Введение в математическую логику
(осень 2018)

В.Б. Шехтман

Лекция 12

Корректность исчисления предикатов (окончание)

Для завершения доказательства теоремы корректности 11.10 осталось проверить общезначимость аксиом II.1 и II.2. Рассмотрим II.1 (II.2 проверяется аналогично — упражнение).

Рассуждаем как в случае II.3 (лекция 11). Нам надо доказать общезначимость формулы

$$A(a, \overrightarrow{b}) := \forall x [x/a] B \to [t/a] B,$$

где $\overrightarrow{b}$ — список дополнительных параметров (кроме a).[1] Тогда запишем B как $B(a, \overrightarrow{b})$, t — как $t(a, \overrightarrow{b})$.

Рассмотрим модель M и заменим набор параметров $a, \overrightarrow{b}$ на набор произвольных элементов $q, \overrightarrow{m}$ из M. Получим оцененную формулу

$$A(q, \overrightarrow{m}) = \forall x [x/a] B(a, \overrightarrow{m}) \to [t(q, \overrightarrow{m})/a] B(a, \overrightarrow{m}).$$

Обозначим

$$B_1(a) := B(a, \overrightarrow{m}),\ t_1 := t(q, \overrightarrow{m})$$

и перепишем формулу $A(q, \overrightarrow{m})$:

$$A(q, \overrightarrow{m}) = \forall x [x/a] B_1(a) \to B_1(t_1).$$

Здесь $B_1(t_1)$ обозначает $[t_1/a] B_1(a)$.

Нам надо доказать, что $M \vDash A(q, \overrightarrow{m})$. Для этого предположим

$$M \vDash \forall x [x/a] B_1(a)$$

[1] Переменная a в формулу A может попасть из терма t. Если она не входит в t (и в A), рассуждение не меняется.

и докажем

$$M \vDash B_1(t_1).$$

Достаточно будет установить следующий факт:

Лемма 12.1. *Пусть* $B_1(a) \in Fm_{\Omega\cup M}$, $r(a) \in Tm_{\Omega\cup M}$, $t_1 \in CTm_{\Omega\cup M}$. *Тогда*

(1) $|r(t_1)|_M = |r(|t_1|_M)|_M$,

(2) $|B_1(t_1)|_M = |B_1(|t_1|_M)|_M$.

(Здесь $r(t_1)$ обозначает $[t_1/a]r(a)$.)

Из утверждения (2) получаем $M \vDash B_1(t_1)$ (в предположении $M \vDash \forall x[x/a]B_1(a)$), поскольку из $M \vDash \forall x[x/a]B_1(a)$ следует $M \vDash B_1(|t_1|_M)$.

Доказательство (леммы). Индекс M при $|\dots|$ не пишем. С некоторыми изменениями повторяется доказательство теоремы 7.4.

(1) Индукция по длине r.

(1.1) (базис индукции). $r = c$, для $c \in Const_\Omega$. Тогда a не входит в r, и доказывать нечего.

(1.2) (базис индукции). $r = m$, для $m \in \underline{M}$. Опять a не входит в r, и все очевидно.

(1.3) (базис индукции). $r = a$. Тогда

$$r(t_1) = t_1,\ r(|t_1|) = |t_1|,$$

и также

$$|t_1| = ||t_1||,$$

по определению значения оцененного терма (лекция 7, опр. 4): $|m| = m$ для всех $m \in M$.

(1.3) (шаг индукции). $r(a) = f(r_1(a), \dots, r_n(a))$. Тогда

$$r(t_1) = f(r_1(t_1), \dots, r_n(t_n)),\ r(|t_1|) = f(r_1(|t_1|), \dots, r_n(|t_n|)),$$

и

$$(*)\quad |r(t_1)| = f_M(|r_1(t_1)|, \dots, |r_n(t_1)|),\ |r(|t_1|)| = f_M(|r_1(|t_1|)|, \dots, |r_n(|t_n|)|).$$

Но по предположению индукции для термов r_i

$$|r_i(t_1)| = |r_i(|t_1|)|.$$

Поэтому из $(*)$ имеем:

$$|r(t_1)| = |r(|t_1|)|.$$

(2) Индукция по числу связок и кванторов в $B_1(a)$.

