиях леммы Цорна и знаем, что P содержит максимальный элемент (E, h) .

Рассмотрим дополнение E до A . Если $A \setminus E \lesssim E$, то $A = (A \setminus E) \cup E \lesssim E$. Получаем, что $A \sim E \sim E \times E \sim A \times A$ и все доказано.

Если $E \lesssim A \setminus E$, то $A \setminus E$ содержит подмножество E' , которое равномощно E .

Если $E \lesssim A \setminus E$, то $A \setminus E$ содержит подмножество E' , которое равномощно E .

Биекцию h из E в $E \times E$ можно продолжить до биекции из $E \cup E'$ в $S = (E \cup E') \times (E \cup E')$, поскольку $E' \sim S \setminus (E \times E)$, действительно

$$S \setminus (E \times E) = (E \times E') \cup (E' \times E') \cup (E' \times E) \sim E \times E \sim E \sim E'$$

Получаем пару из P , которая больше пары (E, h) , что противоречит максимальной (E, h) . Таким образом, этот случай невозможен. \square

Следствие 1.6.6.1. Если множество A бесконечно, то множество всех последовательностей длины $n > 0$, составленных из элементов A , равномощно A , то есть $A^n \sim A$

Следствие 1.6.6.2. Если множество A бесконечно, то множество всех конечных последовательностей, составленных из элементов A , равномножно A , то есть $A^* \sim A$

Доказательство.

$$A^* = \bigcup \{A^n \mid n \in \mathbb{N}\} \sim A \times \mathbb{N} \sim A$$

□

1.7. Лекция 7 (02.08.2021)

Определение. множество называется транзитивным, если $\cup T \subset T$

Лемма 1.7.1. У каждого множества есть транзитивное замыкание

Доказательство. Определим по трансфинитной рекурсии последовательность множеств g такую, что $g(0) = X$, $g(n+1) = \cup g(n)$. Действительно, рассмотрим условие $\varphi(x, y) : x$ – конечная последовательность и

$$y = \begin{cases} X, & \text{если } \text{dom } x = 0 \\ \cup x(n), & \text{если } \text{dom } x = n+1 \end{cases}$$

Последовательность g получается, как единственная непродолжаемая транзитивная последовательность, удовлетворяющая рекурсивному условию, заданному φ .

Положим $T = \bigcup_{n \in \mathbb{N}} g(n) = \bigcup \text{ran } g$. Очевидно, что T – транзитивное и $X \subset T$.

Проверим, что T является \subset -наименьшим из таких множеств.

Предположим, что $X \subset S$ для некоторого транзитивного множества S

Имеем $g(0) = X \subset S$. Кроме того, если $g(m) \subset S$, то $g(m+1) = \cup g(m) \subset \cup S \subset S$

По принципу математической индукции получаем, что $g(m) \subset S$ для любого $m \in \mathbb{N}$

Следовательно, $T = \bigcup_{n \in \mathbb{N}} g(n) \subset S$. Доказали, что T является \subset -наименьшим из транзитивных множеств, содержащих X в качестве подмножества □

Лемма 1.7.2. Объединение семейства транзитивных – транзитивно

Лемма 1.7.3. Пусть X – транзитивно, тогда $X \subset P(X)$ и $P(X)$ транзитивно

Доказательство. Проверим, что $X \subset P(X)$. Если $x \in X$, то $x \subset X$ по транзитивности X . Следовательно $x \in P(X)$

Проверим транзитивность $P(X)$. Если $y \in P(X)$, то $y \subset X \subset P(X)$. Следовательно, $P(X)$ является транзитивным множеством. □

Теорема 1.7.4 (Иерархия фон Неймана). По трансфинитной рекурсии для каждого ординала ξ определим множество \mathbb{V}_ξ так, что $\mathbb{V}_0 = \emptyset$, $\mathbb{V}_{\eta+1} = P(\mathbb{V}_\eta)$, $\mathbb{V}_\lambda = \bigcup_{\eta < \lambda} \mathbb{V}_\eta$. Действительно, рассмотрим условие $\varphi(x, y) : x$ – транзитивная последовательность и

$$y = \begin{cases} \emptyset, & \text{if } \text{dom } x = 0 \\ P(x(\eta)), & \text{if } \text{dom } x = \eta + 1 \\ \cup \text{ran } x \end{cases}$$

Видим, что для любой трансфинитной последовательности x существует ровно одно множество y , удовлетворяющего $\varphi(x, y)$. Мы находимся в условиях теоремы о трансфинитной рекурсии

Получаем, что для любого ординала α существует единственная трансинитная последовательность длины α , удовлетворяющая рекурсивному условию, заданному φ

В силу единственности получающиеся трансинитные последовательности продолжают одна другую.

Множество \mathbb{V}_ξ определяется, как член с номером ξ для некоторой (или любой достаточно длинной) трансфинитной последовательности, удовлетворяющей рекурсивному условию

Так определенный бесконечный ряд множеств \mathbb{V}_ξ называется иерархией фон Неймана

$$\mathbb{V}_0 = \emptyset \mathbb{V}_1 = \{\emptyset\} \mathbb{V}_2 = \{\emptyset, \{\emptyset\}\} \dots$$

Лемма 1.7.5. Для любых ординалов α, β имеет место следующее: \mathbb{V}_α транзитивно, $\mathbb{V}_\beta \subset \mathbb{V}_\alpha$, если $\beta < \alpha$

Доказательство. Оба пункта получаются трансинитой индукцией по ординалу α . Разберем первый пункт

Рассмотрим ординал α такой, что для всех $\gamma < \alpha$ множество \mathbb{V}_{γ} транзитивно. Если $\alpha = 0$, то $\mathbb{V}_0 = \emptyset$ является транзитивным.

Если $\alpha = \alpha_0 + 1$ для некоторого α_0 , то $\mathbb{V}_\alpha = P(\mathbb{V}_{\alpha_0})$. Поскольку \mathbb{V}_{α_0} транзитивно по предположению, множество \mathbb{V}_α транзитивно.

Если α – предельный ординал, то \mathbb{V}_α является объединением транзитивных множеств, и, следовательно транзитивно.

По индукции заключаем, что \mathbb{V}_α транзитивно для любого α .

Чтобы получить утверждение второго пункта, надо индукцией по α доказать, что для всех α верно $\forall \beta < \alpha \quad \mathbb{V}_\beta \subset \mathbb{V}_\alpha$. \square

Теорема 1.7.6 (\in -индукция). Пусть φ – некоторое свойство множеств, тогда

$$\forall x (\forall y \in x \varphi(y) \rightarrow \varphi(x)) \rightarrow \forall x \varphi(x)$$

Доказательство. Допустим, что $\varphi(x)$ не выполнено для некоторого множества x и $\forall a (\forall b \in a \varphi(b) \rightarrow \varphi(a))$

Рассмотрим подмножество Z множества $T = TC(\{x\})$, состоящее из множеств, которые не удовлетворяют свойству φ .

Видим, что множество Z непусто. Тогда по аксиоме регулярности оно содержит элемент z такой, что $z \cup Z = \emptyset$

В силу транзитивности множества T , все элементы множества z лежат в T (и не лежат в Z). Получаем, что $\varphi(z)$ верно, поскольку $\varphi(y)$ верно для любого $y \in z$. Противоречие. \square

Теорема 1.7.7. Для всякого множества x существует ординал α такой, что $x \in \mathbb{V}_\alpha$

Доказательство. Рассмотрим свойство φ : существует ординал α такой, что $x \in \mathbb{V}_\alpha$

Предположим, что нам дано множество y , все элементы которого обладают свойством φ , то есть $\forall z \in y \varphi(z)$

Теперь рассмотрим условие $\psi(c, d) : d - \text{наименьший ординал, для которого } c \in \mathbb{V}_d$. Заметим, что для любого элемента z множества y существует такой ординал β , что выполнено $\psi(z, \beta)$

Кроме того, для любого множества c существует не более одного множества d , удовлетворяющего условию $\psi(c, d)$. По аксиоме подстановки существует множество $D = \{d \mid \exists c \in y \psi(c, d)\}$

Видим, что D – это множество ординалов. Возьмем точную верхнюю грань $\sup D$ всех элементов множества D . Получаем, что $y \subset \mathbb{V}_{\sup D}$, а потому $y \in \mathbb{V}_{\sup D+1}$. Следовательно, имеет место $\varphi(y)$

Согласно принципу \in -индукции $\varphi(x)$ верно для любого множества x □

Определение. Рангом множества x по фон Нейману называется наименьший ординал α , для которого $x \in \mathbb{V}_{\alpha+1}$, или, что эквивалентно, $x \subset \mathbb{V}_\alpha$.

анный ординал обозначается $\text{rnk } x$

Лемма 1.7.8. $\forall x : x \notin \mathbb{V}_{\text{rnk } x}$

Доказательство. Предположим, что $x \in \mathbb{V}_{\text{rnk } x}$ для некоторого ординала β , то по определению ранга $\text{rnk } x = \beta + 1$ для некоторого ординала β , то по определению ранга $x \leq \beta$. Противоречие.

