

Логика предикатов
лекция 5

Лев Дмитриевич Беклемишев
<http://lpcs.math.msu.su/vml2008>

lbek1@yandex.ru

6.03.2008

Предикаты и функции

Пусть M — непустое множество.

- *n -арный предикат на M* : подмножество $Q \subseteq M^n$

$$Q(x_1, \dots, x_n) \stackrel{\text{def}}{\iff} \langle x_1, \dots, x_n \rangle \in Q$$

- *n -арная функция на M* : функция $f : M^n \rightarrow M$
- *константа*: элемент M

Опр.

Сигнатурой называется некоторая совокупность имён функций, предикатов и констант. Сигнатура Σ задаётся:

- Pred_Σ предикатные символы;
- Func_Σ функциональные символы;
- Const_Σ символы констант;
- функция *валентности* (число аргументов):

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

Модели

Опр.

Модель сигнатуры Σ есть непустое множество M вместе с отображением (*интерпретацией*), сопоставляющим

- каждому $P \in \text{Pred}_\Sigma$ некоторый предикат P_M 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 $c_M \in M$.

- Модели называют также *алгебраическими системами* или *интерпретациями*.
- Множество M называют *носителем* или *универсумом* данной интерпретации (модели).
- Модель сигнатуры Σ с носителем M обозначается $(M; \Sigma)$ (если интерпретация символов сигнатуры известна).

- Модели называют также *алгебраическими системами* или *интерпретациями*.
- Множество M называют *носителем* или *универсумом* данной интерпретации (модели).
- Модель сигнатуры Σ с носителем M обозначается $(M; \Sigma)$ (если интерпретация символов сигнатуры известна).

- Модели называют также *алгебраическими системами* или *интерпретациями*.
- Множество M называют *носителем* или *универсумом* данной интерпретации (модели).
- Модель сигнатуры Σ с носителем M обозначается $(M; \Sigma)$ (если интерпретация символов сигнатуры известна).

Примеры

Пример.

Стандартная модель арифметики:

$(\mathbb{N}; =, S, +, \times, 0)$

- $S(x) \Rightarrow x + 1$ есть одноместная функция следования;
- $+$ бинарная функция сложения;
- \times бинарная функция умножения;
- 0 константа ноль.

Пример.

Кольцо целых чисел:

$(\mathbb{Z}; =, +, -, \times, 0, 1)$

Здесь « $-$ » есть одноместная функция $x \mapsto -x$.

Пример.

Любое другое кольцо может рассматриваться как модель той же сигнатуры, например:

- $\mathbb{Q}[X]$ — кольцо многочленов над полем \mathbb{Q} ;
- \mathbb{Z}_n — кольцо вычетов по модулю n ;
- $M_n(\mathbb{R})$ — кольцо матриц порядка n над \mathbb{R} .

Пример.

Кольцо целых чисел:

$(\mathbb{Z}; =, +, -, \times, 0, 1)$

Здесь « $-$ » есть одноместная функция $x \mapsto -x$.

Пример.

Любое другое кольцо может рассматриваться как модель той же сигнатуры, например:

- $\mathbb{Q}[X]$ — кольцо многочленов над полем \mathbb{Q} ;
- \mathbb{Z}_n — кольцо вычетов по модулю n ;
- $M_n(\mathbb{R})$ — кольцо матриц порядка n над \mathbb{R} .

Пример.

Элементарная геометрия плоскости:

$(\mathbb{R}^2; =, \cong, B)$, где

- \mathbb{R}^2 — множество точек евклидовой плоскости;
- $B(a, b, c)$ — трёхместный предикат «точка b лежит на прямой ac между точками a и c »;
- \cong — четырёхместный предикат $ab \cong cd$ «отрезки, задаваемые парами точек ab и cd , имеют равные длины».

Пример.

Модель Пуанкаре геометрии Лобачевского:

$(\mathbf{H}^2; =, \cong, B)$, где

- $\mathbf{H}^2 \Rightarrow \{z \in \mathbb{C} : \text{Im}(z) > 0\}$ — множество точек верхней евклидовой полуплоскости;
- $B(a, b, c)$ — трёхместный предикат «точка b лежит между точками a и c на полуокружности (или полупрямой), проходящей через a , c и ортогональной вещественной оси»;

- \cong — четырёхместный предикат (записываемый $ab \cong cd$)
«*сегменты окружностей, ортогональных вещественной оси, задаваемые парами точек ab и cd , имеют равные длины в смысле метрики Пуанкаре*», то есть

$$ab \cong cd \stackrel{\text{def}}{\iff} \frac{|a - b|}{|a - \bar{b}|} = \frac{|c - d|}{|c - \bar{d}|},$$

где \bar{b} означает комплексно сопряжённое к b .

Пример.

Упорядоченные множества

$(\mathbb{N}; <)$, $(\mathbb{Z}, <)$, $(\mathbb{Q}; <)$, $(\mathbb{R}; <)$.

Пример.

Частично упорядоченные множества

- 1 $(\mathcal{P}(U); \subseteq)$, где U — любое множество;
- 2 $(\mathbb{Z}; |)$, где $a | b$ — бинарное отношение «быть делителем»;
- 3 $(Sub(G); \subseteq)$, где $Sub(G)$ — множество всех подгрупп группы G .

Пример.

Упорядоченные множества

$(\mathbb{N}; <)$, $(\mathbb{Z}, <)$, $(\mathbb{Q}; <)$, $(\mathbb{R}; <)$.