(2.1) (базис индукции) $B_1(a) = P(r_1(a), \ldots, r_n(a))$ — атомарная. Доказательство аналогично (1.3) — упражнение.

(2.2) (шаг индукции) B_1 получается применением $\wedge, \vee, \to$ или $\neg$. Эти случаи почти очевидны — упражнение.

(2.3) (шаг индукции) $B_1(a) = \exists x[x/b]C(a,b)$.

Тогда

$(**)$

$$|B_1(t_1)| = |\exists x[x/b]C(t_1,b)| = \max_{l\in M} |C(t_1,l)|, \ |B_1(|t_1|)| = |\exists x[x/b]C(|t_1|,b)| = \max_{l\in M} |C(|t_1|,l)|.$$

По предположению индукции, примененному к формуле $C(a,l)$,

$$|C(t_1,l)| = |C(|t_1|,l)|$$

для каждого $l \in M$. Теперь из $(**)$ получаем

$$|B_1(t_1)| = |B_1(|t_1|)|.$$

(2.4) (шаг индукции) $B_1(a) = \forall x[x/b]C(a,b)$.

Доказательство аналогично (2.3): $\exists$ заменяется на $\forall$, а max — на min. ■

Исчисление предикатов с равенством

Определение 1. *Пусть Ω — сигнатура, содержащая предикатный символ равенства $=$.* Исчисление предикатов с равенством *в сигнатуре Ω получается из обычного исчисления предикатов PC_Ω добавлением аксиом стандартной теории равенства Eq_Ω (см. лекцию 8).*

Для теорий в такой сигнатуре можно рассматривать нормальные модели и логическое следование на них: $T \vDash_{\text{норм}} A$ означает, что (замкнутая) формула A истинна во всех нормальных моделях теории T.

Также можно определить нормальную общезначимость: формула *нормально общезначима*, если ее универсальное замыкание $\overline{\forall} A$ истинно во всех нормальных моделях данной сигнатуры.

Теорема 12.2. *(Теорема о корректности исчисления предикатов с равенством)*

(1) Пусть T — теория 1го порядка с равенством в сигнатуре Ω. Тогда для любой замкнутой формулы A этой сигнатуры

$$T \vdash_{PC_\Omega^=} A \Rightarrow T \vDash_{\text{норм}} A.$$

(2) Для любой формулы A сигнатуры Ω

$$\vdash_{PC_\Omega} A \ \Rightarrow \vDash_{\text{норм}} A,$$

т.е. все теоремы исчисления предикатов с равенством нормально общезначимы.

Доказательство (1) Пусть $T \vdash_{PC_\Omega^=} A$. По определению, это означает $T \cup Eq_\Omega \vdash_{PC_\Omega} A$. По теореме корректности 11.10

$$T \cup Eq_\Omega \vDash A.$$

Если $M \vDash T$ и M нормальна, то $M \vDash Eq_\Omega$ (лемма 8.4). Тогда $M \vDash A$.

(2) Как и в теореме 11.10, рассмотрим $T = \varnothing$ и применим (1) для $\overline{\forall} A$. ■

Непротиворечивость

Определение 2. *Теория T в сигнатуре Ω называется* противоречивой*, если для некоторой формулы A в этой сигнатуре*

$$T \vdash_{PC_\Omega} A \text{ и } T \vdash_{PC_\Omega} \neg A.$$

Аналогично, теория T в сигнатуре Ω с равенством противоречива*, если $T \vdash_{PC_\Omega^=} A$ и $T \vdash_{PC_\Omega^=} \neg A$ для некоторой формулы A сигнатуры Ω.*

Лемма 12.3. *Если теория T в сигнатуре Ω противоречива, то $T \vdash_{PC_\Omega} B$ для любой формулы сигнатуры B; аналогично — для теорий с равенством.*

Доказательство См. лемму 5.4 (2). ■

Следствие 12.4. *(1) Если теория 1го порядка выполнима, то она непротиворечива.*

(2) Если теория 1го порядка с равенством нормально выполнима (т.е. имеет нормальную модель), то она непротиворечива.

