

Логика предикатов
лекция 8

Лев Дмитриевич Беклемишев
<http://lpcs.math.msu.su/vml2010>

lbekl@yandex.ru

01.04.2010

Исчисление предикатов

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

Аксиомы:

A1. аксиомы исчисления высказываний,

A2. $\forall xA[a/x] \rightarrow A[a/t]$,

A3. $A[a/t] \rightarrow \exists xA[a/x]$.

Здесь A — любая формула сигнатуры Σ и t — любой терм (x не входит в A).

Правила вывода:

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

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

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

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

Правила R2 и R3 называются *правилами Бернайса*.

Выводимость

Опр.

Выводом в исчислении предикатов называется конечная последовательность формул, каждая из которых либо является аксиомой, либо получается из предыдущих формул по одному из правил вывода *R1 – R3*.

Пример.

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

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

Выводимость

Опр.

Выводом в исчислении предикатов называется конечная последовательность формул, каждая из которых либо является аксиомой, либо получается из предыдущих формул по одному из правил вывода $R1 - R3$.

Пример.

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

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

Опр.

Формула A называется *выводимой* в исчислении предикатов или *теоремой* исчисления предикатов (обозначение $\vdash A$), если существует вывод, в котором последняя формула есть A .

Пример.

$\vdash \forall xA[a/x] \rightarrow \forall yA[a/y]$ для любой формулы A .

Выводы в теории

Опр.

Выводом в теории T называется конечная последовательность формул, каждая из которых либо принадлежит множеству T , либо является логической аксиомой вида $A1 - A3$, либо получается из предыдущих формул по одному из правил вывода $R1 - R3$.

Доказуемость, опровержимость

Опр.

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 .

Опр.

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

Опр.

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

Доказуемость, опровержимость

Опр.

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 .

Опр.

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

Опр.

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

Доказуемость, опровержимость

Опр.

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 .

Опр.

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

Опр.

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

Свойства выводимости

- 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*).

Свойства выводимости

- 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*).

Свойства выводимости

- 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*).

Эквивалентность теорий

Пусть T , U — теории сигнатуры Σ .

Опр.

U содержит T , если для любой $A \in T$ $U \vdash A$
(обозначение $U \vdash T$).

Опр.

T и U (дедуктивно) эквивалентны, если $T \vdash U$ и $U \vdash T$ (обозначение $T \equiv U$).

Эквивалентность теорий

Пусть T, U — теории сигнатуры Σ .

Опр.

U содержит T , если для любой $A \in T$ $U \vdash A$
(обозначение $U \vdash T$).

Опр.

T и U (дедуктивно) эквивалентны, если $T \vdash U$ и $U \vdash T$ (обозначение $T \equiv U$).

Теорема о тавтологии

Предложение.

Если $A(P_1, \dots, P_n)$ выводима в исчислении высказываний, то для любых формул C_1, \dots, C_n сигнатуры Σ формула $A[P_1/C_1, \dots, P_n/C_n]$ выводима в исчислении предикатов.

Доказательство.

Индукция по построению вывода формулы A .

Теорема о дедукции

Теорема.

Для любой теории T и замкнутой формулы A

$$T, A \vdash B \iff T \vdash A \rightarrow B.$$

Доказательство.

Индукция по длине вывода $T, A \vdash B$. Разбираем лишь новые случаи, относящиеся к правилам $R2$ и $R3$.

Теорема о дедукции

Теорема.

Для любой теории T и замкнутой формулы A

$$T, A \vdash B \iff T \vdash A \rightarrow B.$$

Доказательство.

Индукция по длине вывода $T, A \vdash B$. Разбираем лишь новые случаи, относящиеся к правилам $R2$ и $R3$.

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

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

Рассмотрим тавтологию

$$(P \rightarrow (Q \rightarrow R)) \leftrightarrow (P \wedge Q \rightarrow R).$$

Подставляя A вместо P , C вместо Q и D вместо R получаем, что формула

$$(A \rightarrow (C \rightarrow D)) \leftrightarrow (A \wedge C \rightarrow D)$$

выводима в исчислении предикатов.

