Введение в математическую логику

Мех-мат МГУ, 1-й курс, весна 2008 г.

Конспект лекций 5 и 6

Л.Д. Беклемишев*

3 Логика предикатов первого порядка

3.1 Модели.

Алгебраические системы или модели являются естественной семантикой логики первого порядка.

Пусть M — непустое множество. *n-арным предикатом на M* называется произвольное подмножество $Q \subseteq M^n = M \times M \times \cdots \times M$ (n раз). *n-арной функцией на M* называется функция $f : M^n \to M$. Если Q — n-арный предикат, то часто пишут $Q(x_1, \ldots, x_n)$ вместо $\langle x_1, \ldots, x_n \rangle \in Q$; аналогично, $f(x_1, \ldots, x_n)$ означает $f(\langle x_1, \ldots, x_n \rangle)$. *Константами* называем произвольные элементы множества M.

Сигнатурой называется некоторая совокупность имён функций, предикатов и констант. Сигнатура Σ задаётся тремя непересекающимися алфавитами Pred_Σ, Func_Σ и Const_Σ *предикатных*, *функциональных символов* и *символов констант*, соответственно, и функцией *валентности*

$$\mathrm{arity} : \mathrm{Pred}_\Sigma \cup \mathrm{Func}_\Sigma \to \mathbb{N} \setminus \{0\},$$

сопоставляющей каждому предикатному и функциональному символу число его аргументов.

Алгебраическая система (или *модель*) *сигнатуры* Σ есть непустое множество M вместе с отображением, сопоставляющим каждому предикатному символу P из Σ некоторый предикат P_M на M той же валентности, каждому функциональному символу f функцию f_M на M

*Данный конспект лекций составлен с использованием лекционных материалов ряда сотрудников кафедры математической логики и теории алгоритмов МГУ, в частности конспекта лекций профессора М.Р. Пентуса (2006 г.), на основе программы, разработанной коллективом кафедры.

той же валентности, и каждой символу $c \in \mathrm{Const}_\Sigma$ константу $c_M \in M$. Такое отображение называется *интерпретацией* Σ *на* M. Множество M называется *универсумом* или *носителем* данной интерпретации (модели). Модель сигнатуры Σ с носителем M обозначается $(M; \Sigma)$.

Замечание 3.1. В математике используются многочисленные стандартные имена для предикатов и функций. Например, на множестве целых чисел «+» означает обычную функцию сложения, «=» означает предикат равенства, «0» константу 0. Так, $(\mathbb{Z}; =, +, 0)$ означает модель с универсумом $\mathbb{Z}$ и заданными на нём бинарным отношением $=$, бинарной функцией $+$ и константой 0. Мы также используем другие стандартные соглашния об обозначениях, например, пишем $a_1 = a_2$ вместо формального $=(a_1, a_2)$ и $a_1 + a_2$ вместо $+(a_1, a_2)$.

3.2 Примеры

Пример 3.2. [Стандартная модель арифметики] $(\mathbb{N}; =, S, +, \times, 0)$

Здесь $S(x) \rightleftharpoons x + 1$ есть одноместная функция следования на множестве $\mathbb{N}$, а все остальные функции и предикаты имеют стандартный смысл.

Пример 3.3. [Кольцо целых чисел] $(\mathbb{Z}; =, +, -, \times, 0, 1)$

Здесь «$-$» есть одноместная функция, отображающая x на $-x$.

Пример 3.4. Любое другое кольцо (с единицей) 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 3.5. [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 (записываемый $ab \cong cd$) «*отрезки, задаваемые парами точек* ab *и* cd*, имеют равные длины*».

Пример 3.6. [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 $ab \cong cd$) «*отрезки, 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 3.7. [Упорядоченные множества] $(\mathbb{N}; <)$, $(\mathbb{Z}, <)$, $(\mathbb{Q}; <)$, $(\mathbb{R}; <)$.

Пример 3.8. [Частично упорядоченные множества]

(i) $(\mathcal{P}(U); \subseteq)$, где U — любое множество;

(ii) $(\mathbb{Z}; |)$, где $a \mid b$ — бинарное отношение «быть делителем»;

(iii) $(Sub(G); \subseteq)$, где $Sub(G)$ — множество всех подгрупп группы G.