Доказательство (1) Предположим, что теория T в сигнатуре Ω противоречива. Предположим, что $M \vDash T$. Возьмем какую-нибудь замкнутую формулу B, истинную в M (например, формулу вида $A \to A$). По лемме 12.3, $T \vdash_{PC_\Omega} \neg B$. Тогда по теореме корректности 11.10, $T \vDash \neg B$. Следовательно, $M \vDash \neg B$, что противоречит выбору B.

(2) Аналогично, с использованием $PC_\Omega^=$. ■

Пример: арифметика Пеано

Арифметика Пеано (PA) — это теория 1го порядка в сигнатуре $\{0, 1, +, \cdot, =\}$ (см. лекцию 6) со следующими аксиомами:

(1) $\forall x\,(x + 1 \neq 0)$.

(2) $\forall x \forall y\,(x + 1 = y + 1 \to x = y)$.

(3) $\forall x\,(x \neq 0 \to \exists y\,(y + 1 = x))$.

(4) $\forall x\,(x + 0 = 0)$.

(5) $\forall x\,(x + (y + 1) = (x + y) + 1)$.

(6) $\forall x\,(x \cdot 0 = 0)$.

(7) $\forall x \forall y\,(x \cdot (y + 1) = x \cdot y + x)$.

(8) $\overline{\forall}\,(A(0) \wedge \forall x\,(A(x) \to A(x + 1)) \to \forall x\,A(x))$.

Здесь (1)–(7) — конкретные формулы, а (8) — схема, т.е. бесконечное множество аксиом определенного вида. Предполагается, что A — формула с несколькими свободными переменными, т.е. $A = A(a, \ldots)$. $A(0),\ A(x)$ обозначают соответственно $[0/a]A,\ [x/a]A$; $\forall x\,(A(x) \to A(x{+}1))$ — это формула $\forall x\,[x/a](A \to [a + 1/a]A)$.

(8) называется *схемой аксиом индукции*. Она выражает принцип математической индукции: если какое-то свойство A верно для 0 и из истинности A для x следует истинность для $x + 1$, то A верно для всех x. Однако в теории PA индукция постулируется только для тех свойств, которые можно записать формулами в данной сигнатуре.

Хотя теория PA и называется "арифметика Пеано", она отличается от той, которую рассматривал сам Пеано: в его теории индукция применима ко всем свойствам натуральных чисел. Теория Пеано (в современном понимании) соответствует арифметике 2го порядка, которая в нашем курсе не изучается.

Теорема PA непротиворечива.

"Доказательство". PA имеет *стандартную модель* $\mathbf{N}$: множество натуральных чисел (включая 0), где $+$ интерпретируется как операция сложения, $\cdot$ — как операция умножения, константа 0 — как число нуль, константа 1 — как число единица. Все аксиомы PA верны в этой модели. По следствию 12.4, PA непротиворечива.

Это — метаматематическое рассуждение; в нем предполагается известным, что такое натуральные числа и какие у них свойства. Чтобы дать строгое математическое доказательство, нужна формальная теория, где мы можем определить множество натуральных чисел. Это делается в аксиоматической теории множеств, о чем будет сказано кратко в лекции 14.

Модальное исчисление S5

Некоторые части логики предикатов можно превратить в логики высказываний — так называемые *модальные логики*. В модальных логиках к обычным булевым связкам добавляются модальные связки, в простейшем случае — одноместная связка "необходимо" ($\Box$).

В отличие от булевых связок, логические свойства связки $\Box$ не очевидны и допускают много вариаций. Первые модальные исчисления были построены К.Льюисом (1918) и названы им S1,..., S5. А вообще имеется огромное число (континуум) различных модальных логик.

В этом курсе мы рассмотрим только исчисление S5. Современная формулировка его была дана Гёделем (1933).