Таким образом, вывод $A \rightarrow (C \rightarrow D)$ в T можно продолжить:

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

$$(A \rightarrow (C \rightarrow D)) \rightarrow (A \wedge C \rightarrow D) \quad (\text{тавтология})$$

$$(A \wedge C) \rightarrow D \quad (\text{MP})$$

$$(A \wedge C) \rightarrow \forall x D[a/x] \quad (\text{R2, } A \text{ замкнута})$$

$$A \rightarrow (C \rightarrow \forall x D[a/x]) \quad (\text{аналогично})$$

Правило $R3$ рассматривается аналогично.

Непротиворечивость теории

Опр.

Теорией сигнатуры Σ называем произвольное множество T замкнутых формул языка \mathcal{L}_Σ .

Опр.

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

Следствие.

$T \cup \{A\}$ противоречива $\iff T \vdash \neg A$.

Непротиворечивость теории

Опр.

Теорией сигнатуры Σ называем произвольное множество T замкнутых формул языка \mathcal{L}_Σ .

Опр.

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

Следствие.

$T \cup \{A\}$ противоречива $\iff T \vdash \neg A$.

Непротиворечивость теории

Опр.

Теорией сигнатуры Σ называем произвольное множество T замкнутых формул языка \mathcal{L}_Σ .

Опр.

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

Следствие.

$T \cup \{A\}$ противоречива $\iff T \vdash \neg A$.

Теорема о корректности исчисления предикатов

Теорема.

Если $M \models T$ и $T \vdash A$, то $M \models A$.

Доказательство.

Индукция по длине вывода A в T .

Следствие.

Если $\vdash A$, то A общезначима.

Теорема о корректности исчисления предикатов

Теорема.

Если $M \models T$ и $T \vdash A$, то $M \models A$.

Доказательство.

Индукция по длине вывода A в T .

Следствие.

Если $\vdash A$, то A общезначима.

Доказательства непротиворечивости

Следствие.

Если теория T имеет модель, то T непротиворечива.

Следствие.

Следующие теории непротиворечивы:

- исчисление предикатов (пустая теория);
- теория отношения эквивалентности;
- теория групп;
- элементарная геометрия.

Доказательства независимости

Следствие.

Если существует модель M теории T для которой $M \not\models A$, то $T \not\models A$.

Пример.

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

Теорема Гёделя о полноте

Теорема.

- 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 $M \not\models A$.
- 3 $T \models A$ влечёт $T \vdash A$.

Покажем равносильность этих утверждений.

(1 \Rightarrow 2) : Если $T \not\models A$, то по теореме о дедукции $T \cup \{\neg A\}$ непротиворечива. Следовательно, $T \cup \{\neg A\}$ имеет модель M .

(2 \Rightarrow 3) : очевидно.

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

Покажем равносильность этих утверждений.

(1 \Rightarrow 2) : Если $T \not\models A$, то по теореме о дедукции $T \cup \{\neg A\}$ непротиворечива. Следовательно, $T \cup \{\neg A\}$ имеет модель M .

(2 \Rightarrow 3) : очевидно.

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

Покажем равносильность этих утверждений.

(1 \Rightarrow 2) : Если $T \not\vdash A$, то по теореме о дедукции $T \cup \{\neg A\}$ непротиворечива. Следовательно, $T \cup \{\neg A\}$ имеет модель M .

(2 \Rightarrow 3) : очевидно.

(3 \Rightarrow 1) : Возьмём $A = (B \wedge \neg B)$. Тогда $T \not\vdash A$, следовательно $T \not\vdash A$ и у теории T должна быть модель (опровергающая A).

Покажем равносильность этих утверждений.

$(1 \Rightarrow 2)$: Если $T \not\models A$, то по теореме о дедукции $T \cup \{\neg A\}$ непротиворечива. Следовательно, $T \cup \{\neg A\}$ имеет модель M .

$(2 \Rightarrow 3)$: очевидно.

$(3 \Rightarrow 1)$: Возьмём $A = (B \wedge \neg B)$. Тогда $T \not\models A$, следовательно $T \not\models A$ и у теории T должна быть модель (опровергающая A).

Теорема Мальцева о компактности

Теорема.

