

Теорема Гёделя о неполноте
лекция 13

Лев Дмитриевич Беклемишев
<http://lpcs.math.msu.su/vml2010>

lbek1@yandex.ru

13.05.2010

Вычислимость и определимость

Опр.

Ограниченные формулы — все вхождения кванторов имеют вид

$$\forall x \leq t A(x) \equiv \forall x (x \leq t \rightarrow A(x)) \text{ или}$$

$$\exists x \leq t A(x) \equiv \exists x (x \leq t \wedge A(x)).$$

Δ_0 = множество ограниченных формул.

Опр.

Σ_1 -формулы имеют вид $\exists \vec{x} A(\vec{x}, \vec{a})$, где $A \in \Delta_0$.

Теорема об определимости

Опр.

Множество $P \subseteq \mathbb{N}^k$ Σ_1 -определимо в \mathbb{N} , если для некоторой формулы $A_P(a_1, \dots, a_k) \in \Sigma_1$

$$\langle x_1, \dots, x_k \rangle \in P \iff \mathbb{N} \models A_P[x_1, \dots, x_n].$$

Теорема.

$P \subseteq \mathbb{N}^k$ перечислимо $\iff P$ Σ_1 -определимо в \mathbb{N} .

Теорема.

Множество TA всех предложений A таких, что $\mathbb{N} \models A$, неперечислимо.

Доказательство.

Пусть $K \subseteq \mathbb{N}$ перечислимо и неразрешимо. По теореме об определимости найдётся формула $A_K(a)$ такая, что

$$n \in K \iff \mathbb{N} \models A_K(\bar{n}).$$

$$n \notin K \iff \mathbb{N} \not\models A_K(\bar{n}) \iff \mathbb{N} \models \neg A_K(\bar{n}).$$

Если TA перечислимо, то таково и $\{n \in \mathbb{N} : \mathbb{N} \models \neg A_K(\bar{n})\}$, т.к. по n эффективно восстанавливается формула $\neg A_K(\bar{n})$. Т.о. перечислимо дополнение K , что противоречит теореме Поста.

Теорема Гёделя

Теорема.

Если T эффективно аксиоматизируема и $\mathbb{N} \models T$, то найдётся предложение A такое, что $T \not\vdash A$ и $T \not\vdash \neg A$.

Доказательство.

В силу корректности $T \subseteq TA$, значит найдётся $A \in TA$ такое, что $T \not\vdash A$. Т.к. $\mathbb{N} \models \neg A$ имеем $T \not\vdash \neg A$.

Следствие.

PA неполна.

Следствие.

ZFC неполна, если она корректна.

Доказательство теоремы о Σ_1 -определимости

Идея: для каждой машины Тьюринга M надо выписать Σ_1 -формулу $T_M(\vec{x})$ выражающую тот факт, что на входе, кодирующем \vec{x} , машина M завершает работу. Это достигается путём кодирования машин Тьюринга и описания их вычислений на арифметическом языке.

Обогащение модели с помощью Δ_0 -определений

Пусть сигнатура модели M содержит арифметическую. Расширяем сигнатуру M новыми предикатными и функциональными символами.

- Определение предиката P такого, что

$$P(\vec{a}) \iff M \models A[\vec{a}],$$

где $A \in \Delta_0$.

Предложение.

Любая Δ_0 -формула расширенной сигнатуры эквивалентна некоторой Δ_0 -формуле сигнатуры M .

Доказательство.

Если $C \in \Delta_0(P)$, то $M \models (C \leftrightarrow C[P/A])$ и $C[P/A] \in \Delta_0$.

Δ_0 -определение функций

- Определение функции f

$$f(\vec{a}) = b \iff M \models F[\vec{a}, b],$$

где $F \in \Delta_0$,

$$M \models \forall \vec{x} \exists! y F(\vec{x}, y)$$

и для некоторого арифм. терма $t(\vec{a})$

$$M \models \forall \vec{x}, y (F(\vec{x}, y) \rightarrow y \leq t(\vec{x})).$$

Предложение.

Любая Δ_0 -формула A расширенной сигнатуры эквивалентна некоторой Δ_0 -формуле сигнатуры M .