Определение 3. Множество модальных формул MFm *строится по следующим правилам:*

- *Если* $A \in Var$, *то* $A \in MFm$.
- *Если* $A, B \in MFm$, *то* $(A \wedge B) \in MFm$.
- *Если* $A, B \in MFm$, *то* $(A \vee B) \in MFm$.
- *Если* $A, B \in MFm$, *то* $(A \to B) \in MFm$.
- *Если* $A \in MFm$, *то* $\neg A \in MFm$.
- *Если* $A \in MFm$, *то* $\Box A \in MFm$.

Также будем использовать связку "возможно" ($\Diamond$), которая определяется как сокращение:

$$\Diamond := \neg\Box\neg$$

.

Схемы аксиом S5

(I) Схемы (1)–(10) из CL, но для модальных формул.

(II)

$$
\begin{array}{ll}
(AK) & \Box(A \to B) \to (\Box A \to \Box B),\\
(AT) & \Box A \to A,\\
(A4) & \Box A \to \Box\Box A,\\
(A5) & \Diamond\Box A \to \Box A.
\end{array}
$$

Правила вывода S5

Modus Ponens (MP),

Правило добавления $\Box$ (Nec): $\dfrac{A}{\Box A}$

Понятия вывода и выводимости в $S5$ определяются аналогично CL (с учетом дополнительного правила), точное определение оставляется читателю.

Семантика Крипке для S5

Определение 4. *Пусть $W \neq \varnothing$ — множество.* Оценка *(пропозициональных переменных) на W — это отображение $Var \longrightarrow \mathcal{P}(W)$.* Модель Крипке[2] *на W — это пара (W, θ), где θ — оценка на W. W называется* множеством (возможных) миров *этой модели.*

Определение 5. *Для модели Крипке $M = (W, \theta)$, мира $u \in W$ и модальной формулы A определяем* значение A в u*; оно обозначается $|A|_u^M$. Определение дается индукцией по длине A сразу для всех миров u:*

- $|P_i|_u^M = 1 \Leftrightarrow u \in \theta(P_i)$ *для каждой переменной P_i,*
- $|A \wedge B|_u^M = \min(|A|_u^M, |B|_u^M)$,
- $|A \vee B|_u^M = \max(|A|_u^M, |B|_u^M)$,
- $|\neg A|_u^M = 1 - |A|_u^M$,
- $|A \to B|_u^M = \max(1 - |A|_u^M, |B|_u^M)$,
- $|\Box A|_u^M = \min\limits_{v \in W} |A|_v^M$.

Чтобы доказать корректность этого определения, нужна лемма об однозначном анализе формул, аналогичная лемме 1.1. См. лекцию 1.

Вместо $|A|_u^M = 1$ пишут также $M, u \vDash A$ и говорят, что формула A *истинна в модели M в мире u.*

В этих обозначениях определение 5 записывается так:

[2]Иногда говорят: модель Крипке – Лейбница

- $M, u \vDash P_i \Leftrightarrow u \in \theta(P_i)$,
- $M, u \vDash A \wedge B \Leftrightarrow M, u \vDash A$ и $M, u \vDash B$,
- $M, u \vDash A \vee B \Leftrightarrow M, u \vDash A$ или $M, u \vDash B$,
- $M, u \vDash \neg A \Leftrightarrow M, u \nvDash A$,
- $M, u \vDash A \to B \Leftrightarrow M, u \nvDash A$ или $M, u \vDash B$,
- $M, u \vDash \Box A \Leftrightarrow \forall v \in W\, M, v \vDash A$.

Из определения сразу получаем:

$$M, u \vDash \Diamond A \Leftrightarrow \exists v \in W\, M, v \vDash A.$$

Таким образом, в семантике Крипке "необходимо" ($\Box$) понимается как истинность во всех мирах ("всегда"), а "возможно" ($\Diamond$) — как истинность в некоторых мирах ("иногда").

Определение 6. *Модальная формула A* общезначима *на (непустом) множестве W, если она истинна во всех мирах в любой модели Крипке на W.*

Общезначимость A на W обозначается $W \vDash A$.

Теорема 12.5. *(теорема корректности для $S5$)*
Если $\vdash_{S5} A$, то $W \vDash A$ для любого $W \neq \varnothing$.