- 1 Теория T выполнима \iff любое конечное подмножество $T_0 \subseteq T$ выполнимо.
- 2 $T \models A \iff$ существует такое конечное множество $T_0 \subseteq T$, что $T_0 \models A$.

Нестандартные модели арифметики

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

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

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

Утверждение.

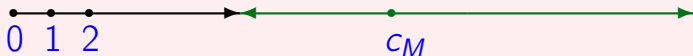
Каждая конечная подтеория $T_0 \subseteq T$ выполнима.

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 $\varphi : n \mapsto \bar{n}_M$.
- $M \models Th(\mathbb{N})$;
- $M \not\cong \mathbb{N}$, в частности $c_M \in M$ есть «бесконечно большое число», поскольку c_M отлично от всякого $n \in \mathbb{N}$.

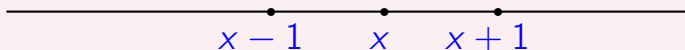


Порядок на модели M

Формула $a < b \Leftrightarrow \exists x (x \neq 0 \wedge a + x = b)$ определяет порядок в \mathbb{N} . Для данной формулы в \mathbb{N} выполнены аксиомы строгого линейного порядка и следующие предложения:

- $\forall x (0 < x \vee 0 = x)$;
- $\forall x \exists y (x < y \wedge \forall z (z < y \rightarrow z = x \vee z < x))$;
- $\forall y (y \neq 0 \rightarrow \exists x (x < y \wedge \forall z (z < y \rightarrow \rightarrow z = x \vee z < x)))$.

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.



Опр.

Элементы $x, y \in M$ *близки*, если для некоторого $n \in \mathbb{N}$ выполнено $y = SS \dots S(x)$ или $x = SS \dots S(y)$ (n символов S).

Классы эквивалентности по отношению близости называем *галактиками*.

Утверждение.

Если G — галактика в M , $G \neq \mathbb{N}$, то порядок $(G, <_M)$ изоморфен $(\mathbb{Z}, <)$.

Пусть \mathcal{G} есть множество всех галактик в M .
Определим $G_1 <_M G_2$, если для любых $x \in G_1$,
 $y \in G_2$ $x <_M y$.

Теорема.

Порядок $(\mathcal{G}, <_M)$ есть плотный порядок без
наибольшего элемента и с наименьшим
элементом \mathbb{N} .

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 $y \notin G_2$.

Пусть St_Σ — множество предложений сигнатуры Σ

Опр.

Элементарная теория модели M есть множество
 $Th(M) \equiv \{A \in St_\Sigma : M \models A\}$.

Элементарная эквивалентность

Опр.

Модели M и N сигнатуры Σ *элементарно эквивалентны* ($M \equiv N$), если в M и в N истинны одни и те же предложения Σ , т.е. если $Th(M) \equiv Th(N)$.

Утверждение.

$M \cong N$ влечёт $M \equiv N$. Обратное, вообще говоря, неверно.

Подмодели

Опр.

$(N; \Sigma)$ есть *подмодель* модели $(M; \Sigma)$, если $N \subseteq M$ и для всех $P \in \text{Pred}_\Sigma$, $f \in \text{Func}_\Sigma$, $c \in \text{Const}_\Sigma$ имеем $P_N = P_M \upharpoonright N$, $c_M \in N$, N замкнуто относительно f_M и $f_N = f_M \upharpoonright N$.

Пример.

Если $(G; \cdot, 1, x^{-1})$ — группа, то подмодели G суть подгруппы группы G . Если же G рассматривается как модель $(G; \cdot, 1)$, то её подмоделями будут подполугруппы с единицей группы G .

Элементарные подмодели

Опр.

Подмодель $(N; \Sigma)$ модели $(M; \Sigma)$ *элементарна* (обозначение $N \preceq M$), если для всех $A \in \text{Fm}_\Sigma$

$$\forall \vec{x} \in N (N \models A[\vec{x}] \iff M \models A[\vec{x}]).$$

Утверждение.

$N \preceq M$ влечёт $N \equiv M$.

Пример.

Если M — нестандартная модель $\text{Th}(\mathbb{N})$, то $\mathbb{N} \preceq M$.