Осталось рассмотреть случай, когда $\text{rnk } x$ – предельный ординал. В этом случае

$$\mathbb{V}_{\text{rnk } x} = \bigcup_{\gamma < \text{rnk } x} \mathbb{V}_\gamma$$

Видим, что $x \in \mathbb{V}_\gamma$ для некоторого $\gamma < \text{rnk } x$, $x \in \mathbb{V}_\gamma \subset \mathbb{V}_{\gamma+1}$ и $\text{rnk } x \leq \gamma$. Противоречие. □

Лемма 1.7.9. Для любого множества x ранг $\text{rnk } x = \sup\{\text{rnk } y + 1 \mid y \in x\}$

Доказательство. Во-первых

$$\forall y \in x \quad y \in \mathbb{V}_{\text{rnk } y+1} \subset \bigcup_{y \in x} \mathbb{V}_{\text{rnk } y+1} \subset \mathbb{V}_{\sup\{\text{rnk } y+1 \mid y \in x\}}$$

Получаем $\text{rnk } x \leq \sup\{\text{rnk } y + 1 \mid y \in x\}$

Теперь проверим, что $\text{rnk } y + 1 \leq \text{rnk } x$ для любого $y \in x$. Если $\text{rnk } x < \text{rnk } y + 1$, то $\text{rnk } x < \text{rnk } y$ и

$$y \in x \subset \mathbb{V}_{\text{rnk } x} \subset \mathbb{V}_{\text{rnk } y}$$

Что противоречит предыдущей лемме

Следовательно, $\text{rnk } y + 1 \leq \text{rnk } x$ для любого $y \in x$, и

$$\sup\{\text{rnk } y + 1 \mid y \in x\} \leq \text{rnk } x$$

□

Глава 2.

Логика Предикатов

2.1. Лекция 8 (02.09.2021)

Философские вопросы математики:

- 1) Что значит доказать теорему?
- 2) Что значит дать определение понятию?
- 3) Правомерно ли рассуждать об актуально бесконечных множествах?
- 4) Когда говорим об истинности и доказуемости, имеются ли ввиду одно и то же?
- 5) Противоречива ли математика? Возможно ли установить непротиворечивость?

Направления Философии математики: Логицизм (Фреге, Рассел, Уайтхед), Интуиционизм (Брауэр, Вейль), Формализм (Гильберт), Платонизм (Гедель) и т.д.

Подробнее в: С.Клини – “Введение в математику”

Аксиоматический метод Гильберта предполагает явную формулировку всех предположений теории и допускает лишь чисто логические выводы из этих посылок.

Логический вывод может быть записан в символьном виде, что превращает его в вычислительный процесс. Это привело к созданию формальных аксиоматических теорий.

Компьютерные реализации: Coq, HOL, Mizar

Программа Гильберта:

- 1) Формализовать математику (теорию множеств) в рамках аксиоматической теории T
- 2) Формальные доказательства в T представляют собой конечные объекты (строки символов), строящиеся по вполне определенным правилам
- 3) Из следует проанализировать элементарными комбинаторными средствами и установить, что противоречие в T не доказуемо
- 4) Тем самым мы сведем использование теоретико-множественных методов к заведомо надежным элементарным методам

Математическая логика – построение и исследование формальных языков математиче-

скими методами.

Метаязык (описание объекта), Метатеория (теория в рамках которой мы рассуждаем об исследуемой теории), Синтаксис (правила построения выражений), Семантика (значение/смысл выражений)

Предикаты и функции

Пусть M – непустое множество

Определение. n -арный предикат на M : функция $Q : M^n \rightarrow \{0, 1\}$ (Интуитивно: $Q(x_1, \dots, x_n)$ есть высказывание, зависящее от выбора параметров $x_1, \dots, x_n \in M$. Предикаты можно также понимать как n -арные отношения на M , то есть подмножества M^n)

Определение. n -арная функция на M : функция $f : M^n \rightarrow M$

Определение. константа: элемент M

Определение. Сигнатурой называется некоторая совокупность имен функций, предикатов и констант. Сигнатура Σ задается:

Pred_Σ предикатные символы

Func_Σ функциональные символы

Const_Σ символы констант

Функция валентности $\text{Pred}_\Sigma \cup \text{Func}_\Sigma \rightarrow \mathbb{N} \setminus \{0\}$

Определение. Модель сигнатуры Σ есть непустое множество M вместе с отображением, сопоставляющим:

Каждому $P \in \text{Pred}_\Sigma$ некоторый предикат P на M той же валентности

Каждому $f \in \text{Func}_\Sigma$ функцию f_M на M той же валентности

Каждому $c \in \text{Const}_\Sigma$ константу $c_M \in M$.

Синтаксис Логики первого порядка

Алфавит \mathcal{L}_Σ содержит:

Символы сигнатуры: Σ

Свободные переменные: $\text{FrVar} = \{a_0, a_1, \dots\}$

Связанные переменные: $\text{BdVar} = \{v_0, v_1, \dots\}$

Булевы связки: $\rightarrow, \neg, \wedge, \vee$;

Кванторы \forall, \exists

Знаки пунктуации: $\ll (\gg, \ll \gg, \ll, \gg$

Определение. Множество термов Tm_Σ есть наименьшее множество, замкнутое относительно следующих двух правил:

1) Свободные переменные и константы суть термы 2) Если $f \in \text{Func}_\Sigma$ валентности n и t_1, \dots, t_n – термы, то выражение $f(t_1, \dots, t_n)$ есть терм

Определение. Множество формул Fm_Σ есть наименьшее множество, замкнутое относительно следующих правил:

Если $P \in \text{Pred}_\Sigma$ валентности n и t_1, \dots, t_n – термы, то $P(t_1, \dots, t_n)$ есть формула (называемая атомарной формулой)

Если A, B – формулы, то формулами являются $(A \rightarrow B)$, $\neg A$, $(A \wedge B)$, $(A \vee B)$

Если A – формула, и a – свободная переменная, то для любой связанной переменной x , не входящей в A , выражения $(\forall x A[a/x])$ и $(\exists x A[a/x])$ – формулы ($A[a/x]$ – замена a на x).

2.2. Лекция 9 (02.16.2021)

Определение. Пусть A – замкнутая формула сигнатуры $\Sigma(M)$. Отношение $M \models A$ формула A истинна в модели M определяется индукцией по построению A

$$M \models P(t_1, \dots, t_n) \stackrel{\text{def}}{\iff} P_M((t_1)_M, \dots, (t_n)_M) = 1, \text{ если} \\ A = P(t_1, \dots, t_n) - \text{ атомарная формула;}$$

Стандартные определения для булевых связок

$$M \models (B \rightarrow C) \stackrel{\text{def}}{\iff} (M \not\models B \text{ или } M \models C) \\ M \models \neg B \stackrel{\text{def}}{\iff} M \not\models B ; \\ M \models (A \wedge B) \stackrel{\text{def}}{\iff} (M \models A \text{ и } M \models B) \\ M \models (A \vee B) \stackrel{\text{def}}{\iff} (M \models A \text{ или } M \models B)$$

Кванторы

$$M \models (\forall x A[a/x]) \stackrel{\text{def}}{\iff} \text{ для всех } c \in M M \models A[a/c] \\ M \models (\exists x A[a/x]) \stackrel{\text{def}}{\iff} \text{ существует } c \in M M \models A[a/c]$$

Нельзя говорить об истинности или ложности незамкнутых формул, поскольку их истинностные значения зависят от выбора значений параметров – входящих в формулу свободных переменных

Пример: формула $a + 1 = b$ в стандартной модели арифметики может быть как истинной, так и ложной

Сокращение: вместо

$$\frac{M}{x} \models A[a_1/c_1, \dots, a_n/c_n]$$

пишут

$$M \models A[a_1/c_1, \dots, a_n/c_n]$$

или даже

$$M \models A[c_1, \dots, c_n]$$

Пример.

В модели $(\mathbb{N}; =, S, +, \cdot, 0)$ истинна формула

$$\exists x, y, z (\neg x = 0 \wedge \neg y = 0 \wedge x \cdot x + y \cdot y = z \cdot z)$$

и ложна формула

$$\exists x, y, z (\neg x = 0 \wedge \neg y = 0 \wedge x \cdot x \cdot x + y \cdot y \cdot y = z \cdot z \cdot z)$$

Пример

В модели $(\mathbb{R}^2; =, \cong, B)$ истинна формула

$$\forall x, y, y', z (B(x, y, z) \wedge B(x, y', z) \rightarrow B(x, y, y') \vee B(x, y', y))$$

Эта же формула верна и в модели $(H^2; =, \cong, \cdot, B)$.

Любая формула A от свободных переменных b_1, \dots, b_n определяет n -местный предикат A_M в модели M :

$$A_M(x_1, \dots, x_n) = 1 \stackrel{\text{def}}{\iff} M \models A[b_1/x_1, \dots, b_n/x_n]$$

Пример.

В модели $(\mathbb{N}; =, +)$ формула $\exists x(x + x = a)$ определяет предикат «а чётно», т.е. множество чётных чисел.

Определение. Предикат $P(x_1, \dots, x_n)$ называется определимым в модели $(M; \Sigma)$, если $P = A_M$ для некоторой формулы A языка \mathcal{L}_Σ .

Определение. Функция f называется определимой в модели M , если определим её график, то есть предикат $G_f(x_1, \dots, x_n, y) \stackrel{\text{def}}{\iff} f(x_1, \dots, x_n) = y$

Пример. В модели $(\mathbb{Z}; \leq)$ предикат $b = a + 1$ определим формулой

$$\neg b \leq a \wedge \forall x(x \leq a \vee b \leq x)$$

Следовательно, функция $s(x) \doteq x + 1$ определима в $(\mathbb{Z}; \leq)$.