Пример 3.9. [Упорядоченные поля рациональных и действительных чисел]

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

Естественно было бы обогатить сигнатуру поля операцией взятия обратного элемента (или операцией деления), но эта операция не определена в нуле. Однако, эту операцию можно выразить из уже имеющихся средствами логики первого порядка (см. ниже), поэтому включать её в сигнатуру нет необходимости.

Пример 3.10. [Булева алгебра] $(B; =, \underline{\wedge}, \underline{\vee}, \underline{\supset}, \underline{\rightarrow}, 0, 1)$

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

3.3 Синтаксис логики первого порядка

Язык логики первого порядка $\mathcal{L}_\Sigma$ определяется его сигнатурой Σ. Помимо всех символов сигнатуры, в алфавит языка $\mathcal{L}_\Sigma$ входят два фиксированных счётных алфавита *свободных* и *связанных переменных*

$$\begin{aligned} \mathrm{FrVar} &= \{a_0, a_1, a_2, \dots\}, \\ \mathrm{BdVar} &= \{v_0, v_1, v_2, \dots\}, \end{aligned}$$

и следующие специальные символы:

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

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

Знаки пунктуации: «(», «)» (скобки) и «,» (запятая).

Произвольное слово в описанном алфавите называем *выражением*. Некоторые выражения называются *термами* и *формулами*. Множества термов и формул языка $\mathcal{L}_\Sigma$ определяются индуктивно.

Определение 3.11. Множество термов Tm_Σ есть наименьшее множество, замкнутое относительно следующих правил:

1. Свободные переменные и константы суть термы.
2. Если f — функциональный символ валентности n и $t_1, \dots, t_n$ — термы, то выражение $f(t_1, \dots, t_n)$ есть терм.

Пример 3.12. Если $f \in \mathrm{Func}_\Sigma$ — бинарный функциональный символ, то $f(a_0, a_1)$ — терм, а $f(v_0, a_1)$ — не терм.

Определение 3.13. Множество формул Fm_Σ есть наименьшее множество, замкнутое относительно следующих правил:

1. Если P — предикатный символ валентности n и $t_1, \dots, t_n$ — термы, то $P(t_1, \dots, t_n)$ есть формула (называемая *атомарной формулой*).
2. Если A, B — формулы, то формулами являются также выражения $(A \to B)$, $\neg A$, $(A \wedge B)$, $(A \vee B)$.
3. 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 3.14. $f(a_0, a_1) = f(a_0, a_1)$ и $(\forall v_0(\forall v_1 f(v_0, v_1) = f(v_0, v_1)))$ — формулы (с учётом соглашения о написании предиката $=$), а $g(a_0) = g(v_1)$ — не формула.

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

Так же как и в логике высказываний, в логике предикатов действуют стандартные соглашения об опускании скобок, сокращения для логических связок, и другие сокращения. В частности,

- пишут буквы 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 существования.

3.4 Семантика логики первого порядка

Пусть M — модель сигнатуры Σ. Обозначим через $\Sigma(M)$ сигнатуру, получаемую из Σ добавлением новых символов констант $\{\underline{c} : c \in M\}$. Для каждого элемента $c \in M$ добавляется ровно одна константа $\underline{c}$, и все эти символы отличны друг от друга и от символов сигнатуры Σ.

Определение 3.15. Пусть t — замкнутый терм языка $\mathcal{L}_{\Sigma(M)}$. *Значение терма t в модели M* есть элемент $t_M \in M$, определяемый индукцией по построению t.

(i) Если $a \in M$, то $\underline{a}_M \rightleftharpoons a$.

(ii) Если $c \in \mathrm{Const}_\Sigma$, то $c_M \in M$ есть данная нам интерпретация c.

(iii) Если t есть $f(t_1, \dots, t_n)$, где $f \in \mathrm{Func}_\Sigma$, то $t_M \rightleftharpoons f_M((t_1)_M, \dots, (t_n)_M)$.

Определение 3.16. Пусть A — замкнутая формула языка $\mathcal{L}_{\Sigma(M)}$. *Истинностное значение формулы A в модели M* определяется индукцией по построению A (отношение $M \vDash A$ читается «формула A истинна в модели M»).