Доказательство.

Индукция по построению A . Для атомарных формул применяем:

$s(f(\vec{q})) = s' \leftrightarrow \exists z \leq t(\vec{q}) (f(\vec{q}) = z \wedge s(z) = s')$,
где термы \vec{q} не содержат f .

Примеры

$$x \neq y \quad :\Leftrightarrow \quad \neg x = y$$

$$x < y \quad :\Leftrightarrow \quad x \leq y \wedge x \neq y$$

$$x \div y = z \quad :\Leftrightarrow \quad (y \leq x \wedge x = z + y) \vee (\neg y \leq x \wedge z = 0)$$

Двоичное разложение

Любое $x > 0$ однозначно представляется в виде

$$x = a_n \cdot 2^n + a_{n-1} \cdot 2^{n-1} + \dots + a_1 \cdot 2 + a_0,$$

где $a_0, \dots, a_n \in \{0, 1\}$ и $a_n \neq 0$.

Обозначения:

- $bit(x, i) \Leftrightarrow a_i$ есть $i + 1$ -й бит x ;
- $|x| \Leftrightarrow n$.

Кодирование двоичных слов

Слово $a_{n-1} \dots a_0$ кодируем числом $1a_{n-1} \dots a_0$ в двоичной записи. Пустое слово Λ кодируется числом 1 .

Замечание.

$|x|$ есть длина двоичной записи слова, кодируемого числом x .

$$\text{String}(x) \quad :\leftrightarrow \quad x \neq 0$$

$$|x| = y \quad :\leftrightarrow \quad (x = 0 \wedge y = 0) \vee (2^y \leq x \wedge x < 2^{y+1})$$

$$x * y = z \quad :\leftrightarrow \quad z = x \cdot 2^{|y|} + (y \div 2^{|y|})$$

Кодирование алфавита Σ

Пусть $\Sigma = \{C_0, \dots, C_n\}$.

Возьмём $c: 2^c \geq n + 2$.

Положим $\lceil C_i \rceil \Rightarrow 2^c + i$ для $0 \leq i \leq n$ и

$\lceil ; \rceil \Rightarrow 2^c + n + 1$ (разделитель).

$$\Sigma(x) :\Leftrightarrow x = \lceil C_0 \rceil \vee \dots \vee x = \lceil C_n \rceil$$

$$\text{Byte}(x) :\Leftrightarrow \text{String}(x) \wedge |x| = \bar{c}$$

Слова в алфавите Σ

Слово = последовательность байтов

Σ -слово = последовательность байтов из Σ

$$\mathit{Word}(x) \quad :\leftrightarrow \quad \mathit{String}(x) \wedge \exists k \leq x \ |x| = \bar{c} \cdot k$$

$$\|x\| = y \quad :\leftrightarrow \quad (\mathit{Word}(x) \wedge \bar{c} \cdot y = |x|) \vee (\neg \mathit{Word}(x) \wedge y = 0)$$

$$x \subseteq_w y \quad :\leftrightarrow \quad \mathit{Word}(x) \wedge \mathit{Word}(y) \wedge \\ \exists v, w \leq y \ (\mathit{Word}(v) \wedge y = v * x * w)$$

$$x \in_w y \quad \leftrightarrow \quad \mathit{Byte}(x) \wedge x \subseteq_w y$$

$$\mathit{Word}_\Sigma(x) \quad :\leftrightarrow \quad \mathit{Word}(x) \wedge \forall y \leq x \ (y \in_w x \rightarrow \Sigma(y))$$

Последовательности слов

Посл-ть $\langle w_1, \dots, w_s \rangle$ Σ -слов кодируем словом $w_1; w_2; \dots; w_s$, где $;$ — разделитель. Код пустой посл-ти $\langle \rangle$ есть 0 .

Замечание.