Определим следующие предикаты в $(\mathbb{R}^2; =, \cong, B)$

$$a \neq b \doteq \neg a = b$$

$c \in ab$ «с лежит на прямой ab »

$$c \in ab \doteq (B(c, a, b) \vee B(a, c, b) \vee B(a, b, c))$$

$ab \parallel cd$ «прямые a ab и cd параллельны»

$$ab \parallel cd \doteq a \neq b \wedge c \neq d \wedge \neg \exists x(x \in ab \wedge x \in cd)$$

«Через точку z вне прямой xy можно провести не более одной прямой, параллельной данной.»

$$\forall x, y, z (x \neq y \wedge \neg z \in xy \rightarrow \forall u, v (zu \parallel xy \wedge zv \parallel xy \rightarrow v \in zu))$$

Верно в \mathbb{R}^2 , но не в H^2 .

Определение. Формула $A(b_1, \dots, b_n)$ сигнатуры Σ выполнима в модели (M, Σ) , если для некоторых констант $c_1, \dots, c_n \in M$ предложение $A[b_1/c_1, \dots, b_n/c_n]$ (сигнатуры $\Sigma(M)$) истинно. Формула A сигнатуры Σ выполнима, если она выполнима в некоторой модели (M, Σ) .

Определение. Формула A общезначима (тождественно истинна), если $\neg A$ не выполнима

Определение. Формула A тождественно ложна, если A не выполнима.

Пример.

Формулы $P(a) \vee \neg P(a), \exists x \forall y A(x, y) \rightarrow \forall y \exists x A(x, y)$ общезначимы. Формула $P(a_0) \rightarrow P(a_1)$ выполнима, но не общезначима.

Общезначимые формулы представляют собой универсальные законы логики, истинные вне зависимости от предметной области и интерпретации входящих в них предикатных символов.

Логическое следование утверждения B из утверждений A_1, \dots, A_n сводится к проверке общезначимости формулы $A_1 \wedge A_2 \wedge \dots \wedge A_n \rightarrow B$

Entscheidungsproblem: найти алгоритм, определяющий по данной формуле A , общезначима ли она. Гильберт считал этот вопрос важнейшей математической проблемой.

- Пропозициональные переменные: $\text{Var} = \{P_0, P_1, \dots\}$.
- Связки: $\neg, \wedge, \vee, \rightarrow$; константы \perp (ложь), \top (истина).
- Формулы F_m строятся по правилам:
 - (1) Если $P \in \text{Var}$ или $P \in \{\top, \perp\}$, то P – формула;
 - (2) Если A и B – формулы, то $(\neg A), (A \wedge B), (A \vee B), (A \rightarrow B)$ – формулы.
- F_m есть наименьшее множество, удовлетворяющее условиям 1 и 2.

Лемма 2.2.1. Любая формула F , отличная от переменной или константы, однозначно представляется в виде $(A \wedge B), (A \vee B), (A \rightarrow B)$ или $(\neg A)$ для некоторых формул A, B .

Доказательство. Соображения баланса скобок в формуле. □

Определение. - A и B называются непосредственными подформулами F ; - G – подформула F , если $G \overset{\circ}{=} F_{\text{или}} G$ – подформула одной из непосредственных подформул F .

- Опускаем внешние скобки;
- Приоритет связок: $\neg, \wedge, \vee, \rightarrow$; $\neg P \wedge Q \rightarrow R$ читается как $((\neg P) \wedge Q) \rightarrow R$
- Кратные \wedge и \vee ассоциируем влево: $A \wedge B \wedge C$ читается как $((A \wedge B) \wedge C)$.

Определение. Истинностные значения: $\mathbb{B} \rightleftharpoons \{\text{Л}, \text{И}\} \rightleftharpoons \{0, 1\}$.

Булевы функции: $f : \mathbb{B}^n \rightarrow \mathbb{B}$.

	x_1	x_2	\dots	x_n	$f(x_1, x_2, \dots, x_n)$
	0	0	\dots	0	$f(0, 0, \dots, 0)$
Функции $f : \mathbb{B}^n \rightarrow \mathbb{B}$ принято задавать таблицами истинности вида	0	0	\dots	1	$f(0, 0, \dots, 1)$
	\dots	\dots	\dots	\dots	\dots
	1	1	\dots	1	$f(1, 1, \dots, 1)$

В такой таблице 2^n строк

Определение. Оценка переменных: функция $f : \text{Var} \rightarrow \mathbb{B}$. Любая оценка продолжается естественным образом до отображения $f : F_m \rightarrow \mathbb{B}$.

Определение. $f(A)$ = значение формул A при оценке f . Определяется индукцией по построению A :

Значение $f(A)$ определяется индукцией по построению A :

$$\begin{aligned}
f(\top) &= 1; f(\perp) = 0 \\
f(\neg A) &= 1 - f(A) \\
f(A \wedge B) &= \min(f(A), f(B)) \\
f(A \vee B) &= \max(f(A), f(B)) \\
f(A \rightarrow B) &= \max(1 - f(A), f(B))
\end{aligned}$$

В частности, $f(A \rightarrow B) = 1 \iff f(A) \leq f(B)$

Лемма 2.2.2. Пусть $\text{Var} = \{P_1, \dots, P_n\}$

Тогда существует взаимно-однозначное соответствие между оценками $f : \text{Var} \rightarrow \mathbb{B}$ и наборами $\vec{x} = (x_1, \dots, x_n) \in \mathbb{B}^n$.

$$f \mapsto (f(P_1), \dots, f(P_n)) \in \mathbb{B}^n$$

$\vec{x} = (x_1, \dots, x_n) \mapsto f_{\vec{x}}$, где оценка $f_{\vec{x}}$ определена таблицей

P_1	P_2	\dots	P_n
x_1	x_2	\dots	x_n

Определение. Таблица истинности формулы A от n переменных есть булева функция $\varphi_A : \mathbb{B}^n \rightarrow \mathbb{B}$ такая, что

$$\varphi_A(\vec{x}) = f_{\vec{x}}(A)$$

для всех $\vec{x} \in \mathbb{B}^n$

Теорема 2.2.3. Для любой функции $\varphi : \mathbb{B}^n \rightarrow \mathbb{B}$ найдётся такая формула A от n переменных, что $\varphi = \varphi_A$. При этом можно считать, что A содержит лишь связки \neg и \vee .

Доказательство. Для $x \in \mathbb{B}$ положим

$$P^x = \begin{cases} P, & \text{если } x = \text{И} \\ \neg P, & \text{если } x = \text{Л} \end{cases}$$

Для $\vec{x} = (x_1, \dots, x_n) \in \mathbb{B}^n$ обозначим

$$A_{\vec{x}} \equiv \bigwedge_{i=1}^n P_i^{x_i}$$

где $\bigwedge_{j=1}^m B_j \equiv ((B_1 \wedge B_2) \wedge \dots \wedge B_m)$

имеем: для любой оценки f

$$f(A_{\vec{x}}) = \text{И} \iff f = f_{\vec{x}}$$

Пусть список $\vec{x}_1, \dots, \vec{x}_m$ исчерпывает все $\vec{x} \in \mathbb{B}^n$ для которых $\varphi(\vec{x}) = h$, то есть

$$\varphi(\vec{x}) = \text{И} \iff \exists j \vec{x} = \vec{x}_j$$

Положим

$$A \equiv \bigvee_{j=1}^m A_{\vec{x}_j}$$

Тогда

$$\begin{aligned} f_{\vec{x}}(A) = \text{И} &\iff \exists j f_{\vec{x}}(A_{\vec{x}_j}) = \text{И} \\ &\iff \exists j \vec{x} = \vec{x}_j \\ &\iff \varphi(\vec{x}) = \text{И} \end{aligned}$$

Значит, $\varphi_A(\vec{x}) = f_{\vec{x}}(A) = \varphi(\vec{x})$

□

Определение. Формула A выполнима, если $\exists f : f(A) = \text{И}$.

Определение. Формула A - тавтология, если $\forall f : f(A) = \text{И}$.

Определение. Формула A - тождественно ложна, если $\forall f : f(A) = \text{Л}$.

Лемма 2.2.4. Следующие условия равносильны.

- (1) Формула A тождественно ложна.
- (2) Формула A не выполнима.
- (3) Формула $\neg A$ - тавтология.

Пример:

$\neg(P \rightarrow P)$ тождественно ложна (и не выполнима); $P \rightarrow P$ тавтология; $P \rightarrow Q$ выполнима, но не тавтология.

2.3. Лекция 10 (02.22.2021)

Определение. Формула $A(b_1, \dots, b_n)$ сигнатуры Σ общезначима, если для любой модели $(M; \Sigma)$ и любых констант $c_1, \dots, c_n \in M$ $M \models A[b_1/\underline{c}_1, \dots, b_n/\underline{c}_n]$

Определение. Формулы A и B сигнатуры Σ равносильны (обозначение $A \equiv B$), если в любой модели $(M; \Sigma)$ они определяют один и тот же предикат, то есть если $A_M = B_M$.

Утверждение.

$A \equiv B \iff$ формула $A \leftrightarrow B$ общезначима.

$A \leftrightarrow B$ есть сокращение для $(A \rightarrow B) \wedge (B \rightarrow A)$.