Пример.

Частично упорядоченные множества

- 1 $(\mathcal{P}(U); \subseteq)$, где U — любое множество;
- 2 $(\mathbb{Z}; |)$, где $a | b$ — бинарное отношение «быть делителем»;
- 3 $(Sub(G); \subseteq)$, где $Sub(G)$ — множество всех подгрупп группы G .

Пример.

Упорядоченное поле действительных чисел:

$(\mathbb{R}; =, <, +, -, \times, 0, 1)$

Пример.

Булева алгебра $(B; =, \underline{\Delta}, \underline{\vee}, \underline{\supset}, \underline{\Rightarrow}, 0, 1)$

Подчёркнутые символы означают операции булевой алгебры (а не логические связки), то есть функции на B .

Синтаксис логики первого порядка

Алфавит языка \mathcal{L}_Σ содержит:

Символы сигнатуры: Σ ;

Свободные переменные: $\text{FrVar} = \{a_0, a_1, a_2, \dots\}$,

Связанные переменные: $\text{BdVar} = \{v_0, v_1, v_2, \dots\}$,

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

Кванторы: \forall (квантор общности, «для всех»);

\exists (квантор существования, «существует»);

Знаки пунктуации: $\langle\langle \rangle\rangle, \langle\langle \rangle\rangle$ и $\langle\langle , \rangle\rangle$.

Термы

Опр.

Множество *термов* Tm_{Σ} есть наименьшее множество, замкнутое относительно следующих правил:

- 1 Свободные переменные и константы суть термы.
- 2 Если $f \in Func_{\Sigma}$ валентности n и t_1, \dots, t_n — термы, то выражение $f(t_1, \dots, t_n)$ есть терм.

Пример.

Если $f \in \text{Func}_\Sigma$ — бинарный функциональный символ, то $f(a_0, a_1)$ и $f(f(a_5, a_0), a_1)$ — термы, а $f(v_0, a_1)$ — не терм.

Формулы

Опр.

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.

(Здесь $A[a/x]$ означает результат замены всех вхождений a в A на x .)

Пример.

$P(f(a_0, a_1))$ и $(\forall v_0(\forall v_1 P(f(v_0, v_1))))$ — формулы,
 $(\forall v_0(\forall v_0 P(f(v_0, v_0))))$ — не формула.

Опр.

- Формулы, в которые не входят кванторы, называются *бескванторными*.
- Формулы и термы, в которые не входят свободные переменные, называются *замкнутыми*.
- Замкнутые формулы также называются *предложениями*.

Сокращения

- соглашения об опускании скобок;
- сокращения для логических связок;
- пишут a, b, c вместо a_0, a_1, a_2 и т.д.; x, y, z вместо v_0, v_1, v_2 и т.д.;
- пишут $\forall x_1 \dots x_n A$ вместо $(\forall x_1(\forall x_2(\dots(\forall x_n A) \dots)))$ и аналогично для последовательностей кванторов \exists .
- пишут $a = b$ вместо $= (a, b)$,
- $a + b$ вместо $+ (a, b)$;
- и т.д.

Семантика логики первого порядка

Пусть M — модель сигнатуры Σ . Обозначим через $\Sigma(M)$ сигнатуру, получаемую из Σ добавлением новых символов констант для всех элементов M , то есть $\{c : c \in M\}$.

Значение терма в модели

Опр.

Пусть t — замкнутый терм сигнатуры $\Sigma(M)$.

Значение t в модели M есть элемент $t_M \in M$, определяемый индукцией по построению t .

- 1 Если $a \in M$, то $\underline{a}_M \Rightarrow a$.
- 2 Если $c \in \text{Const}_\Sigma$, то $c_M \in M$ есть данная нам интерпретация c .
- 3 Если t есть $f(t_1, \dots, t_n)$, где $f \in \text{Func}_\Sigma$, то $t_M \Rightarrow f_M((t_1)_M, \dots, (t_n)_M)$.

Истинность формулы в модели

Опр.

Пусть A — замкнутая формула сигнатуры $\Sigma(M)$.

Отношение $M \models A$ «формула A истинна в модели M » определяется индукцией по построению A .

- $M \models P(t_1, \dots, t_n) \stackrel{\text{def}}{\iff} P_M((t_1)_M, \dots, (t_n)_M)$,
если $A = P(t_1, \dots, t_n)$ — 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:

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

Замечание.

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 истинна, так и ложна, в зависимости от значений a и b .

Сокращение: ВМЕСТО

$$M \models A[a_1/\underline{c}_1, \dots, a_n/\underline{c}_n]$$

пишут

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

или даже

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

.

Примеры

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 $(\mathbb{H}^2; =, \cong, B)$.

Определимость в модели

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

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

Пример.

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

Опр.

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 .

Опр.

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

$$a \leq b \wedge \forall x (x \leq b \rightarrow (x \leq a \vee b \leq x)).$$

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

Аксиома о параллельных

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

- $a \neq b \Leftrightarrow \neg a = b$
- $c \in ab$ « c лежит на прямой ab »
 $c \in ab \Leftrightarrow (B(c, a, b) \vee B(a, c, b) \vee B(a, b, c))$
- $ab \parallel cd$ «прямые ab и cd параллельны»
 $ab \parallel cd \Leftrightarrow a \neq b \wedge c \neq d \wedge \neg \exists x (x \in ab \wedge x \in cd)$

Аксиома о параллельных

«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 \mathbf{H}^2 .