Интерпретируемость Вычислимость лекция 9

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

lbekl@yandex.ru

3.04.2008

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:

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

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.

Общие интерпретации

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

Многомерные интерпретации

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

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

$$\begin{array}{ccc} P & \longmapsto & P_I(\vec{a}_1, \ldots, \vec{a}_n) \\ f & \longmapsto & F_I(\vec{a}_1, \ldots, \vec{a}_n, \vec{b}) \\ c & \longmapsto & C_I(\vec{a}) \end{array}$$

Положим

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

I — интерпретация, 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.

Пример.

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

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

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

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

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

Мягкое равенство

Опр.

Пусть $(M; =, P, f)$ — нормальная модель, I — перевод. Вместо изоморфизма $(M_I; =_I, P_I, f_I) \cong M$ требуем:

- Формула $\vec{a} =_I \vec{b}$ удовлетворяет в N аксиомам равенства для сигнатуры Ω, напр.

  $$N \vDash D_I(\vec{x}) \wedge D_I(\vec{y}) \wedge \vec{x} =_I \vec{y} \to (P_I(\vec{x}) \leftrightarrow P_I(\vec{y}));$$

  и аналогично для F_I.
- $(M; =, P, f) \cong (M_I; =_I, P_I, f_I) / =_I$.

Пример.

$(\mathbb{Z}; =, +, \cdot, 0, 1)$ интерпретируема в $(\mathbb{N}; =, S, +, \cdot)$.
Число $z \in \mathbb{Z}$ представляем парой $(m, n) \in \mathbb{N}^2$, где $z = m - n$.

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

$$(a_1, a_2) =_I (b_1, b_2) \rightleftharpoons (a_1 + b_2 = a_2 + b_1)$$

$$(a_1, a_2) +_I (b_1, b_2) \rightleftharpoons (a_1 + b_1, a_2 + b_2)$$

$$(a_1, a_2) \cdot_I (b_1, b_2) \rightleftharpoons (a_1 b_1 + a_2 b_2, a_1 b_2 + a_2 b_1)$$

$$0_I(a_1, a_2) \rightleftharpoons (a_1 = a_2) \qquad 1_I(a_1, a_2) \rightleftharpoons (a_1 = S(a_2))$$

Интерпретации с параметрами

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

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

Опр.

Перевод I есть *интерпретация M в N*, если для некоторого набора констант $\vec{c} \in N$:

- $=_I(\vec{a}, \vec{b}, \vec{c})$ удовлетворяет в N аксиомам равенства для сигнатуры Ω;
- $(M_I; P_I, f_I)/{=_I}$ изоморфна M, где $M_I = \{\vec{x} \in N^n : N \vDash D_I[\vec{x}, \vec{c}]\}$, а P_I и 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 выполнены эти условия, 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 выполнены эти условия, называется *допустимым* для данной интерпретации I.

Опр.

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

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

Пример.

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

Параметры p_0, p_1 — две различные точки;

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

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

$$a \cdot_I b = c \rightleftharpoons \exists u, v\, (Bp_0uv \wedge p_0u \cong p_0b \wedge \\ \wedge p_1u \| av \wedge p_0v \cong p_0c).$$

(для положительных a, b, c)

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 $x \in M$.

Теорема.

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.

Следствие.

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 $Th(\mathbb{R})$.

Интерпретируемость теорий

Опр.

Перевод I с определимыми параметрами есть *интерпретация теории T в U*, если

- для любой аксиомы $A \in T$ $U \vdash Par_I(\vec{p}) \to A^I$;
- $U \vdash Par_I(\vec{p}) \to \exists \vec{x} D_I(\vec{x}, \vec{p})$;
- в U выводимы переводы аксиом равенства для сигнатуры Ω;
- $U \vdash Par_I(\vec{p}) \to (\forall x \exists! y\, f(x) = y)^I$ для всех $f \in \mathrm{Func}_\Omega$.

Интерпретируемость теорий

Опр.

Перевод I с определимыми параметрами есть *интерпретация теории* T *в* U, если

- для любой аксиомы $A \in T$ $U \vdash Par_I(\vec{p}) \to A^I$;
- $U \vdash Par_I(\vec{p}) \to \exists \vec{x} D_I(\vec{x}, \vec{p})$;
- в U выводимы переводы аксиом равенства для сигнатуры Ω;
- $U \vdash Par_I(\vec{p}) \to (\forall x \exists ! y\, f(x) = y)^I$ для всех $f \in \mathrm{Func}_\Omega$.

Интерпретируемость теорий

Опр.

Перевод I с определимыми параметрами есть *интерпретация теории T в U*, если

- для любой аксиомы $A \in T$ $U \vdash Par_I(\vec{p}) \to A^I$;
- $U \vdash Par_I(\vec{p}) \to \exists \vec{x} D_I(\vec{x}, \vec{p})$;
- в U выводимы переводы аксиом равенства для сигнатуры Ω;
- $U \vdash Par_I(\vec{p}) \to (\forall x \exists! y\, f(x) = y)^I$ для всех $f \in \mathrm{Func}_\Omega$.

Интерпретируемость теорий

Опр.

Перевод I с определимыми параметрами есть *интерпретация теории T в U*, если

- для любой аксиомы $A \in T$ $U \vdash Par_I(\vec{p}) \to A^I$;
- $U \vdash Par_I(\vec{p}) \to \exists \vec{x} D_I(\vec{x}, \vec{p})$;
- в U выводимы переводы аксиом равенства для сигнатуры Ω;
- $U \vdash Par_I(\vec{p}) \to (\forall x \exists ! y\, f(x) = y)^I$ для всех $f \in \mathrm{Func}_\Omega$.

Интерпретируемость теорий

Опр.