Для любого $w \in \Sigma^*$, $\lceil \langle w \rangle \rceil = \lceil w \rceil$, в частности, $\lceil \langle \Lambda \rangle \rceil = 1$.

$$\text{Seq}_\Sigma(x) \quad :\leftrightarrow \quad \text{Word}(x) \wedge \forall y \in_w x (\Sigma(y) \vee y = \ulcorner; \urcorner) \\ \vee x = 0$$

$$x; y = z \quad :\leftrightarrow \quad (x = 0 \wedge z = y) \vee (y = 0 \wedge z = x) \vee \\ (x \neq 0 \wedge y \neq 0 \wedge z = x * \ulcorner; \urcorner * y)$$

$$x \subseteq_s y \quad :\leftrightarrow \quad \text{Seq}_\Sigma(x) \wedge \text{Seq}_\Sigma(y) \wedge \\ \exists u, v \leq y (\text{Seq}_\Sigma(u) \wedge \text{Seq}_\Sigma(v) \wedge y = u; x; v)$$

$$x \in_s y \quad :\leftrightarrow \quad \text{Word}_\Sigma(x) \wedge x \subseteq_s y$$

Кодирование Машин Тьюринга

$\Sigma(x)$ рабочий алфавит

$Q(x)$ алфавит состояний

$\Gamma(x) \Rightarrow Q(x) \vee \Sigma(x)$

$P(x)$ множество команд

$Word_{\Sigma}(x)$ слово в рабочем алфавите

Конфигурации

$$\begin{aligned} \text{Config}(z) \quad :\Leftrightarrow \quad & \text{Word}_\Gamma(z) \wedge \exists u, v, q \leq z \\ & (\text{Word}_\Sigma(u) \wedge \text{Word}_\Sigma(v) \wedge Q(q) \wedge \\ & v \neq 1 \wedge z = u * q * v) \end{aligned}$$

(1 есть код пустого слова)

Переходы

$Step_M(x, y) :\leftrightarrow$

$Config(x) \wedge Config(y) \wedge$

$\exists u, v, p, q, a, b, c \subseteq_w x * y$

$[Word_\Sigma(u) \wedge Word_\Sigma(v) \wedge Q(p) \wedge Q(q) \wedge \Sigma(a) \wedge \Sigma(b) \wedge \Sigma(c) \wedge$

$[(x = u * p * a * v \wedge y = u * q * b * v \wedge P(p * a * q * b * \lceil N \rceil))$

$\vee (x = u * c * p * a * v \wedge y = u * q * c * b * v \wedge P(p * a * q * b * \lceil L \rceil))$

$\vee (x = p * a * v \wedge y = q * \lceil \# \rceil * b * v \wedge P(p * a * q * b * \lceil L \rceil))$

$\vee (x = u * p * a * v \wedge v \neq 1 \wedge y = u * b * q * v \wedge P(p * a * q * b * \lceil R \rceil))$

$\vee (x = u * p * a \wedge y = u * b * q * \lceil \# \rceil \wedge P(p * a * q * b * \lceil R \rceil))$

$]]$

$]]$

Вычисления

$$Init_M(x, z) \quad :\leftrightarrow \quad Config(z) \wedge z = \ulcorner q_1 \urcorner * \ulcorner \# \urcorner * x$$

$$Stop_M(z) \quad :\leftrightarrow \quad Config(z) \wedge \exists u, v \subseteq_w z (z = u * q_0 * v)$$

$$Comp_M(x, z) \quad :\leftrightarrow \quad Seq_{\Gamma}(z) \wedge \exists v \in_s z Stop_M(v) \wedge \forall u, v, w \leq z \\ (z = u; v; w \wedge Word_{\Gamma}(v) \rightarrow \\ (Init_M(x, v) \vee \exists y \in_s u Step_M(y, v)))$$

Кодирование входа

Пусть Σ содержит $1, \$$.

$code(n) \Rightarrow 1 \dots 1$ (n раз)

$$code(x) = y \quad :\Leftrightarrow \quad Word(y) \wedge \|y\| = x \wedge \\ \forall y \in_w x \quad y = \ulcorner 1 \urcorner$$

Предикат остановки

$T_M(a_1, \dots, a_n) :\leftrightarrow$

$\exists z \text{ Comp}_M(\text{code}(a_1) \$ \dots \$ \text{code}(a_n), z)$

Имеем:

$$\mathbb{N} \models T_M[x_1, \dots, x_n] \iff !M(x_1, \dots, x_n).$$