Равносильности логики высказываний

$A \wedge B \equiv B \wedge A$	$A \vee B \equiv B \vee A$
$A \wedge (B \wedge C) \equiv (A \wedge B) \wedge C$	$A \vee (B \vee C) \equiv (A \vee B) \vee C$
$A \wedge A \equiv A$	$A \vee A \equiv A$
$A \wedge (B \vee C) \equiv (A \wedge B) \vee (A \wedge C)$	$A \vee (B \wedge C) \equiv (A \vee B) \wedge (A \vee C)$
$A \vee (A \wedge B) \equiv A$	$A \wedge (A \vee B) \equiv A$
$\neg(A \wedge B) \equiv \neg A \vee \neg B$	$\neg(A \vee B) \equiv \neg A \wedge \neg B$
$\perp \equiv A \wedge \neg A$	$T \equiv A \vee \neg A$
$\neg\neg A \equiv A$	$A \rightarrow B \equiv \neg A \vee B$

Кванторы

$$\begin{aligned}
\forall x A[a/x] &\equiv \forall y A[a/y] \\
\exists x A[a/x] &\equiv \exists y A[a/y] \\
(\forall x A[a/x] \vee B) &\equiv \forall x (A[a/x] \vee B) \\
(\exists x A[a/x] \vee B) &\equiv \exists x (A[a/x] \vee B) \\
(\forall x A[a/x] \wedge B) &\equiv \forall x (A[a/x] \wedge B) \\
(\exists x A[a/x] \wedge B) &\equiv \exists x (A[a/x] \wedge B) \\
\neg \forall x A[a/x] &\equiv \exists x \neg A[a/x] \\
\neg \exists x A[a/x] &\equiv \forall x \neg A[a/x]
\end{aligned}$$

Стандартные факты:

- (1) Допустимость правил подстановки и замены подформулы на эквивалентную
- (2) Переименование связанных переменных
- (3) Теорема о предварённой нормальной форме

(1) Обогатим язык логики первого порядка пропозициональными переменными. Можно считать переменную P нульместным предикатным символом

(2) Распространим на расширенный язык все синтаксические понятия, включая понятие формулы.

(3) Пропозициональные переменные считаются атомарными формулами.

Определение. $C[P/A]$ означает результат замены всех вхождений P в формулу C на формулу A . (т

Замечание.

$C[P/A]$ не всегда является формулой. Если $C = \forall x(Q(x) \wedge P)$ и $A = \exists x R(x)$, то $C[P/A] = \forall x(Q(x) \wedge \exists x R(x))$

Лемма 2.3.1. $C[P/A]$ - формула, если и только если любое вхождение P в формулу C не находится в области действия квантора по переменной $x \in \text{BdVar}$, входящей в A .

Определение. Говорим, что разрешена подстановка формулы A вместо P в C , если выполнено условие предыдущей леммы.

Теорема 2.3.2. Если $A \equiv B$ и разрешена подстановка формул A, B вместо P в C , то $C[P/A] \equiv C[P/B]$

Доказательство. индукция по построению формулы C . Шаг индукции на основе леммы:

Лемма 2.3.3. Если $A \equiv A'$ и $B \equiv B'$, то

- (1) $(A \wedge B \equiv A' \wedge B', \quad A \vee B \equiv A' \vee B', \quad \neg A \equiv \neg A',$
- (2) $\forall x A[a/x] \equiv \forall x A'[a/x]$ (если \tilde{o} не входит в A и A')
- (3) $(\exists x A[a/x] \equiv \exists x A'[a/x])$ (если x не входит в A и A').

□

(1) Пропозициональная переменная P в модели M интерпретируется как логическая константа, то есть P_M is \mathbb{B} .

(2) Считается $M \models P_M$, если $P_M = \text{И}$ и $M \not\models P_M$, если $P_M = \text{Л}$.

(3) Понятие общезначимой формулы распространяется на формулы расширенного языка.

Теорема 2.3.4. Пусть формула A общезначима и разрешена подстановка формулы C вместо P в A , тогда общезначима формула $A[P/C]$

Доказательство. (1) Допустим, $M \not\models f(A[P/C])$ при некоторой оценке f .

(2) Расширим M до модели (M, P) сигнатуры с переменной $P : P_M = \text{И} \iff M \models f(C)$

(3) Индукцией по построению формулы B проверим, что

$$(M, P) \models B \iff M \models B[P/C]$$

для любой замкнутой формулы B , в которую разрешена подстановка C вместо P .

(4) Отсюда получаем $(M, P) \models f(A)$.

□

Следствие 2.3.4.1. Если $A \equiv B$ и разрешена подстановка C вместо P в A и B , то $A[P/C] \equiv B[P/C]$

Лемма 2.3.5. Пусть $y \in \text{BdVar}$ не входит в формулу B . Тогда $B[x/y]$ есть формула и $B[x/y] \equiv B$.

Доказательство. Применяем индукцию по числу вхождений кванторов по переменной \times в B . Каждая подформула $\forall x C[a/x]$ или $\exists x C[a/x]$ заменяется на эквивалентную $\forall y C[a/y]$ или $\exists y C[a/y]$.

□

Определение. Формула A называется предварённой, если A имеет вид $Qx_1 Qx_2 \dots Qx_n A_0 [b_1/x_1, \dots, b_n/x_n]$ где Q означает квантор \forall или \exists , а формула A_0 бескванторная.

Теорема 2.3.6. Для каждой формулы \hat{A} можно указать эквивалентную ей предварённую формулу A' от тех же свободных переменных.

Доказательство. Последовательно выносим кванторы наружу, используя основные эквивалентности и леммы о замене связанных переменных и о подстановке. Разбор алгоритма на семинарских занятиях. \square

Определение. Теорией сигнатуры Σ называем произвольное множество T замкнутых формул языка \mathcal{L}_Σ . Элементы $A \in T$ называем нелогическими аксиомами T .

Пример.

Теория отношения эквивалентности:

- (1) $\forall x R(x, x)$
- (2) $\forall x, y (R(x, y) \rightarrow R(y, x))$
- (3) $\forall x, y, z (R(x, y) \wedge R(y, z) \rightarrow R(x, z))$

Пример

Модель $(M; <)$ есть строгий частичный порядок, если в $(M; <)$ истинны следующие предложения:

- (1) $\forall x, y, z (x < y \wedge y < z \rightarrow x < z)$
- (2) $\forall x \neg x < x$

Пример

Простой граф - это модель вида $(V; E)$, где E - бинарный предикат смежности, причём отношение E симметрично и иррефлексивно:

- (1) $\forall x \neg E(x, x)$
- (2) $\forall x, y (E(x, y) \rightarrow E(y, x))$

Пример.

$(M; =, \cdot, 1)$ есть группа, если M есть модель следующей теории (при условии, что '=' в M понимается как равенство):

- (1) $\forall x, y, z \quad x \cdot (y \cdot z) = (x \cdot y) \cdot z$
- (2) $\forall x (1 \cdot x = x \wedge x \cdot 1 = x)$
- (3) $\forall x \exists y (x \cdot y = 1 \wedge y \cdot x = 1)$

Пусть Σ - сигнатура, содержащая выделенный предикатный символ $=$

Определение. Нормальной моделью называем модель $(M; \Sigma)$, в которой $=$ интерпретируется как равенство $\{\langle x, x \rangle \mid x \in M\}$.

Определение. Аксиомы равенства для Σ - универсальные замыкания следующих формул:

- (1) аксиомы отношения эквивалентности для $=$
- (2)

$$a_1 = b_1 \wedge a_2 = b_2 \wedge \dots \wedge a_n = b_n \rightarrow (P(a_1, \dots, a_n) \leftrightarrow P(b_1, \dots, b_n))$$

(3)

$$a_1 = b_1 \wedge a_2 = b_2 \wedge \dots \wedge a_n = b_n \rightarrow (f(a_1, \dots, a_n) = f(b_1, \dots, b_n))$$

для всех $f \in \text{Func}_\Sigma$ and $P \in \text{Pred}_\Sigma$

Предложение.

Если $(M; \Sigma)$ - нормальная модель, то в M истинны все аксиомы равенства.

Определение. Теорией с равенством называем теорию сигнатуры Σ с равенством, содержащую все аксиомы равенства.

Теорема 2.3.7. Пусть T - теория с равенством. Если T выполнима, то T имеет нормальную модель.

Доказательство. Пусть $M \models T$. Предикат $=_M$ есть отношение эквивалентности на M . Положим $M' = M / =_M$ - множество классов эквивалентности и $\varphi : M \rightarrow M'$ сопоставляет любому $x \in M$ его класс $\varphi(x) \in M'$

Интерпретируем предикатные и функц. символы в M' :

$$P_{M'}(\varphi(x_1)^{\{m_2\}} \dots, \varphi(x_n)) \stackrel{\text{def}}{\iff} P_M(x_1, \dots, x_n) \quad f_{M'}(\varphi(x_1), \dots, \varphi(x_n)) := \varphi(f_M(x_1, \dots, x_n))$$

В силу аксиом равенства в M , определение корректно и M' - нормальная модель.

Индукцией по построению формулы A проверяем

$$M \models A[x_1, \dots, x_n] \iff M' \models A[\varphi(x_1), \dots, \varphi(x_n)]$$

Отсюда следует $M' \models T$. □

Формальная арифметика Пеано

Сигнатура $\Sigma = \{0, S, +, \cdot, =\}$

(1) аксиомы равенства для Σ

(2) $\neg S(a) = 0, \quad S(a) = S(b) \rightarrow a = b$

(3) $a + 0 = a, \quad a + S(b) = S(a + b)$

(4) $a \cdot 0 = 0, \quad a \cdot S(b) = a \cdot b + a$

(5) (Схема аксиом индукции) $A[a/0] \wedge \forall x(A[a/x] \rightarrow A[a/S(x)]) \rightarrow \forall x A[a/x]$ для любой формулы A .