1. $M \vDash P(t_1, \dots, t_n) \overset{\text{def}}{\iff} P_M((t_1)_M, \dots, (t_n)_M)$, если $A = P(t_1, \dots, t_n)$ — атомарная формула;

2. $M \vDash (B \to C) \overset{\text{def}}{\iff} (M \nvDash B \text{ или } M \vDash C)$;

3. $M \vDash \neg B \overset{\text{def}}{\iff} M \nvDash B$;

4. $M \vDash (A \wedge B) \overset{\text{def}}{\iff} (M \vDash A \text{ и } M \vDash B)$;

5. $M \vDash (A \vee B) \overset{\text{def}}{\iff} (M \vDash A \text{ или } M \vDash B)$;

6. $M \vDash (\forall x A[a/x]) \overset{\text{def}}{\iff}$ для всех $x \in M$ $M \vDash A[a/\underline{x}]$;

7. $M \vDash (\exists x A[a/x]) \overset{\text{def}}{\iff}$ существует $x \in M$ $M \vDash A[a/\underline{x}]$.

Если список $b_1, \ldots, b_n$ содержит все свободные переменные формулы A, а $x_1, \ldots, x_n \in M$, то $M \vDash A[b_1/\underline{x}_1, \ldots, b_n/\underline{x}_n]$ сокращённо записываем как $M \vDash A[b_1/x_1, \ldots, b_n/x_n]$ или даже $M \vDash A[x_1, \ldots, x_n]$.

Замечание 3.17. Нельзя говорить об истинности или ложности незамкнутых формул, поскольку их истинностные значения зависят от выбора значений параметров — входящих в формулу свободных переменных.

Пример 3.18. Формула $a + 1 = b$ в стандартной модели арифметики может быть как истинна, так и ложна, в зависимости от значений a и b.

Пример 3.19. 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 3.20. 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 $(\mathbf{H^2}; =, \cong, B)$.

3.5 Определимые предикаты и функции

Пусть $b_1, \ldots, b_n$ — упорядоченный набор свободных переменных. Запись $A(b_1, \ldots, b_n)$ означает, что все свободные переменные формулы A входят в набор $b_1, \ldots, b_n$.

Для фиксированного набора переменных любая формула $A(b_1, \ldots, b_n)$ определяет n-местный предикат A_M в модели M:

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

Определение 3.21. Предикат $P(x_1, \ldots, x_n)$ называется *определимым (или выразимым) в модели* $(M; \Sigma)$, если $P = A_M$ для некоторой формулы $A(a_1, \ldots, a_n)$ в языке $\mathcal{L}_\Sigma$.

Определение 3.22. Функция f называется *определимой в модели* M, если определим её график, то есть предикат

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

Пример 3.23. *В модели* $(\mathbb{Z}; \leq)$ *предикат* $a_2 = a_1 + 1$ *определим формулой*

$$a_1 \leq a_2 \wedge \forall v_0 \, (v_0 \leq a_2 \to (v_0 \leq a_1 \vee a_2 \leq v_0)).$$

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

Пример 3.24. (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.»*

может быть выражена следующим образом:

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

Это утверждение верно в $\mathbb{R}^2$, но не в $\mathbf{H}^2$.

Пример 3.25. В модели $(\mathbb{R}; =, +, \cdot, 0, 1)$ выразимы порядок и деление.

- $a \leq b \rightleftharpoons \exists x\ (b = a + (x \cdot x))$
- Предикат «$a/b = c$» выразим формулой

$$D(a, b, c) \rightleftharpoons (b \neq 0 \wedge c \cdot b = a).$$

3.6 Изоморфизм моделей.

Пусть M и M' — модели сигнатуры Σ.

Определение 3.26. *Гомоморфизм* $\varphi : M \to M'$ есть отображение из M в M', сохраняющее все предикаты, функции и константы Σ. То есть, $\varphi : M \to M'$ — гомоморфизм, если для всех $P \in \mathrm{Pred}_\Sigma$, $f \in \mathrm{Func}_\Sigma$ и $c \in \mathrm{Const}_\Sigma$ валентности n, для всех $x_1, \ldots, x_n \in M$

$$\begin{array}{rcl} P_M(x_1, \ldots, x_n) & \Rightarrow & P_{M'}(\varphi(x_1), \ldots, \varphi(x_n)) \\ \varphi(f_M(x_1, \ldots, x_n)) & = & f_{M'}(\varphi(x_1), \ldots, \varphi(x_n)) \\ \varphi(c_M) & = & c_{M'} \end{array}$$

Предложение 3.27. *Композиция гомоморфизмов — гомоморфизм.*

Определение 3.28. *Изоморфизм* $\varphi : M \to M'$ есть гомоморфизм, у которого есть обратный, то есть гомоморфизм $\psi : M' \to M$ такой, что

$$\varphi \circ \psi = id_{M'}, \qquad \psi \circ \varphi = id_M,$$

где $id_M : M \to M$ — тождественный гомоморфизм $id_M(x) = x$.

