Логика предикатов лекция 5

Лев Дмитриевич Беклемишев
http://lpcs.math.msu.su/vml2009

lbekl@yandex.ru

12.03.2008

Предикаты и функции

Пусть M — непустое множество.

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

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

- *n-арная функция на M*: функция $f : M^n \to M$
- *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):

$$\mathrm{Pred}_\Sigma \cup \mathrm{Func}_\Sigma \to \mathbb{N} \setminus \{0\}.$$

Модели

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

- каждому $P \in \mathrm{Pred}_\Sigma$ некоторый предикат P_M на M той же валентности;
- каждому $f \in \mathrm{Func}_\Sigma$ функцию f_M на M той же валентности;
- каждому $c \in \mathrm{Const}_\Sigma$ 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:

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

- $S(x) \rightleftharpoons x + 1$ 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

- $\mathbf{H}^2 \rightleftharpoons \{z \in \mathbb{C} : \mathrm{Im}(z) > 0\}$ — 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

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

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 $a \mid b$ — 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 $a \mid b$ — 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 $(B; =, \underline{\wedge}, \underline{\vee}, \underline{\neg}, \underline{\rightarrow}, 0, 1)$

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

Синтаксис логики первого порядка

Алфавит языка $\mathcal{L}_\Sigma$ содержит:

Символы сигнатуры: Σ;

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

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

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

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

$\exists$ (квантор существования, «существует»);

Знаки пунктуации: «(», «)» и «,».

Термы

Опр.

Множество *термов* Tm_Σ есть наименьшее множество, замкнутое относительно следующих правил:

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

Пример.

Если $f \in \mathrm{Func}_\Sigma$ — 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 $P \in \mathrm{Pred}_\Sigma$ валентности n и $t_1, \ldots, t_n$ — термы, то $P(t_1, \ldots, t_n)$ есть формула (называемая *атомарной формулой*).
- Если A, B — формулы, то формулами являются $(A \to B)$, $\neg A$, $(A \wedge B)$, $(A \vee B)$.

- 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 $\forall x_1 \ldots x_n\, A$ вместо $(\forall x_1 (\forall x_2 (\ldots (\forall x_n A) \ldots)))$ 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 $\{\underline{c} : c \in M\}$.

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

Истинность формулы в модели

Опр.

Пусть A — замкнутая формула сигнатуры $\Sigma(M)$. Отношение $M \vDash A$ «*формула A истинна в модели M*» определяется индукцией по построению A.

- $M \vDash P(t_1, \ldots, t_n) \stackrel{\text{def}}{\Longleftrightarrow} P_M((t_1)_M, \ldots, (t_n)_M)$, если $A = P(t_1, \ldots, t_n)$ — атомарная формула;

Стандартные определения для булевых связок:

- $M \vDash (B \to C) \overset{\text{def}}{\iff} (M \nvDash B \text{ или } M \vDash C)$;
- $M \vDash \neg B \overset{\text{def}}{\iff} M \nvDash B$;
- $M \vDash (A \wedge B) \overset{\text{def}}{\iff} (M \vDash A \text{ и } M \vDash B)$;
- $M \vDash (A \vee B) \overset{\text{def}}{\iff} (M \vDash A \text{ или } M \vDash B)$;

Кванторы:

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

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

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

пишут

$$M \vDash A[a_1/c_1, \ldots a_n/c_n]$$

или даже

$$M \vDash A[c_1, \ldots c_n]$$

.

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

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

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

Определимость в модели

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

$$A_M(x_1, \ldots, x_n) \overset{\text{def}}{\Longleftrightarrow} M \models A[b_1/x_1, \ldots, b_n/x_n].$$

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 $\mathcal{L}_\Sigma$.

Опр.

Функция f называется *определимой в модели* M, если определим её график, то есть предикат

$$G_f(x_1, \dots, x_n, y) \overset{\text{def}}{\Longleftrightarrow} f(x_1, \dots, x_n) = y.$$

Пример.

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

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

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

Аксиома о параллельных

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

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

Аксиома о параллельных

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

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

Верно в $\mathbb{R}^2$, но не в $\mathbf{H}^2$.