Теория множеств ZFC

Сигнатура $\Sigma = \{=, \in\}$

(1) (Аксиомы равенства)

(2) (Экстенсинальность) $a = b \leftrightarrow \forall x(x \in a \leftrightarrow x \in b)$

(3) (Пара) $\exists z \forall x(x \in z \leftrightarrow (x = a \vee x = b))$

(4) (Объединение) $\exists z \forall x(x \in z \leftrightarrow \exists y(x \in y \wedge y \in a))$

- (5) (Степень) $\exists z \forall x (x \in z \leftrightarrow \forall y (y \in x \rightarrow y \in a))$
- (6) (Схема выделения) $\exists z \forall x (x \in Z \leftrightarrow (x \in a \wedge \varphi[b/x]))$ для всех формул φ сигнатуры Σ
- (7) (Бесконечность) $\exists z (\emptyset \in z \wedge \forall x (x \in z \rightarrow x \cup \{x\} \in z))$
- (8) (Регулярность) $\exists z (z \in a \wedge \forall x (x \in a \rightarrow x \notin z))$
- (9) (Схема подстановки)
- (10) (Аксиома выбора)

Аксиоматика Тарского:

- G1. $ab \cong ba$
- G2. $ab \cong pq \wedge ab \cong rs \rightarrow pq \cong rs$
- G3. $ab \cong cc \rightarrow a = b$
- G4. $Babd \wedge Bbcd \rightarrow Babc$
- G5. $\exists x (Bqax \wedge ax \cong bc)$ G6. $(a \neq b \wedge Babc \wedge Ba'b'c' \wedge ab \cong a'b' \wedge bc \cong b'c' \wedge ad \cong a'd' \wedge bd \cong b'd') \rightarrow cd \cong c'd'$ (Аналог равенства треугольников)
- G7. (аксиома Паша)
 $Barc \wedge Bqcb \rightarrow \exists x (Baxq \wedge Bbpx)$
- G8. $\exists x, y, z (\neg Bxyz \wedge \neg Byzx \wedge \neg Bzxy)$
- G9. $(\dim \leq 2) (p_1 \neq p_2 \wedge ap_1 \cong ap_2 \wedge bp_1 \cong bp_2 \wedge cp_1 \cong cp_2) \rightarrow a \in bc$
- G10. (аксиома Евклида)
- G11. (схема аксиом непрерывности)

$$\begin{aligned} \exists u \forall x, y (C[a/x] \wedge D[a/y] \rightarrow Buxy) \rightarrow \\ \exists v \forall x, y' (C[a/x] \wedge D[a/y] \rightarrow Bxvy) \end{aligned}$$

Здесь x, y, u, v не входят в C, D .

- G11'. (аксиома непрерывности 2-го порядка)

$$\begin{aligned} \forall X, Y (\exists u \forall x, y (x \in X \wedge y \in Y \rightarrow Buxy) \rightarrow \\ \exists v \forall x, y (x \in X' \wedge y \in Y \rightarrow Bxvy)) \end{aligned}$$

Теорема 2.3.8 (Тарского о полноте). Для любого предложения A языка элементарной геометрии, если $(\mathbb{R}^2; =, B, \cong) \models A$, то A логически следует из аксиом $G1 - G11$

Теорема 2.3.9. Существует алгоритм проверки формулы A на выполнимость в \mathbb{R}^2

2.4. Лекция 11 (03.01.2021)

Исчисление предикатов сигнатуры Σ задаётся след. аксиомами и правилами вывода.

Аксиомы:

- A1. Подстановочные примеры тавтологий,
- A2. $\forall x A[a/x] \rightarrow A[a/t]$
- A3. $A[a/t] \rightarrow \exists x A[a/x]$

Подстановочным примером тавтологии A мы называем результат замены всех пропозициональных переменных A на некоторые формулы сигнатуры Σ .

Пример:

$B \vee \neg B$, где B – любая формула. В A2 и A3 A – любая формула сигнатуры Σ и t – любой терм (\times не входит в A).

Правила вывода:

R1. $\frac{A \quad A \rightarrow B}{B}$ (modus ponens)

R2. $\frac{A \rightarrow B}{A \rightarrow \forall x B[a/x]}$

R3. $\frac{B \rightarrow A}{\exists x B[a/x] \rightarrow A}$

Здесь a не входит в A (и x не входит в B).

Правила R2 и R3 называются правилами Бернаиса.

Определение. Выводом в исчислении предикатов называется конечная последовательность формул, каждая из которых либо является аксиомой, либо получается из предыдущих формул по одному из правил вывода R_1, R_2, R_3

Пример $\forall x A[A/x] \rightarrow A$ (A2)

$\forall x A[A/x] \rightarrow \forall y A[a/y]$ (R2)

Определение. Формула A называется выводимой в исчислении предикатов или теоремой исчисления предикатов если существует вывод, в котором последняя формула есть A

Определение. Вывод в теории T называется конечная последовательность формул, каждая из которых либо принадлежит множеству T , либо является логической аксиомой вида A_1, A_2, A_3 , либо получается из предыдущих формул по одному из правил R_1, R_2, R_3

Определение. Формула A называется выводимой (доказуемой) в теории T или теоремой T (обозначение $T \vdash A$), если существует вывод в T , в котором последняя формула есть A .

Определение. Формула A опровержима в T , если $T \vdash \neg A$.

Определение. Формула A независима от T , если $T \not\vdash A$ и $T \not\vdash \neg A$.

Если $T \subseteq U$ и $T \vdash A$, то $U \vdash A$ (монотонность)

Если $T \vdash A$, то существует такое конечное множество $T_0 \subseteq T$, что $T_0 \vdash A$ (компактность)

Если $T \vdash A$ и для каждой аксиомы $B \in T$ имеет место $U \vdash B$, то $U \vdash A$ (транзитивность)

Определение. Теорией сигнатуры Σ называем произвольно множество T замкнутых формул языка Σ . Теорию $T \cup \{A\}$ обозначают также T, A или $T + A$

Теорема 2.4.1. Для любой теории T и любой замкнутой формулы A

$$T, A \vdash B \Leftrightarrow T \vdash A \rightarrow B$$

Доказательство. Индукция по длине вывода $T, A \vdash B$

Если B является логической аксиомой или $B \in T$, то в T выводимо:

$$\begin{array}{l} B \\ B \rightarrow (A \rightarrow B) \quad (\text{тавтология}) \\ A \rightarrow B \quad (\text{MP}) \end{array}$$

Если $A = B$, то используем $A \rightarrow A$

Пусть B получена из C и $C \rightarrow B$ по modus ponens. Имеем $T \vdash (A \rightarrow C)$ и ${}_{\chi}T \vdash (A \rightarrow (C \rightarrow B))$ по предположению индукции. Соединяем эти два вывода и достраиваем так:

$$\begin{array}{l} (A \rightarrow (C \rightarrow B)) \rightarrow ((A \rightarrow C) \rightarrow (A \rightarrow B)) \quad (\text{тавтология}) \\ (A \rightarrow C) \rightarrow (A \rightarrow B) \quad (\text{MP}) \\ A \rightarrow B \quad (\text{MP}) \end{array}$$

Допустим $B = (C \rightarrow \forall x D[a/x])$ получена из $C \rightarrow D$ по $R2$. По пр. индукции

$$T \vdash A \rightarrow (C \rightarrow D)$$

Надо построить вывод

$$T \vdash A \rightarrow (C \rightarrow \forall x D[a/x])$$

Достраиваем вывод $A \rightarrow (C \rightarrow D)$ в T :

$$\begin{array}{l} A \rightarrow (C \rightarrow D) \\ (A \rightarrow (C \rightarrow ID)) \rightarrow (A \wedge C \rightarrow D) \quad (\text{тавтология}) \\ (A \wedge C) \rightarrow D \quad (\text{MP}) \\ (A \wedge C) \rightarrow \forall x D[a/x] \quad (R2, A \text{ замкнута}) \\ A \rightarrow (C \rightarrow \forall x D[a/x]) \end{array}$$

(аналогично)

Правило $R3$ рассматривается аналогично. □

Определение. Теория T противоречива, если существует A такая, что $T \vdash A$ и $T \vdash \neg A$. В противном случае теория T называется непротиворечивой.

Следствие 2.4.1.1. $T \cup \{A\}$ противоречива $\Leftrightarrow T \vdash \neg A$.

Теорема 2.4.2 (О корректности). Если $M \models T$ и $T \vdash A$, то $M \models A$

Доказательство. Индукция по длине вывода A в T □

Следствие 2.4.2.1. Если $\vdash A$, то A общезначима.

Следствие 2.4.2.2. Если теория T имеет модель, то T непротиворечива

Следствие 2.4.2.3. Следующие теории непротиворечивы:

Исчисление предикатов(пустая теория)

Теория групп

Элементарная геометрия

Формальная арифметика

Следствие 2.4.2.4. Если существует модель M теории T для которой $M \models A$, то $T \models A$

Пример

Модель Пуанкаре H^2 показывает, что аксиома Евклида независима от остальных аксиом элементарной геометрии.

Теорема 2.4.3 (Геделя о полноте). (1) Всякая непротиворечивая теория T выполнима, то есть имеет модель $M \models T$.

(2) Если $T \not\models A$, то найдётся модель $M \models T$ для которой $M \not\models A$

Покажем равносильность этих утверждений.