Определение 3.29. M и M' изоморфны, если существует изоморфизм $\varphi : M \to M'$.

Теорема 3.30. *Если* $\varphi : M \to M'$ *— изоморфизм, то для любой формулы* $A(a_1, \ldots, a_n)$ *и любых* $c_1, \ldots, c_n \in M$

$$M \vDash A[c_1, \ldots, c_n] \iff M' \vDash A[\varphi(c_1), \ldots, \varphi(c_n)].$$

Доказательство. Индукция по построению A. $\boxtimes$

Следствие 3.31. *В изоморфных моделях истинны одни и те же предложения.*

3.7 Доказательство невыразимости с помощью автоморфизмов.

Определение 3.32. *Автоморфизмом* $\varphi : M \to M$ называется изоморфизм модели на себя.

Поскольку все определимые предикаты и функции сохраняются при автоморфизмах модели, для доказательства невыразимости достаточно построить автоморфизм, не сохраняющий ту или иную функцию или предикат.

Пример 3.33. В модели $(\mathbb{Z}; =, +)$ не выразим предикат $\leq$.

Доказательство. Отображение $\varphi : x \mapsto -x$ есть автоморфизм $(\mathbb{Z}; =, +)$, не сохраняюжщий $\leq$, поскольку $\mathbb{Z} \vDash 0 \leq 1$, но $\mathbb{Z} \nvDash \varphi(0) \leq \varphi(1)$. $\boxtimes$

Пример 3.34. В модели $(\mathbb{Z}; \leq)$ не выразима функция $+$.

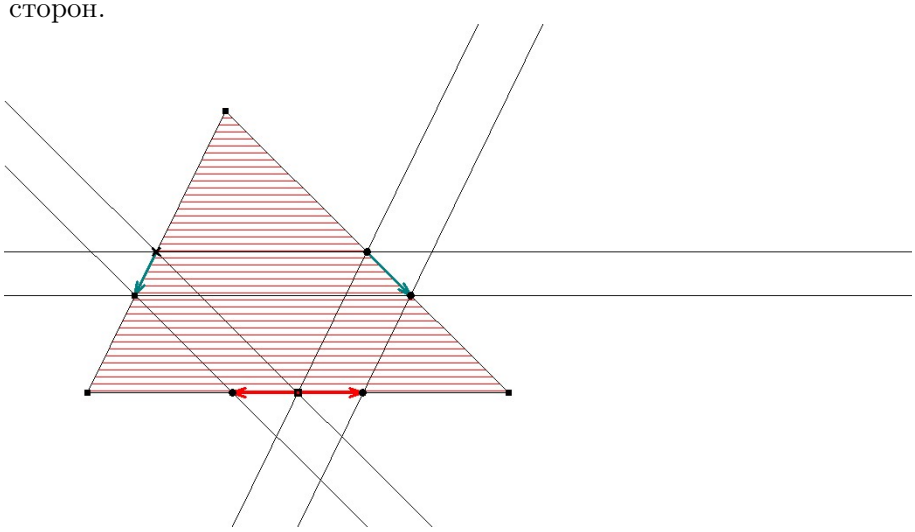
Доказательство. Отображение $\varphi : x \mapsto x + 1$ есть автоморфизм $(\mathbb{Z}; \leq)$, не сохраняющий $+$. $\boxtimes$

Пример 3.35. Автоморфизмами модели $(\mathbb{R}^2; =, B)$ являются все взаимно однозначные аффинные преобразования плоскости и только они.

Этот факт вытекает из следующих соображений.