Это утверждение можно доказать индукцией по длине вывода A. У нас оно получится как следствие другой теоремы на следующей лекции.

Стандартный перевод модальных формул

Определение 7. *Рассмотрим сигнатуру со счетным множеством одноместных предикатных символов: $P_1^1, P_2^1, \ldots$* Стандартный перевод *(или перевод Вайсберга) $A \mapsto A^*$ модальных формул в формулы 1го порядка в этой сигнатуре определяется по индукции:*

- $P_i^* := P_i^1(a)$,
- $(A \circ B)^* := (A^* \circ B^*)$ *для* $\circ = \vee, \to, \wedge$,
- $(\neg A)^* := \neg A^*$,

- $(\Box A)^* := \forall x\,[x/a]A^*$, *где* x *— первая связанная переменная (в общем списке* $BVar$ *— см. лекцию 6), не входящая в* A.[3]

Таким образом, A^* — формула с одной свободной переменной a или замкнутая.

Определение 8. *Каждой модели Крипке* $M = (W, \theta)$ *поставим в соответствие модель* M^* *сигнатуры* $\{P_1^1, P_2^1, \ldots\}$ *с носителем* W*. А именно, полагаем для каждого* $u \in W$

$$M^* \vDash P_i^1(u) \Leftrightarrow M, u \vDash P_i.$$

Это можно записать и так:

$$|P_i^1(u)|_{M^*} := |P_i|_u^M.$$

Лемма 12.6. *Для любой модальной формулы* A

$$|A^*(u)|_{M^*} = |A|_u^M.$$

Доказательство Индукцией по длине A доказываем утверждение для всех u.

Если A — переменная, утверждение следует из определений 7, 8.

Если A имеет вид отрицания, конъюнкции, дизъюнкции или импликации, утверждение легко следует из определений истинности для модальных формул и формул 1го порядка — упражнение.

Пусть $A = \Box B$. Тогда по определению 5 лекции 7 и опр. 5 выше,

$$|A^*(u)|_{M^*} = |(\forall x\,[x/a]B^*)(u)|_{M^*} = \min_{v \in W} |B^*(v)|_{M^*},$$

$$|A|_u^M = \min_{v \in W} |B|_v^M.$$

По предположению индукции, $|B^*(v)|_{M^*} = |B|_v^M$. Поэтому утверждение верно для A. ■

Лемма 12.7. [4] *Для любой модальной формулы* A *и непустого* W

$$W \vDash \forall x\,[x/a]A^* \text{ в классической логике } \Leftrightarrow W \vDash A \text{ в модальной логике }.$$

[3]Можно взять и любую другую переменную, не попавшую в A, но мы выбираем первую для единообразия.

[4]На лекции в формулировке этой леммы была допущена неточность: запись $\forall u A^*(u)$ неправомерна.

Доказательство ($\Rightarrow$) Доказываем от противного. Пусть $W \not\models A$, тогда для некоторой модели Крипке на W и какого-то мира $u \in W$

$$M, u \not\models A.$$

Отсюда по лемме 12.6

$$M^* \not\models A^*(u),$$

следовательно,

$$M^* \not\models \forall x\, [x/a] A^*,$$

и потому

$$W \not\models \forall x\, [x/a] A^*.$$

($\Leftarrow$) Тоже рассуждаем от противного. Пусть

$$W \not\models \forall x\, [x/a] A^*.$$

Тогда найдется модель μ нашей сигнатуры (с одноместными предикатами) с носителем W такая, что

$$\mu \not\models \forall x\, [x/a] A^*.$$

т.е. для некоторого $u \in W$

$$(\sharp) \qquad \mu \not\models A^*(u).$$

Но $\mu = M^*$ для некоторой модели Крипке M на W: она однозначно задается равенствами

$$|P_i|^M_v = |P^1_i(v)|_\mu$$

для всех v, i. Поэтому из ($\sharp$) по лемме 12.6 получаем

$$M, u \not\models A.$$

Таким образом, $W \not\models A$. ∎