Теорема Лёвенгейма–Сколема

Пусть Σ — счётная сигнатура.

Теорема.

Всякая модель $(M; \Sigma)$ имеет (конечную или) счётную элементарную подмодель.

Следствие.

Всякая непротиворечивая теория в счётной сигнатуре имеет (конечную или) счётную модель.

Следствия

- Существуют счётные модели $Th(\mathbb{R})$ и $Th(\mathbb{C})$.
- Существует счётная модель элементарной геометрии.
- Если теория множеств ZFC непротиворечива, то существует и счётная модель ZFC .

Доказательство.

Построим последовательность счётных подмножеств M $N_0 \subseteq N_1 \subseteq N_2 \subseteq \dots$ такую, что

- N_0 — непустое счётное подмножество M .
- Для каждой формулы $A[a, \vec{b}]$ и набора $\vec{y} \in N_k$, если $M \models \exists v A[v, \vec{y}]$ выберем $x \in M$ такой, что $M \models A[x, \vec{y}]$. Добавим все такие x к N_k и получим N_{k+1} .

Положим $N \Leftrightarrow \bigcup_{k \geq 0} N_k$.

Лемма.

Для любой формулы A и всех $\vec{y} \in N$

$$M \models \exists v A[v, \vec{y}] \iff \exists x \in N \ M \models A[x, \vec{y}].$$

Лемма.

N есть подмодель M .

Доказательство.

Пусть $\vec{x} \in N$, $f \in \text{Func}_\Sigma$. Поскольку

$M \models \exists v f(\vec{x}) = v$, имеем $y \in N$ такой, что

$M \models f(\vec{x}) = y$, т.е. $f_M(\vec{x}) \in N$.

Индукцией по построению A теперь покажем

$$\forall \vec{y} \in N (N \models A[\vec{y}] \iff M \models A[\vec{y}]).$$

- Для атомарных формул A следует из того, что N — подмодель M .
- Для $A = \neg B$, $B \wedge C$, $B \vee C$ вытекает из предположения индукции.
- Допустим $A = \exists v B[a/v]$. Тогда

$$\begin{aligned} M \models \exists v B[a/v, \vec{y}] &\iff \exists x \in N \ M \models B[x, \vec{y}] \\ &\iff \exists x \in N \ N \models B[x, \vec{y}] \iff N \models \exists v B[a/v, \vec{y}]. \end{aligned}$$

Обобщение о понижении мощности

Теорема.

Пусть $(M; \Sigma)$ — бесконечная модель в счётной сигнатуре и $\lambda \leq |M|$ — бесконечная мощность.

Тогда найдётся подмодель $N \preceq M$ такая, что $|N| = \lambda$.

Доказательство.

Та же конструкция, но начинаем с любого подмножества $N_0 \subseteq M$ мощности λ .

Теорема Мальцева о повышении мощности

Пусть Σ — счётная сигнатура.

Теорема.

Для любой бесконечной модели $(M; \Sigma)$ и мощности $\lambda \geq |M|$ найдётся модель $(N; \Sigma)$ такая, что $M \preccurlyeq N$ и $|N| = \lambda$.

Доказательство.

Возьмём $X \supseteq M$, $|X| = \lambda$. Рассмотрим сигнатуру $\Sigma_X \Rightarrow \Sigma \cup \{\underline{c} : c \in X\}$ и теорию $T := Th(M; \Sigma_X) \cup \{\underline{c} \neq \underline{d} : c, d \in X, c \neq d\}$.

Каждая конечная подтеория T совместна. По теореме о компактности T имеет нормальную модель N . Но функция $\varphi : c \mapsto (\underline{c})_N$ инъективна в силу аксиом T , следовательно $|N| \geq |X| = \lambda$. Т.к. $N \models Th(M; \Sigma_X)$, то $\varphi(M)$ есть подмодель N , изоморфная M и $\varphi(M) \preceq N$.

Следствие.

Если теория T имеет бесконечную модель, то T имеет модели любой бесконечной мощности.

Следствие.

Множество $Th(\mathbb{N})$ всех предложений истинных в стандартной модели арифметики имеет модели любой бесконечной мощности.