- Всякий автоморфизм переводит отрезки в отрезки.
- Всякий автоморфизм сохраняет параллельность прямых, поскольку предикат параллельности $ab \| cd$ выразим в этой модели.
- Для любого автоморфизма φ существует аффинное преобразование h такое, что $h \circ \varphi$ сохраняет три различные точки. Действительно, выберем произвольно точки a, b, c, не лежащие на одной прямой. Их образы при автоморфизме φ также не лежат на одной прямой. Каждое аффинное преобразование определяется однозначно образами трёх вершин треугольника. Выберем h таким образом, чтобы $\varphi(a) \mapsto a$, $\varphi(b) \mapsto b$, $\varphi(c) \mapsto c$.
- Если автоморфизм φ имеет три различные неподвижные точки, то $\varphi = id$.

Докажем последнее утверждение. Следующий рисунок показывает, что если φ сохраняет вершины треугольника, то сохраняются и середины его сторон.



Повторяя эту конструкцию для каждого из треугольников, образованных разбиением сторон данного, получаем, что на каждой из сторон треугольника есть всюду плотное множество неподвижных точек φ. Отсюда следует, что все точки сторон треугольника должны быть неподвижны: если $x \neq \varphi(x)$, рассмотрим неподвижную точку, лежащую между x и $\varphi(x)$, и легко придём к противоречию. Но если неподвижны все точки сторон треугольника, то неподвижными должны быть и все его внутренние точки и даже все точки большего треугольника, образованного прямыми, проходящими через вершины данного треугольника и параллельными его противоположным сторонам (каждая точка большего треугольника определется своими проекциями на пару сторон данного треугольника). Итерируя эту конструкцию мы замостим всю плоскость треугольниками, точки которых неподвижны.

Следствие 3.36. *В модели* $(\mathbb{R}^2; =, B)$ *не определимы:*

- *никакая конкретная точка;*
- *никакая конкретная фигура (множество точек), за исключением всей плоскости;*
- *предикат* $\cong$*;*
- *равенство углов, то есть шестиместный предикат* $\angle abc \cong \angle a_1 b_1 c_1$.

Пример 3.37. Автоморфизмы модели $(\mathbb{R}^2; =, B, \cong)$ суть все преобразования плоскости, являющиеся композицией гомотетии и движения.

Для доказательства этого факта отметим, что

- Предикаты B и $\cong$ сохраняются при движениях и гомотетиях.
- Аффинное преобразование, сохраняющее длины сторон некоторого треугольника, есть движение.
- Любой автоморфизм φ переводит равносторонний треугольник в (подобный ему) равносторонний.
- Для некоторой гомотетии h автоморфизм $h \circ \varphi$ сохраняет длины сторон заданного равностороннего треугольника.

Значит, $h \circ \varphi$ — движение.

Следствие 3.38. *B модели $(\mathbb{R}^2; =, B, \cong)$ не определимы:*

- *никакая конкретная фигура, за исключением всей плоскости;*
- *единица длины, то есть предикат «длина отрезка ab равна 1»;*
- *ориентация, то есть предикат «вершины треугольника abc обходятся против часовой стрелки»;*
- *направление «вдоль оси x».*

3.8 Выполнимость, общезначимость, логическое следование.

Определение 3.39. Формула $A(b_1, \ldots, b_n)$ сигнатуры Σ *выполнима в модели* (M, Σ), если для некоторых констант $c_1, \ldots, c_n \in M$ предложение $A[b_1/\underline{c}_1, \ldots, b_n/\underline{c}_n]$ сигнатуры $\Sigma(M)$ истинно. Формула A сигнатуры Σ *выполнима*, если она выполнима в некоторой модели $(M; \Sigma)$.

Определение 3.40. Множество формул Γ сигнатуры Σ *выполнимо в модели* M, если существует функция $f : \mathrm{FrVar} \to M$ такая, что при подстановке вместо каждой переменной a_i константы $\underline{f(a_i)}$ сигнатуры $\Sigma(M)$ все формулы Γ истинны в M. Такую функцию f будем называть *выполняющей оценкой* для Γ.

Множество формул Γ *выполнимо*, если Γ выполнимо в некоторой модели.

Определение 3.41. Формула A *общезначима* (*тождественно истинна*), если $\neg A$ не выполнима.

Определение 3.42. Формула A *тождественно ложна*, если A не выполнима.

Пример 3.43. Формулы $P(a) \vee \neg P(a)$, $\exists x \forall y A(x,y) \to \forall y \exists x\, A(x,y)$ общезначимы. Формула $P(a_0) \to P(a_1)$ выполнима, но не общезначима.