(1 \Rightarrow 2) : Если $T \not\models A$, то $T \cup \{\neg A\}$ непротиворечива. Действительно, если $T, \neg A$ противоречива, то $T \vdash \neg\neg A$, а Значит $T \vdash A$ (используем тавтологию $\neg\neg A \rightarrow A$). Следовательно, $T \cup \{\neg A\}$ имеет модель M .

(2 \Rightarrow 1) : Пусть T непротиворечива. Возьмём $A = (B \wedge \neg B)$. Тогда $T \not\models A$, следовательно у теории T должна быть модель (опровергающая A).

Теорема 2.4.4 (Геделя-Мальцева о компактности). Теория T выполнима \iff любое конечное подмножество $T_0 \subseteq T$ выполнимо.

Доказательство. Если T невыполнима, то существует вывод противоречия в T , использующий лишь конечное число аксиом T . \square

Пример.

Пусть $(\mathbb{N}; =, S, +, \cdot, 0)$ - стандартная модель арифметики и $Th(\mathbb{N})$ есть множество всех истинных в \mathbb{N} предложений. Добавим к сигнатуре новую константу c и рассмотрим теорию

$$T = Th(\mathbb{N}) \cup \{\neg c = 0, \neg c = S0, \neg c = SS0, \dots\}$$

Терм $\bar{n} = SS \dots S0$ (n раз) называем нумералом. Нумералы служат именами натуральных чисел.

Лемма 2.4.5. Каждая конечная подтеория $T_0 \subseteq T$ выполнима. Доказательство. T_0 содержит лишь конечное число аксиом вида $c \neq \bar{n}_1, \dots, c \neq \bar{n}_k$. Интерпретируем константу c в стандартной модели как любое число $m > n_1, \dots, n_k$.

По теореме о компактности существует (нормальная) модель $M \models T$. Модель M обладает следующими свойствами:

- \mathbb{N} изоморфна начальному сегменту M ; вложение $\mathbb{N} \rightarrow M$ задаётся функцией $\varphi : n \mapsto \bar{n}_M$.
- $M \models Th(\mathbb{N})$

- $M \not\subseteq \mathbb{N}$, в частности $c_M \in M$ есть «бесконечно большое число», поскольку c_M отлично от всякого $n \in \mathbb{N}$.

Следовательно, те же аксиомы выполнены и в M . Поэтому предикат $<_M$ на M представляет собой строгий линейный порядок с наименьшим элементом 0. При этом каждый элемент имеет последователя, и каждый элемент, кроме 0, имеет непосредственного предшественника.

Доказательство. Если $G_1 < G_2$, возьмём чётные $x_1 \in G_1$ и $x_2 \in G_2$ и рассмотрим $y = (x_1 + x_2) / 2$ (функция $g(x) = x/2$ определима в \mathbb{N} , а значит и в M). Если $y \in G_1$, то $(x_1 + x_2) / 2 = x_1 + \bar{n}$ для некоторого $n \in \mathbb{N}$. Тогда $2x_1 + 2\bar{n} = x_1 + x_2$, откуда $x_1 + 2\bar{n} = x_2$, то есть $x_2 \in G_1$. Аналогично показываем $y \notin G_2$. \square

Глава 3.

Теория Моделей

3.1. Лекция 12 (03.09.2021)

Определение. Пусть T – теория, A – замкнутая формула в ее сигнатуре. A логически следует из T (обозначение: $T \models A$), если любая модель теории T является моделью формулы A .

Теорема 3.1.1 (о корректности для исчисления предикатов). Если $T \vdash A$, то $T \models A$.

Теорема 3.1.2 (Гёделя о полноте для исчисления предикатов). Если $T \models A$, то $T \vdash A$.

Версия для теорий с равенством:

$T \vdash A$ означает выводимость с использованием аксиом равенства. $T \models A$ означает логическое следование на нормальных моделях.

Определение. Пусть M, M' – модели сигнатуры Ω . Отображение носителей $\alpha : M \rightarrow M'$ называется изоморфизмом M на M' , если

- α – биекция,
- $\alpha(c_M) = c_{M'}$ для всех констант c (из Ω)
- $\alpha(f_M(m_1, \dots, m_k)) = f_{M'}(\alpha(m_1), \dots, \alpha(m_k))$ для любого k -местного функционального символа f и $m_1, \dots, m_k \in M$,
- $P_M(m_1, \dots, m_k) = P_{M'}(\alpha(m_1), \dots, \alpha(m_k))$ для любого k -местного предикатного символа P и $m_1, \dots, m_k \in M$. Запись $\alpha : M \cong M'$ означает, что α – изоморфизм M на M' .

Лемма 3.1.3. (1) Если $\alpha : M \cong M'$ и $\beta : M' \cong M''$, то $\beta\alpha : M \cong M''$.

(2) Если $\alpha : M \cong M'$, то $\alpha^{-1} : M' \cong M$.

Определение. Модели M, M' называются изоморфными (обозначение: $M \cong M'$) если существует изоморфизм $\alpha : M \cong M'$. \cong задает отношение эквивалентности на классе всех моделей данной сигнатуры.

Определение. Терм, оцененный в M , – это замкнутый терм расширенной сигнатуры $\Omega(M)$. Из обычного терма $t(a_1, \dots, a_n)$, получаются оцененные термы

$$t(m_1, \dots, m_n) := t[a_1, \dots, a_n / \underline{m_1}, \dots, m_n]$$

$|r|_M$ – значение оцененного терма r в модели M ; это элемент из M .

Определение. Формула, оцененная в M , - это замкнутая формула сигнатуры $\Omega(M)$, $|A|_M$ - значение оцененной формулы A в M (0 или 1)

Пусть M, M' - модели сигнатуры Ω , $\alpha : M \cong M'$. Для терма t , оцененного в M , обозначим через $\alpha \cdot t$ терм, полученный заменой всех констант m из M на их образы $\alpha(m)$. (Формально $\alpha \cdot t$ определяется по индукции) - Аналогично по формуле A , оцененной в M , строится формула $\alpha \cdot A$, оцененная в M' .

Теорема 3.1.4. Пусть M, M' - модели сигнатуры Ω , $\alpha : M \cong M'$.

- Если t - терм, оцененный в M , то $|\alpha \cdot t|_{M'} = \alpha(|t|_M)$.
- Если A - формула, оцененная в M , то $|\alpha \cdot A|_{M'} = |A|_M$ Определение

Пусть M - модель сигнатуры Ω . Элементарная теория модели M - это множество всех замкнутых формул сигнатуры Ω , которые истинны в M .

$$Th(M) := \{A \mid M \models A\}$$

Модели M_1, M_2 одной сигнатуры называются элементарно эквивалентными, если в них истинны одни и те же замкнутые формулы, т.е. $Th(M_1) = Th(M_2)$; обозначение: $M_1 \equiv M_2$.

3.2. Лекция 13 (03.1.2021)

Все сигнатуры с равенством, все модели нормальные.

Определение. Теория сильно категорична, если все ее модели изоморфны.

Теория конечно аксиоматизируема, если она эквивалентна конечной теории.

Теорема 3.2.1. Пусть Ω - конечная сигнатура, M - конечная модель Ω . Тогда

- $Th(M)$ конечно аксиоматизируема.
- $Th(M)$ сильно категорична.

Доказательство. Пусть M - конечная модель конечной сигнатуры Ω . Строим формулу A_M , которая полностью описывает M .

Пусть $M = \{m_1, \dots, m_n\}$. Положим

$$A_M := \exists x_1 \dots \exists x_n B_M(x_1, \dots, x_n)$$

где

$$\begin{aligned} B_M(a_1, \dots, a_n) := & \bigwedge_{1 \leq i < j \leq n} (a_i \neq a_j) \wedge \forall y \bigvee_{i=1}^n (y = a_i) \wedge \\ & \bigwedge \{c = a_i \mid c \in \text{Const } \Omega, M \models c = m_i\} \wedge \\ & \bigwedge \{f(a_{i_1}, \dots, a_{i_k}) = a_j \mid f \in \text{Fun}_\Omega, M \models f(m_{i_1}, \dots, m_{i_k}) = m_j\} \wedge \\ & \bigwedge \{P(a_{i_1}, \dots, a_{i_k}) \mid P \in \text{Pred}_\Omega, M \models P(m_{i_1}, \dots, m_{i_k})\} \wedge \\ & \bigwedge \{\neg P(a_{i_1}, \dots, a_{i_k}) \mid P \in \text{Pred}_\Omega, M \models \neg P(m_{i_1}, \dots, m_{i_k})\} \end{aligned}$$

□

Лемма 3.2.2. Для модели M' сигнатуры Ω

$$M' \models A_M \Leftrightarrow M' \cong M$$

Доказательство. (\Leftarrow) Проверяем $M \models A_M$, это следует из $M \models B_M(m_1, \dots, m_n)$.

(\Rightarrow) Предположим, что $M' \models A_M$ и построим изоморфизм M на M'

По определению истинности, найдутся $m'_1, \dots, m'_n \in M'$, для которых

$$M' \models B_M(m'_1, \dots, m'_n)$$

Докажем, что отображение φ , переводящее каждый m_i в m'_i - искомый изоморфизм \square

Доказательство. Окончание доказательства теоремы.

Заметим: $Th(M) \sim \{A_M\}$. 1. По лемме 1.7 $A_M \in Th(M)$ и значит,

$$M' \models Th(M) \Rightarrow M' \models A_M$$

2. Обратно, если $M' \models A_M$, то по лемме 1.7, $M' \cong M$. И тогда $M' \models Th(M)$ \square

$Th(M)$ сильно категорична, т.к. эквивалентная ей теория $\{A_M\}$ сильно категорична по лемме

Следствие 3.2.2.1. Если M — конечная модель и $M' \equiv M$, то $M' \cong M$.