Перевод I с определимыми параметрами есть *интерпретация теории T в U*, если

- для любой аксиомы $A \in T$ $U \vdash Par_I(\vec{p}) \to A^I$;
- $U \vdash Par_I(\vec{p}) \to \exists \vec{x} D_I(\vec{x}, \vec{p})$;
- в U выводимы переводы аксиом равенства для сигнатуры Ω;
- $U \vdash Par_I(\vec{p}) \to (\forall x \exists ! y\, f(x) = y)^I$ для всех $f \in \mathrm{Func}_\Omega$.

Опр.

Теория T *интерпретируема в* U, если существует интерпретация T в U.

Предложение.

Если T *интерпретируема в* U *и* $T \vdash A$, *то* $U \vdash \forall \vec{x}\,(Par_I(\vec{p}) \wedge D_I(\vec{x}, \vec{p}) \to A^I(\vec{x}, \vec{p}))$.

Доказательство.

Индукция по длине вывода формулы A.

Опр.

Теория T *интерпретируема в* U, если существует интерпретация T в U.

Предложение.

Если T *интерпретируема в* U *и* $T \vdash A$*, то* $U \vdash \forall \vec{x}\,(Par_I(\vec{p}) \land D_I(\vec{x}, \vec{p}) \to A^I(\vec{x}, \vec{p}))$.

Доказательство.

Индукция по длине вывода формулы A.

Следствие.
Если T интерпретируема в U и теория U непротиворечива, то такова и T.

Замечание.
Этот результат установлен элементарными (синтаксическими) методами, не опирающимися на теорию множеств.

Следствие.

Если непротиворечива евклидова геометрия, то непротиворечива геометрия Лобачевского.

Следствие.

Если непротиворечива арифметика Пеано, то непротиворечива $Th(\mathbb{R})$ и элементарная геометрия.

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.

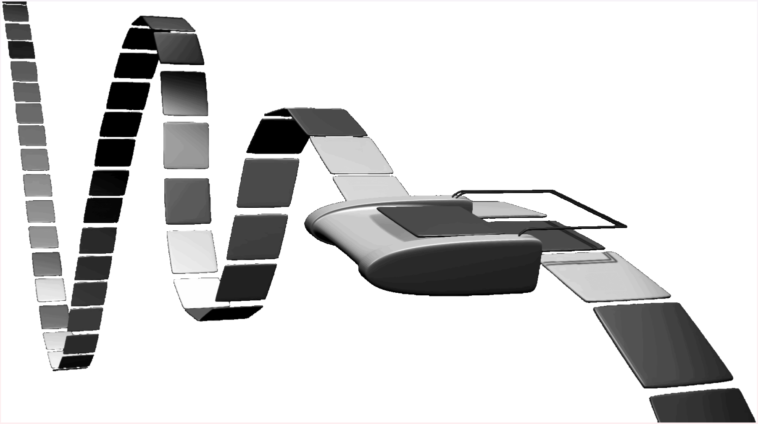
Физический тезис Чёрча–Тьюринга

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 $qa \to qaN$, 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:

$$
\begin{array}{rcl}
q_1\# & \mapsto & q_1\#R \\
q_1 0 & \mapsto & q_1 1 R \\
q_1 1 & \mapsto & q_1 0 R
\end{array}
$$

Что делает эта машина Тьюринга?

Модифицируем программу.

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

$$
\begin{aligned}
q_1\# &\mapsto q_1\#R \\
q_1 0 &\mapsto q_2 1R \\
q_1 1 &\mapsto q_2 0R \\
q_2 0 &\mapsto q_2 1R \\
q_2 1 &\mapsto q_2 0R \\
q_2\# &\mapsto q_0\#N
\end{aligned}
$$

Конфигурации

Опр.

Конфигурация машины M определяется содержимым ленты, состоянием и положением головки. Конфигурация записывается словом вида $XqaY$, где

- $XaY \in \Sigma^*$ есть содержимое ленты,
- $q \in Q$ есть состояние M,
- головка обозревает символ a.

Функция, вычислимая машиной Тьюринга

Пусть $\Delta \subset \Sigma$ и $\# \notin \Delta$.

Опр.

M вычисляет частичную функцию $f : \Delta^* \to \Delta^*$, если для каждого $x \in \Delta^*$

- если $x \in dom(f)$, то начав работу в конфигурации $q_1\#x$, машина M останавливается в конфигурации $q_0\#f(x)$;
- если $x \notin dom(f)$, то машина M не останавливается.

Пример.

Машина M из примера (почти) вычисляет функцию $\mathsf{neg} : \{0,1\}^* \longrightarrow \{0,1\}^*$, заменяющую в данном слове 0 на 1 и 1 на 0. Чтобы вернуть головку в начало модифицируем M:

$$
\begin{array}{rcl}
q_1\# & \mapsto & q_1\#R \\
q_1 0 & \mapsto & q_2 1R \\
q_1 1 & \mapsto & q_2 0R \\
q_2 0 & \mapsto & q_2 1R \\
q_2 1 & \mapsto & q_2 0R \\
q_2\# & \mapsto & q_3\#L \\
q_3 0 & \mapsto & q_3 0L \\
q_3 1 & \mapsto & q_3 1L \\
q_3\# & \mapsto & q_3\#N
\end{array}
$$

Упражнения

Построить машины Тьюринга, вычисляющие следующие функции над алфавитом $\{0, 1\}$:

- $f(x) = xx$ (копирование слова)
- $g(x_1 \dots x_n) = \sum_{i=1}^{n} x_i \mod 2$ (сумма битов по модулю 2)

Программы, симулирующие машины Тьюринга. В интернете есть много хороших и разных. См., например, http://ironphoenix.org/tril/tm/