Определение 3.44. Пусть Γ — некоторое множество формул сигнатуры Σ и A — формула той же сигнатуры. Говорят, что A *логически следует* (или *семантически следует*) из множества Γ (обозначение $\Gamma \models A$), если для любой модели M сигнатуры Σ формула A истинна в M при любой выполняющей оценке для множества Γ.

Пример 3.45. $\{P(a) \to Q(b), P(a)\} \models P(a) \wedge \exists x Q(x)$.

Пример 3.46. $P(a) \not\models \forall x P(x)$.

Соотношения между понятиями выполнимости, общезначимости и логическим следованием в логике предикатов такие же, как и в логике высказваний.

Предложение 3.47. (i) A — *общезначима* $\iff \varnothing \models A$.

(ii) Γ *выполнимо* $\iff \Gamma \not\models \bot$.

(iii) $\Gamma \models A \iff \Gamma \cup \{\neg A\}$ *не выполнимо.*

Предложение 3.48. $\{B_1, \ldots, B_n\} \models A \iff (\bigwedge_{i=1}^{n} B_i) \to A$ *общезначима.*

3.9 Эквивалентность формул.

Определение 3.49. Формулы A и B сигнатуры Σ равносильны (обозначение $A \equiv B$), если для любой модели $(M;\Sigma)$ и оценки f на M

$$M \models f(A) \iff M \models f(B).$$

Пусть список $b_1, \ldots, b_n$ содержит все свободные переменные A, B.

Утверждение 3.50. *$A \equiv B$, если и только если в любой модели M формулы A и B определяют один и тот же предикат, то есть если $A_M = B_M$ (для данного набора переменых).*

Утверждение 3.51. (i) *Отношение $\equiv$ рефлексивно, симметрично и транзитивно.*

(ii) *$A \equiv B$, если и только если формула $A \leftrightarrow B$ общезначима.*

(iii) *Формула A общезначима тогда и только тогда, когда $A \equiv \top$.*

Перечислим основные равносильности с кванторами.

Лемма 3.52 (замена связанной переменной). *Если $x, y \in BdVar$ не входят в формулу A, то $\forall x\, A[a/x] \equiv \forall y\, A[a/y]$ и $\exists x\, A[a/x] \equiv \exists y\, A[a/y]$.*

Доказательство.

$$\begin{array}{rcl} M \vDash \forall x\, A[a/x] & \iff & M \vDash A[a/c] \quad \text{для всех } c \in M \\ & \iff & M \vDash \forall y\, A[a/y]. \end{array}$$

Для квантора существования рассуждение аналогично. $\boxtimes$

Лемма 3.53. *Если $x \in BdVar$ не входит в формулы A, B, то*

$$(\forall x\, A[a/x] \vee B) \equiv \forall x\, (A[a/x] \vee B).$$

Доказательство. Прежде всего заметим, что правая часть эквивалентности, так же как и левая часть, является формулой. В самом деле, выберем $a' \in \mathrm{FrVar}$, не входящую в A, B. Тогда $B[a'/x] = B$, $A[a/x] = A[a/a'][a'/x]$ и тем самым $\forall x(A[a/x] \vee B)$ совпадает с $\forall x(A[a/a'] \vee B)[a'/x]$. Получаем

$$\begin{array}{rcl} M \vDash \forall x\, (A[a/x] \vee B) & \iff & M \vDash (A[a/c] \vee B) \quad \text{для всех } c \in M \\ & \iff & (M \vDash B \text{ или для всех } c \in M\ M \vDash A[a/c]) \\ & \iff & (M \vDash B \text{ или } M \vDash \forall x\, A[a/x]) \\ & \iff & M \vDash (\forall x\, A[a/x] \vee B). \end{array}$$

$\boxtimes$

Аналогично обосновываются остальные равносильности, входящие в следующую таблицу (где предполагается, что переменные x, y не входят в формулы A и B).

