Полные теории Вычислимость лекция 9

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

lbekl@yandex.ru

9.04.2009

Полные теории

Опр.

Теория T *полна*, если

- T непротиворечива;
- Для любого предложения A в языке T $T \vdash A$ или $T \vdash \neg A$.

Пример.

$Th(M)$ для любой модели M.

Утверждение.

Если T полна и $M \models T$, то $T \equiv Th(M)$.

Теорема. (Линденбаум)

Всякая непротиворечивая теория имеет полное расширение.

Аксиоматизируемость

Опр.

Теория T *эффективно аксиоматизируема*, если существует алгоритм, распознающий аксиомы T.

Опр.

Теория T *разрешима*, если существует алгоритм, распознающий теоремы T.

Теорема.

Если T полна и эффективно аксиоматизируема, то T разрешима.

Доказательство.

Пусть дано предложение A. Перебираем все возможные выводы в T до тех пор, пока не встретим доказательство A или доказательство $\neg A$. Полнота гарантирует, что одно из двух произойдёт.

Примеры полных эфф. аксиоматизируемых теорий

- Элементарная геометрия (G1-G11). $Th(\mathbb{R}^2; =, \cong, B)$
- Теория вещественно замкнутых упорядоченных полей. $Th(\mathbb{R}; =, <, +, \cdot, 0, 1)$
- Теория алгебраически замкнутых полей характеристики 0. $Th(\mathbb{C}; =, +, \cdot, 0, 1)$
- Теория плотных линейных порядков без первого и последнего элементов. $Th(\mathbb{Q}; =, <)$

Универсальные теории

- *Арифметика Пеано* PA.
  Формализует математику конечного.
  Основана на аксиомах для натуральных чисел в сигнатуре $=$, 0, S, $+$, $\cdot$.

- *Теория множеств Цермело–Френкеля (с аксиомой выбора)* ZFC.
  Формализует всю «обычную» математику.
  Основана на аксиомах для множеств и отношения принадлежности $\in$.

Аксиомы PA

1. аксиомы равенства для S, $+$, $\cdot$;
2. $\neg S(a) = 0, \quad S(a) = S(b) \to a = b$,
3. $a + 0 = a, \quad a + S(b) = S(a + b)$,
4. $a \cdot 0 = 0, \quad a \cdot S(b) = a \cdot b + a$,
5. (Схема аксиом индукции)

   $$A[a/0] \wedge \forall x\,(A[a/x] \to A[a/S(x)]) \to \forall x\,A[a/x]$$

   для любой формулы A.

Первая теорема Гёделя о неполноте

Теорема.

Если T содержит PA, непротиворечива и эффективно аксиоматизируема, то T неполна.

Следствие.

- PA неполна.
- ZFC неполна при условии её непротиворечивости.

Интерпретации

Опр.

Модель $(M; \Omega)$ *интерпретируема в* $(N; \Sigma)$, если её носитель M и все предикаты, функции и константы сигнатуры Ω на M определимы в N.

Опр.

Перевод I сигнатуры Ω в сигнатуру Σ задаётся:

- формулой $D_I(a) \in \mathrm{Fm}_\Sigma$, определяющей носитель M;
- сопоставляет каждому символу Ω формулу сигнатуры Σ соответствующей валентности:

$$
\begin{array}{ccc}
P & \longmapsto & P_I(a_1, \dots, a_n) \\
f & \longmapsto & F_I(a_1, \dots, a_n, b) \\
c & \longmapsto & C_I(a)
\end{array}
$$

Для данного перевода I и модели $(N; \Sigma)$ положим

$$M_I \rightleftharpoons \{x \in N : N \vDash D_I[x]\}.$$

Опр.

I есть *интерпретация M в N*, если

$$(M_I; P_I, f_I, c_I) \cong (M; P, f, c),$$

а P_I, f_I и c_I — предикат, функция и константа на M_I, определимые в N формулами P_I, F_I и C_I, соответственно.

Замечание.

Для нормальной модели M условие изоморфизма

$$(M_I; =_I) \cong (M; =)$$

говорит о том, что $=_I$ есть отношение равенства на множестве M_I.

Т.е. можно считать, что $=_I$ есть $=$.

Пример.
$(\mathbb{Z}; <)$ интерпретируема в $(\mathbb{N}; +, =)$.