Доказательство. Если $M' \equiv M$, то $M' \models Th(M)$. Тогда, по теореме 1.6, $M' \cong M$ \square

k -местный предикат на множестве M — это отображение $\gamma : M^k \rightarrow \{0, 1\}$

k -местное отношение на множестве M — это множество $R \subset M^k$.

Рассмотрим формулу $A(\vec{b})$, где $\vec{b} = (b_1, \dots, b_k)$. k -местный предикат, определяемый формулой $A(\vec{b})$ в модели M , — это $A_M : M^k \rightarrow \{0, 1\}$ такое, что для всех m_1, \dots, m_k

$$A_M(m_1, \dots, m_k) = |A(m_1, \dots, m_k)|_M$$

Теорема 3.2.3. Пусть α — автоморфизм модели, $A(b_1, \dots, b_k)$ — формула в ее сигнатуре. Тогда для всех $m_1, \dots, m_k \in M$

$$A_M(\alpha(m_1), \dots, \alpha(m_k)) = A_M(m_1, \dots, m_k)$$

В сокращенной записи:

$$A_M(\alpha \vec{m}) = A_M(\vec{m})$$

Таким образом, определяемый в M предикат инвариантен при всех автоморфизмах M

3.3. Лекция 14 (03.22.2021)

Определение. Пусть M, M' — модели сигнатуры Ω . M' — подмодель M , если

- $M' \subset M$ как множество,

- $c_M = c_{M'}$ для всех $c \in \text{Const } \Omega$,

- $f_M(m_1, \dots, m_k) = f_{M'}(m_1, \dots, m_k)$ для всех k -местных $f \in \text{Fun } \Omega$ и $m_1, \dots, m_k \in M'$,

- $P_M(m_1, \dots, m_k) = P_{M'}(m_1, \dots, m_k)$ для всех k -местных $P \in \text{Pred}_\Omega$ и $m_1, \dots, m_k \in M'$.

Обозначение подмодели: $M' \subset M$.

Определение. Подмодель $M' \subset M$ – элементарная, если

$$M' \models A(m_1, \dots, m_k) \Leftrightarrow M \models A(m_1, \dots, m_k)$$

для любой формулы $A(a_1, \dots, a_k)$ и $m_1, \dots, m_k \in M'$. (Тогда, в частности, $M' \equiv M$.)
Обозначение элементарной подмодели: $M' \prec M$.

Мощность сигнатуры Ω

$$|\Omega| := | \text{Const}_\Omega \cup \text{Fun}_\Omega \cup \text{Pred}_\Omega |$$

Теорема 3.3.1 (Лёвенгейм - Сколем - Тарский). Для любой модели M сигнатуры Ω существует $M' \prec M$ такая, что

$$|M'| \leq \max(|\Omega|, \aleph_0)$$

Определение. Зафиксируем модель M и $m_0 \in M$. Для каждой формулы $\exists x A(x, \vec{a})$, где $\vec{a} = (a_1, \dots, a_k)$ – список свободных переменных, и для каждого $\vec{m} \in M^k$ положим

$$S_{\exists x A(x, \vec{m})} := \begin{cases} \{e \in M \mid M \models A(e, \vec{m})\}, & \text{если это множество непусто;} \\ m_0, & \text{иначе.} \end{cases}$$

Функция выбора для семейства множеств $(S_{\exists x A(x, \vec{m})})_{\vec{m} \in M^k}$ называется сколемовской функцией для формулы $\exists x A(x, \vec{a})$ и обозначается $s_{\exists x A(x, \vec{a})}$ (или короче: $s_{\exists x A}$). (Случай $k = 0$ тоже включается; тогда просто берем $s_{\exists x A} \in M$.) Таким образом:

$$s_{\exists x A}(\vec{m}) \in S_{\exists x A(x, \vec{m})}$$

и тогда

$$M \models A(s_{\exists x A}(\vec{m}), \vec{m})$$

если

$$M \models \exists x A(x, \vec{m})$$

Доказательство. Пусть $M_0 := \{m_0\}$ (это множество, еще не модель). По рекурсии строим счетную последовательность множеств $M_0 \subset M_1 \subset M_2 \dots$ Их объединение даст M' .

$$\begin{aligned} M_{n+1} &:= M_n \cup \left\{ s_{\exists x A(x, \vec{a})} [M_n^k] \mid \exists x A(x, \vec{a}) \in Fm \right\}, \\ (Fm &\text{ – множество всех формул нашей сигнатуры}). \\ M' &:= \bigcup_n M_n \text{ (как множество)}. \end{aligned}$$

Его можно превратить в модель $M' \subset M$, положив - $M' \models P(\vec{m}) \Leftrightarrow M \models P(\vec{m})$,

- $c_{M'} = s_{\exists x}(x = c)$

- $f_{M'}(\vec{m}) = s_{\exists x(x=f(\vec{a}))}(\vec{m})$.

Доказываем, что $M' \prec M$ – искомая. □

3.4. Лекция 15 (03.23.2021)

Определение. Фильтр на множестве I — это непустое $\mathcal{F} \subset \mathcal{P}(I)$ со свойствами $\bullet X, Y \in \mathcal{F} \Rightarrow (X \cap Y) \in \mathcal{F}$ $\bullet X \in \mathcal{F} \& X \subset Y \Rightarrow Y \in \mathcal{F}$ Фильтр \mathcal{F} собственный, если $\emptyset \notin \mathcal{F}$ Ультрафильтр — максимальный по включению собственный фильтр.

Лемма 3.4.1. Свойства ультрафильтров:

- $X \in \mathcal{F} \& Y \in \mathcal{F} \Leftrightarrow (X \cap Y) \in \mathcal{F}$
- $X \notin \mathcal{F} \Leftrightarrow (I \setminus X) \in \mathcal{F}$

Лемма 3.4.2. Любой собственный фильтр можно расширить до ультрафильтра,

Определение. Фильтр \mathcal{F} главный, если $\bigcap \mathcal{F} \neq \emptyset$.

Лемма 3.4.3. Ультрафильтр \mathcal{U} главный, если и только если существует конечное $J \in \mathcal{U}$.

Определение. Пусть задан ультрафильтр \mathcal{U} на I . Рассмотрим свойства элементов I (одно-местные предикаты). Свойство Φ верно почти всегда (относительно \mathcal{U}), если

$$\{i \mid \Phi(i)\} \in \mathcal{U}$$

Обозначение: $\forall^\infty i \Phi(i)$.

Лемма 3.4.4. Свойства квантора \forall^∞ .

- $\forall^\infty i (\Phi(i) \wedge \Psi(i)) \Leftrightarrow \forall^\infty i \Phi(i) \wedge \forall^\infty i \Psi(i)$
- $\forall^\infty i \neg \Phi(i) \Leftrightarrow \neg \forall^\infty i \Phi(i)$.

Лемма 3.4.5. Пусть $(M_i)_{i \in I}$ — семейство моделей сигнатуры Ω, \mathcal{U} ультрафильтр на I . Тогда

$$\alpha \approx_{\mathcal{U}} \beta := \forall^\infty i (\alpha_i = \beta_i)$$

задает отношение эквивалентности на множестве $\prod M_i$.

Класс элемента $(\alpha_i)_{i \in I}$ обозначается $[\alpha_i]_{i \in I}$.

Определение. Пусть $(M_i)_{i \in I}$ — семейство моделей сигнатуры Ω . \mathcal{U} — ультрафильтр на I . Ультрапроизведение семейства $(M_i)_{i \in I}$ по ультрафильтру \mathcal{U} задается следующим образом.

- Носитель M это $\prod_{i \in I} M_i / \approx_{\mathcal{U}}$. $c_M := [c_{M_i}]_{i \in I}$ $f_M([m_i^1], \dots, [m_i^k]) := [f_{M_i}(m_i^1, \dots, m_i^k)]$
- $M \models P([m_i^1], \dots, [m_i^k]) \Leftrightarrow \forall^\infty i M_i \models P(m_i^1, \dots, m_i^k)$ Обозначение: $\prod_{\mathcal{U}} M_i$.

Теорема 3.4.6 (Лось).

$$\prod_{\mathcal{U}} M_i \models A([m_i^1], \dots, [m_i^k]) \Leftrightarrow \forall^\infty i M_i \models A(m_i^1, \dots, m_i^k)$$

3.5. Лекция 16 (04.05.2021)

Теорема 3.5.1 (Гёделя - Мальцева). Пусть T — теория в некоторой сигнатуре. Если каждое конечное подмножество T выполнимо, то T выполнима.

Доказательство. Рассмотрим

$$I := \{S \subset T \mid I \text{ конечно} \}.$$

Для каждого $S \in I$ существует модель $M_S \models S$.

Для $A \in T$ пусть

$$J_A := \{S \in I \mid A \in S\}$$

□

Лемма 3.5.2. Существует ультрафильтр на I , содержащий все J_A .

Доказательство. $J_{A_1} \cap \dots \cap J_{A_k} \neq \emptyset$, т.к. содержит $\{A_1, \dots, A_k\}$. Поэтому найдется фильтр, содержащий все такие пересечения. Пусть \mathcal{U} содержит все J_A для $A \in T$. Тогда

$$\prod_{\mathcal{U}} M_S \models T.$$

Действительно,

$$J_A \in \mathcal{U} \Leftrightarrow \forall^\infty S A \in S.$$

Тогда

$$\forall^\infty S M_S \models A$$

По теореме Лося,

$$\prod_{\mathcal{U}} M_S \models A.$$

□

Теорема 3.5.3. Если теория имеет конечные модели неограниченной мощности, то она имеет и бесконечную модель.