$\forall x\, A[a/x]$	$\equiv$	$\forall y\, A[a/y]$	$\exists x\, A[a/x]$	$\equiv$	$\exists y\, A[a/y]$
$(\forall x\, A[a/x] \vee B)$	$\equiv$	$\forall x\, (A[a/x] \vee B)$	$(\exists x\, A[a/x] \vee B)$	$\equiv$	$\exists x\, (A[a/x] \vee B)$
$(\forall x\, A[a/x] \wedge B)$	$\equiv$	$\forall x\, (A[a/x] \wedge B)$	$(\exists x\, A[a/x] \wedge B)$	$\equiv$	$\exists x\, (A[a/x] \wedge B)$
$\neg\forall x A[a/x]$	$\equiv$	$\exists x \neg A[a/x]$	$\neg\exists x A[a/x]$	$\equiv$	$\forall x \neg A[a/x]$

3.10 Правила подстановки и замены подформулы на эквивалентную.

Определение 3.54. Обогатим язык логики первого порядка пропозициональной переменной P. Можно считать P нульместным предикатным символом. Распространим на расширенный язык все синтаксические понятия, включая понятие формулы (P считается атомарной формулой). Запись $C[P/A]$ означает результат замены всех вхождений P в формулу C на A.

Заметим, что $C[P/A]$ не всегда является формулой. Для этого достаточно, чтобы связанные переменные A не входили в C. Необходимое и достаточное условие формулируется следующим образом.

Лемма 3.55. *$C[P/A]$ — формула, если и только если любое вхождение P в формулу C не находится в области действия квантора по переменной $x \in BdVar$, входящей в A.*

Доказательство. Необходимость этого условия очевидна. Достаточность доказывается простой индукцией по построению формулы C. $\boxtimes$

Определение 3.56. Говорим, что *разрешена подстановка формулы A вместо P в C*, если выполнено условие предыдущей леммы.

Лемма 3.57. (i) *Если $A \equiv B$, то $\neg A \equiv \neg B$. Если $A_1 \equiv B_1$ и $A_2 \equiv B_2$, то $A_1 \wedge A_2 \equiv B_1 \wedge B_2$, $A_1 \vee A_2 \equiv B_1 \vee B_2$, $A_1 \to A_2 \equiv B_1 \to B_2$.*

(ii) *Если $A \equiv B$ и $x \in BdVar$ не входит в A, B, то $\forall x A[a/x] \equiv \forall x B[a/x]$ и $\exists x A[a/x] \equiv \exists x B[a/x]$.*

Теорема 3.58 (замена подформулы на эквивалентную). *Если $A \equiv B$ и разрешена подстановка формул A, B вместо P в C, то $C[P/A] \equiv C[P/B]$.*

Доказательство. Теорема доказывается индукцией по построению формулы C на основе очевидной леммы 3.57. Рассмотрим лишь один наиболее интересный случай.

Допустим C имеет вид $\forall x D[a/x]$. Поскольку $C = \forall x D[a/a'][a'/x]$, переходя в случае необходимости к формуле $D[a/a']$ мы можем считать, что переменная a не входит в A, B. По предположению индукции

$D[P/A] \equiv D[P/B]$. Так как подстановка формул A, B в C разрешена, переменная x не входит в A, B. Отсюда по лемме 3.57 (ii) получаем

$$\forall x D[P/A][a/x] \equiv \forall x D[P/B][a/x].$$

Поскольку a не входит в A, B мы имеем $D[P/A][a/x] = D[a/x][P/A]$, откуда

$$(\forall x D[a/x])[P/A] = (\forall x D[P/A][a/x]) \equiv (\forall x D[P/B][a/x]) = (\forall x D[a/x])[P/B].$$

$\boxtimes$

Комбинируя эту теорему вместе с леммой 3.52 мы получаем следующее утверждение о переименовании связанных переменных в формуле.

Лемма 3.59. *Пусть $y \in BdVar$ не входит в формулу B. Тогда $B[x/y]$ есть формула и $B[x/y] \equiv B$.*

Доказательство. Применяем индукцию по числу вхождений кванторов $\forall x$ в B. Если таких вхождений нет, то утверждение очевидно. Иначе $B = B'[P/C]$, где $C = \forall x A[a/x]$ для некоторых формул B' и A. По предположению индукции $B' \equiv B'' \rightleftharpoons B'[x/y]$. По лемме 3.52 $C \equiv C' \rightleftharpoons \forall y A[a/y]$, поэтому

$$B'[P/C] \equiv B''[P/C] \equiv B''[P/C'].$$

Но формула $B''[P/C']$ совпадает с $B[x/y]$. $\boxtimes$

Понятие модели также распространяется на формулы языка, расширенного пропозициональной переменной P. При этом P в модели M интерпретируется как логическая константа, то есть $P_M \in \mathbb{B}$. Считается $M \vDash P_M$, если $P_M = \text{И}$ и $M \nvDash P_M$, если $P_M = \text{Л}$. При этих соглашениях понятие общезначимой формулы и равносильности формул распространяется на расширенный язык.