$E(a) \rightleftharpoons (\exists x\, x + x = a)$ «a чётно»

$$\begin{aligned} a <_I b \quad \Longleftrightarrow \quad & (E(a) \wedge E(b) \wedge a > b) \vee \\ & (E(a) \wedge \neg E(b)) \vee \\ & (\neg E(b) \wedge \neg E(a) \wedge a < b) \end{aligned}$$

Чётные $=$ отрицательные,
нечётные $=$ положительные.

Более общие интерпретации

- Допустима интерпретация одного объекта из M набором объектов из N (*многомерные интерпретации*).
- Допустимы параметры (*параметрические интерпретации*).

Многомерные интерпретации с параметрами

$a \in M \longmapsto \vec{a} = (a_1, \ldots, a_n) \in N^n$

Перевод I задаётся формулой $D_I(\vec{a}, \vec{p})$ и переводами символов Ω:

$$\begin{aligned} P &\longmapsto P_I(\vec{a}_1, \ldots, \vec{a}_n, \vec{p}) \\ f &\longmapsto F_I(\vec{a}_1, \ldots, \vec{a}_n, \vec{b}, \vec{p}) \end{aligned}$$

Опр.

Для данного набора параметров $\vec{c}$ из N положим

$$M_I \rightleftharpoons \{\vec{x} \in N^n : N \vDash D_I[\vec{x}, \vec{c}]\}.$$

I — интерпретация, если

$$(M_I; P_I, f_I) \cong (M; P, f),$$

а P_I, f_I — предикат и функция на M_I, определимые в $(N; \vec{c})$ формулами P_I и F_I, соответственно.

Опр.

Набор констант $\vec{c}$, для которого выполнено это условие, называется *допустимым* для данной интерпретации I.

Опр.

Интерпретация I имеет *определимые параметры*, если для некоторой формулы $Par_I(\vec{p})$ сигнатуры Σ

- $N \models \exists \vec{x} Par_I(\vec{x})$;
- если $N \models Par_I[\vec{c}]$, то набор $\vec{c}$ допустим для I.

Опр.

Набор констант $\vec{c}$, для которого выполнено это условие, называется *допустимым* для данной интерпретации I.

Опр.

Интерпретация I имеет *определимые параметры*, если для некоторой формулы $Par_I(\vec{p})$ сигнатуры Σ

- $N \models \exists \vec{x} Par_I(\vec{x})$;
- если $N \models Par_I[\vec{c}]$, то набор $\vec{c}$ допустим для I.

Пример.

$(\mathbb{R}^2; =, B, \cong)$ интерпретируема в $(\mathbb{R}; =, +, \cdot, 0, 1)$.

$a \leq b \rightleftharpoons (\exists z\ a + z \cdot z = b)$
$a - b = c \rightleftharpoons (c + b = a)$

$$D_I(a_1, a_2) \rightleftharpoons (a_1 = a_1 \wedge a_2 = a_2)$$

$$B_I(\vec{a}, \vec{b}, \vec{c}) \rightleftharpoons \exists \lambda, \mu \,(0 \leq \lambda \wedge 0 \leq \mu \wedge \\ \wedge \lambda + \mu = 1 \wedge \vec{b} = \lambda\vec{a} + \mu\vec{c})$$

$$\vec{a}\vec{b} \cong_I \vec{c}\vec{d} \rightleftharpoons (a_1 - b_1)^2 + (a_2 - b_2)^2 = \\ = (c_1 - d_1)^2 + (c_2 - d_2)^2.$$

Пример.

$(\mathbb{R}; =, +, \cdot, 0, 1)$ интерпретируема в $(\mathbb{R}^2; =, B, \cong)$.

Параметры p_0, p_1 — две различные точки;

$$D_I(a) \rightleftharpoons (a \in p_0 p_1),\ 0_I \rightleftharpoons p_0,\ 1_I \rightleftharpoons p_1$$

$$\begin{aligned} a +_I b = c \rightleftharpoons (Bp_0ac \wedge Bp_0bc \wedge p_0b \cong ac)\vee \\ \vee(Bap_0b \wedge Bacb \wedge ap_0 \cong bc) \end{aligned}$$

$$\begin{aligned} a \cdot_I b = c \rightleftharpoons \exists u, v\ (Bp_0uv \wedge p_0u \cong p_0b\wedge \\ p_1u \| av \wedge p_0v \cong p_0c) \wedge (Bap_0b \leftrightarrow Bcp_0p_1). \end{aligned}$$

Упражнения

Определить интерпретации:

- $(\mathbb{C}; =, +, \cdot, 0, 1)$ в поле $\mathbb{R}$.
- $(\mathbb{Q}; =, +, \cdot, 0, 1)$ в стандартной модели $\mathbb{N}$.
- Доказать, что поле $\mathbb{R}$ не интерпретируемо в поле $\mathbb{Q}$.