Теорема 3.5.4 (Лёвенгейма - Сколема о подъеме). Если теория в сигнатуре Ω имеет бесконечную модель, то она имеет модели любой бесконечной мощности $k \geq |\Omega|$.

3.6. Лекция 21 (04.27.2021)

Рассматриваем модели в конечной сигнатуре Ω без функциональных символов. Игра Эренфойхта $G_n(M, \mathbf{m}, M', \mathbf{m}')$ длины n на моделях M, M' с начальной позицией $(\mathbf{m}, \mathbf{m}')$, где $\mathbf{m} \in M^k$, $\mathbf{m}' \in M'^k$ для некоторого k описывается правилами:

- Ходы делаются поочередно, первый ход делает \forall , каждый игрок делает n ходов.
- Ход \forall — это пара (M, l) , где $l \in M$ или (M', l') . Ответный ход \exists — в другой модели.
- Партия — последовательность ходов по этим правилам. Законченная партия — длины $2n$.

Последняя позиция $p(\pi)$ в партии π определяется по рекурсии:

$p() = (\mathbf{m}, \mathbf{m}')$. Если $p(\pi) = (\mathbf{d}, \mathbf{e})$, то

$$p(\pi, (M, l)) = (dl, \mathbf{e}), p(\pi, (M', l')) = (\mathbf{d}, \mathbf{e}l')$$

- \exists выигрывает законченную партию π , если $p(\pi)$ задает частичный изоморфизм.

Частичный изоморфизм: $M, \mathbf{m} \equiv_0 M', \mathbf{m}'$, если

$$M \models A(\mathbf{m}) \Leftrightarrow M' \models A(\mathbf{m}')$$

для любой простой атомарной $A(\mathbf{a})$. Простые атомарные формулы:

$$a_i = a_j, a_i = c, P(a_1, \dots, a_n)$$

Определение. Стратегия для \exists . σ : партии нечетной длины $< 2n \rightarrow$ допустимые ходы

Партия $\pi = \chi_1, \dots, \chi_{2n}$ согласована с σ , если

$$\forall p < n \chi_{2p} = \sigma(\chi_1, \dots, \chi_{2p-1})$$

σ - выигрышная для \exists , если для любой партии π , согласованной с σ , π выиграна \exists

Определение. Игровая эквивалентность $(M, \mathbf{m}) \approx_n (M', \mathbf{m}')$, если \exists имеет выигрышную стратегию в $G_n(M, \mathbf{m}, M', \mathbf{m}')$.

Лемма 3.6.1. \approx_n задает отношение эквивалентности.

Лемма 3.6.2. (Индуктивное определение \approx_n) $(M, \mathbf{m}) \approx_{n+1} (M', \mathbf{m}') \Leftrightarrow \begin{cases} \forall d \in M \exists d' \in M'(M, \mathbf{m}d) \approx_n (M', \mathbf{m}'d') \\ \forall d' \in M' \exists d \in M(M, \mathbf{m}d) \approx_n (M', \mathbf{m}'d') \end{cases}$

Определение. $q(A)$ — кванторная глубина формулы A определяется по рекурсии:

$q(A) = 0$ для атомарной A ,

$q(\neg A) = q(A)$

$q(A * B) = \max(q(A), q(B))$, где $*$ - бинарная связка,

$q(\forall x A[a \setminus x]) = q(\exists x A[a \setminus x]) = q(A) + 1$.

Определение. Формульная эквивалентность $(M, \mathbf{m}) \equiv_n (M', \mathbf{m}')$, если для любой простой формулы $A(\mathbf{a})$, где $q(A) \leq n$

$$M \models A(\mathbf{m}) \Leftrightarrow M' \models A(\mathbf{m}')$$

Теорема 3.6.3 (Эренфойхта - Фраиссе).

$$(M, \mathbf{m}) \approx_n (M', \mathbf{m}') \Leftrightarrow (M, \mathbf{m}) \equiv_n (M', \mathbf{m}').$$

Следствие 3.6.3.1.

$$M \equiv M' \Leftrightarrow \forall n M \approx_n M'.$$

Рассмотрим сигнатуру Ω_1 с 1-местными предикатами и равенством.

Определение. Замкнутая формула A финитно выполнима, если она имеет конечную модель

Теорема 3.6.4 (Лёвенгейм, 1915). Всякая выполнимая формула A сигнатуры Ω_1 выполнима в модели мощности $\leq 2^k \cdot n$, где $n = q(A)$ (для простой A), k — число предикатных символов в A .

Следствие 3.6.4.1. Конечный спектр формулы в Ω_1 не может быть равен $2\mathbf{N}$.

Определение. Бесконечная игра Эренфойхта $G_\omega(M, \mathbf{m}, M', \mathbf{m}')$ задается теми же правилами, что $G_n(M, \mathbf{m}, M', \mathbf{m}')$, с отличиями:

число ходов бесконечно,

бесконечная партия выиграна \exists , если выигран любой ее начальный отрезок четной длины.

Игровая эквивалентность $M \approx_\omega M'$ определяется соответственно.

Теорема 3.6.5. Для счетных моделей сигнатуры Ω

$$M \approx_\omega M' \Leftrightarrow M \cong M'$$

Теорема 3.6.6 (Кантор). Теория DLO_{\leftrightarrow} счетно категорична.

Глава 4.

Алгоритмы

4.1. Лекция 22 (05.11.2021)

- Процесс применения алгоритма \mathcal{A}_K данным $x \in X$ происходит по шагам.
 - Процесс или заканчивается после конечного числа шагов с результатом $y \in Y$, или останавливается без результата или продолжается бесконечно.
 - Таким образом, с алгоритмом \mathcal{A} связывается частичная функция $f : X \rightarrow Y$
- Мы будем говорить: Алгоритм \mathcal{A} вычисляет функцию f .

Определение. Частичной функцией $f : X \rightarrow Y$ называется подмножество $f \subseteq X \times Y$ такое, что из $\langle x, y_1 \rangle \in f$ и $\langle x, y_2 \rangle \in f$ следует $y_1 = y_2$.

Пишем $f(x) = y$ вместо $\langle x, y \rangle \in f$;
 $!f(x)$ вместо $\exists y f(x) = y$

Определение. Областью определения частичной функции f называется множество $\text{dom}(f) := \{x \in X : \exists y \in Y \langle x, y \rangle \in f\}$

Определение. Областью значений частичной функции f называется множество $\text{rng}(f) := \{y \in Y : \exists x \in X \langle x, y \rangle \in f\}$.

Определение. Частичная функция $f : X \rightarrow Y$ вычислима, если она вычисляется некоторым алгоритмом.

В частности, можно говорить о вычислимых функциях $f : \Sigma^* \rightarrow \Sigma^*$, $f : \mathbb{N}^k \rightarrow \mathbb{N}$ и т.д.

Теорема 4.1.1. Каждая из вышеперечисленных моделей определяет один и тот же класс вычислимых частичных функций $f : \Sigma^* \rightarrow \Sigma^*$.

Такие модели (языки программирования) называются полными по Тьюрингу.

Теорема 4.1.2 (Тезис Черча-Тьюринга). Любая вычислимая в интуитивном смысле частичная функция $f : \Sigma^* \rightarrow \Sigma^*$ вычислима на машине Тьюринга.

Замечание

Это утверждение не является математическим, но говорит об адекватности математической модели (вычислимости по Тьюрингу) реальному явлению (вычислимости).

Теорема 4.1.3. Всякая функция $f : \Sigma^* \rightarrow \Sigma^*$, вычислимая на (идеализированном) физически реализуемом устройстве, вычислима на машине Тьюринга.

Замечание

Физический тезис предполагает возможность аналогового вычисления, квантово-механические эффекты и т.д.

Машина Тьюринга задаётся конечными

- рабочим алфавитом Σ , содержащим символ $\#$ (пробел);
- множеством состояний Q , содержащим состояния q_1 (начальное) и q_0 (конечное);
- набором команд (программой) P

- Команды имеют вид $qa \rightarrow rb\nu$, где $q, r \in Q, a, b \in \Sigma$ и $\nu \in \{L, N, R\}$. «прочтя символ a в состоянии q перейти в состояние r , заменить содержимое ячейки на b и сместиться влево (L), остаться на месте (N) или сместиться вправо (R) на одну ячейку, в зависимости от значения ν » - Требуется, чтобы в программе P была ровно одна команда с левой частью qa для каждого $q \in Q/\{q_0\}$ и $a \in \Sigma$

Определение. Машина Тьюринга есть набор $M = \langle Q, \Sigma, P, q_0, q_1 \rangle$.

Определение. Конфигурация машины M определяется содержимым ленты, состоянием и положением головки. Конфигурация записывается словом вида $XqaY$, где

- $XaY \in \Sigma^*$ есть содержимое ленты,
- $q \in Q$ есть состояние M .
- головка обозревает символ a .

Определение. M вычисляет частичную функцию $f : \Delta^* \rightarrow \Delta^*$, если для каждого $x \in \Delta^*$

- если $x \in \text{dom}(f)$, то начав работу в конфигурации $q_1\#x$ машина M останавливается в конфигурации $q_0\#f(x)$;
- если $x \notin \text{dom}(f)$, то машина M не останавливается.

Глава 5.

Дополнительно

Литература