Теорема 3.60 (о подстановке). *Пусть формула A общезначима и разрешена подстановка формулы C вместо P в A, тогда общезначима формула $A[P/C]$.*

Доказательство. Рассуждаем от противного. Допустим, $M \nvDash A[P/C]$ при некоторой подстановке элементов M вместо свободных переменных

этой формулы. Поскольку формула C не содержит других свободных переменных, при данной подстановке она истинна или ложна. Положим

$$P_M = \text{И} \iff M \vDash C.$$

Тем самым мы доопределили модель M до модели языка с пропозициональной переменной P. Индукцией по построению формулы B этого языка легко проверяется, что

$$M \vDash B[P/C] \iff M \vDash B$$

для любой формулы B, в которую разрешена подстановка C вместо P. Отсюда получаем $M \nvDash A$. $\boxtimes$

3.11 Предварённые формулы

Определение 3.61. Формула A называется *предварённой*, если A имеет вид $\mathsf{Q}x_1\mathsf{Q}x_2 \ldots \mathsf{Q}x_n A_0[b_1/x_1, \ldots, b_n/x_n]$, где Q означает квантор $\forall$ или $\exists$, а формула A_0 бескванторная.

Теорема 3.62 (о предварённой форме). *Для каждой формулы A можно указать эквивалентную ей предварённую формулу A' от тех же свободных переменных.*

Такую формулу A' называем *предварённой формой* формулы A.

Доказательство. Применяя основные эквивалентности с кванторами постепенно выносим все кванторы наружу. Более формально, доказываем теорему индукцией по построению A.

Удобно ввести следующее обозначение. Пусть α, β означают произвольные последовательности кванторов вида $\mathsf{Q}x_1\mathsf{Q}x_2 \ldots \mathsf{Q}x_n$, а αA означает результат применения последовательности кванторов α к формуле A.

Лемма 3.63. *Для любых α, β и любых формул A, B, не содержащих переменных из α, β, имеем:*

(i) $\alpha A \wedge B \equiv \alpha(A \wedge B)$; $\alpha A \vee B \equiv \alpha(A \vee B)$;

(ii) $\neg\, \alpha A \equiv \bar{\alpha} \neg A$, *где $\bar{\alpha}$ получается из α заменой всех символов $\exists$ на $\forall$ и наоборот.*

Доказательство. Утверждение (i) доказывается индукцией по длине α. Шаг индукции есть вторая и третья строка таблицы основных эквивалентностей. Утверждение (ii) получается по индукции из последней строки таблицы эквивалентностей. $\boxtimes$

Доказательство теоремы. Можем считать, что формула A не содержит связки импликации.

Если A атомарна, то можно взять $A' = A$.

Если $A = \forall x B[a/x]$, пусть B' — предварённая форма B. Переходя к эквивалентной формуле $B'' = B'[x/x']$, где x' — новая переменная, добиваемся того, что x не входит в B''. Тогда $A' \rightleftharpoons \forall x B''[a/x]$ — требуемая формула.

Если $A = \neg B$ и B' — предварённая форма B, то применяем утверждение (ii) предыдущей леммы.

Если $A = (B \vee C)$, по теореме о замене подформулы на эквивалентную получаем $A \equiv (B' \vee C')$, где $B' = \alpha B_0$ и $C' = \beta C_0$ — предварённые формы B и C, соответственно (формулы B_0 и C_0 бесквантворные). Произведя замену связанных переменных, входящих в C', на новые, можно считать, что последовательности α и β содержат не пересекающиеся множества переменных. Тогда дважды применимо утверждение (i) предыдущей леммы и мы получаем

$$A \equiv \alpha B_0 \vee \beta C_0 \equiv \alpha(B_0 \vee \beta C_0) \equiv \alpha\beta(B_0 \vee C_0),$$

что и требовалось доказать.

Случай конъюнкции рассматривается аналогично. $\boxtimes$