Перевод формул

Пусть I — перевод сигнатуры Ω в Σ. Перевод A^I формулы $A \in \mathrm{Fm}_\Omega$ определим индуктивно:

- $P(a, b)^I \rightleftharpoons P_I(\vec{a}, \vec{b}, \vec{p})$,
  $(f(a) = b)^I \rightleftharpoons F_I(\vec{a}, \vec{b}, \vec{p})$,
- $(\neg A)^I \rightleftharpoons \neg A^I$, $(A \wedge B)^I \rightleftharpoons (A^I \wedge B^I)$,
- $(\forall x A[a/x])^I \rightleftharpoons \forall \vec{x}\,(D_I(\vec{x}, \vec{p}) \to A^I[\vec{a}/\vec{x}])$,
- $(\exists x A[a/x])^I \rightleftharpoons \exists \vec{x}\,(D_I(\vec{x}, \vec{p}) \wedge A^I[\vec{a}/\vec{x}])$.

Замечание.

Всякая формула A логически эквивалентна формуле A', в которой любая атомарная подформула имеет вид $P(x_1, \ldots, x_n)$ или $f(x_1, \ldots, x_n) = y$, где $x_1, \ldots, x_n, y$ — переменные.

Доказательство.

$f(g(a)) = b \;\equiv\; \exists x \, (g(a) = x \wedge f(x) = b)$.

Пусть $\vec{x}_I$ означает элемент модели M_I, соответствующий $x \in M$.

Лемма.

Для любой A в языке M, любых $\vec{x} \in M$ и допустимых $\vec{c} \in N$

$$M \models A[\vec{x}] \iff N \models A^I[\vec{x}_I, \vec{c}].$$

Доказательство.

Индукция по построению A.

Теорема.

Если M интерпретируема в N с определимыми параметрами и $Th(N)$ разрешима, то такова и $Th(M)$.

Доказательство.

Для данного предложения A в языке M имеем

$$M \models A \iff N \models \forall \vec{x}\,(Par_I(\vec{x}) \to A^I(\vec{x})).$$

Следствие.

Разрешимость элементарной геометрии равносильна разрешимости $Th(\mathbb{R})$.

Вычислимость. Неформальное представление об алгоритмах.

- *Алгоритм* есть предписание выполнить точно определённую последовательность действий.
- Для данного алгоритма $\mathcal{A}$ определены:
  - *область возможных исходных данных* X;
  - *область возможных значений* Y.

  В качестве данных обычно рассматриваются слова $X = \Sigma^*$, где Σ — конечный алфавит, или числа $X = \mathbb{N}^n$.

Выполнение алгоритма

- Процесс применения алгоритма $\mathcal{A}$ к данным $x \in X$ происходит по шагам.
- Процесс или заканчивается после конечного числа шагов с результатом $y \in Y$, или останавливается без результата или продолжается бесконечно.
- Таким образом, с алгоритмом $\mathcal{A}$ связывается *частичная функция* $f : X \to Y$.

Частичные функции

Опр.

Частичной функцией $f : X \to Y$ называется подмножество $f \subseteq X \times Y$ такое, что из $\langle x, y_1 \rangle \in f$ и $\langle x, y_2 \rangle \in f$ следует $y_1 = y_2$.

Опр.

Пишем $f(x) = y$ вместо $\langle x, y \rangle \in f$;

$!f(x)$ вместо $\exists y\, f(x) = y$.

Опр.

Областью определения частичной функции f называется множество $dom(f) \rightleftharpoons \{x \in X : \exists y \in Y\ \langle x, y \rangle \in f\}$.

Опр.

Областью значений частичной функции f называется множество $rng(f) \rightleftharpoons \{y \in Y : \exists x \in X\ \langle x, y \rangle \in f\}$.

Вычислимые функции

Опр.

Частичная функция $f : X \to Y$ *вычислима*, если она вычисляется некоторым алгоритмом.

В частности, можно говорить о вычислимых функциях $f : \Sigma^* \to \Sigma^*$, $f : \mathbb{N}^k \to \mathbb{N}$ и т.д.

Вычислительные модели

- Машины Тьюринга (А. Тьюринг, Э. Пост)
- Частично рекурсивные функции (К. Гёдель, С. Клини)
- Лямбда-исчисление (А. Чёрч)
- Алгорифмы Маркова
- Машины с неограниченными регистрами
- Pascal, C, Java, Lisp, ...

Эквивалентность вычислительных моделей

Теорема.

Каждая из вышеперечисленных моделей определяет один и тот же класс вычислимых частичных функций $f : \Sigma^* \to \Sigma^*$.

Тезис Чёрча–Тьюринга

Тезис: Любая вычислимая в интуитивном смысле частичная функция $f : \Sigma^* \to \Sigma^*$ вычислима на машине Тьюринга.

Замечание.
Это утверждение не является математическим, но говорит об адекватности математической модели (вычислимости по Тьюрингу) *реальному* явлению (вычислимости).

Подтверждения тезиса Чёрча–Тьюринга

Все попытки построения более общих вычислительных моделей неизбежно приводили к тому же самому классу вычислимых функций.

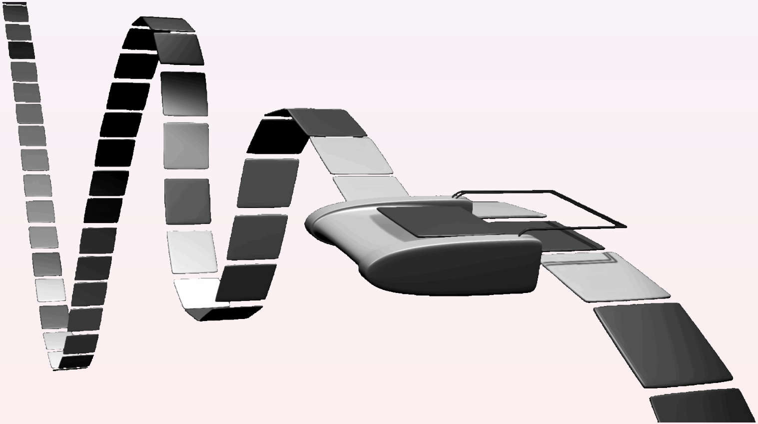
Физический тезис Чёрча–Тьюринга

Текущему уровню знаний не противоречит и более сильный

Тезис: Всякая функция $f : \Sigma^* \to \Sigma^*$, вычислимая на (идеализированном) *физически реализуемом* устройстве, вычислима на машине Тьюринга.

Замечание.
Физический тезис предполагает возможность аналогового вычисления, квантово–механические эффекты и т.д.

Машина Тьюринга



Машины Тьюринга

Опр.

Машина Тьюринга задаётся конечными

- рабочим алфавитом Σ, содержащим символ $\#$ (пробел);
- множеством состояний Q, содержащим состояния q_1 (начальное) и q_0 (конечное);
- набором команд (программой) P.

Команды

- Команды имеют вид $qa \to rb\nu$, где $q, r \in Q$, $a, b \in \Sigma$ и $\nu \in \{L, N, R\}$.

  «прочтя символ a в состоянии q перейти в состояние r, заменить содержимое ячейки на b и сместиться влево (L), остаться на месте (N) или сместиться вправо (R) на одну ячейку, в зависимости от значения ν»

- Требуется, чтобы в программе P была ровно одна команда с левой частью qa для каждого $q \in Q \setminus \{q_0\}$ и $a \in \Sigma$.

Соглашение: команды вида $qa \longrightarrow qaN$, приводящие к зацикливанию, можно не указывать.

Опр.

Машина Тьюринга есть набор
$M = \langle Q, \Sigma, P, q_0, q_1 \rangle$.

Пример.

Пусть $\Sigma = \{\#, 0, 1\}$, $Q = \{q_0, q_1\}$, а P состоит из следующих команд:

$$
\begin{aligned}
q_1\# &\mapsto q_1\#R \\
q_10 &\mapsto q_11R \\
q_11 &\mapsto q_10R
\end{aligned}
$$

Что делает эта машина Тьюринга?

Модифицируем программу.

Пусть $\Sigma = \{\#, 0, 1\}$, $Q = \{q_0, q_1, q_2\}$, а P состоит из следующих команд:

$$\begin{array}{rcl} q_1\# & \mapsto & q_1\#R \\ q_10 & \mapsto & q_21R \\ q_11 & \mapsto & q_20R \\ q_20 & \mapsto & q_21R \\ q_21 & \mapsto & q_20R \\ q_2\# & \mapsto & q_0\#N \end{array}$$