

Вычислимость

лекция 12

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

`lbek1@yandex.ru`

29.04.2010

Установленные факты

- Универсальная вычислимая функция $F(e, x)$.
- Частичная вычислимая $f : \mathbb{N} \rightarrow \{0, 1\}$, не продолжаемая до тотальной вычислимой:

$$f(x) \equiv \begin{cases} 1, & \text{если } F(x, x) = 0; \\ 0, & \text{если } !F(x, x) \neq 0; \\ \text{неопр.}, & \text{иначе.} \end{cases}$$

- $K \equiv \{x \in \mathbb{N} : !F(x, x)\}$ перечислимое, неразрешимое.

Установленные факты

- Универсальная вычислимая функция $F(e, x)$.
- Частичная вычислимая $f : \mathbb{N} \rightarrow \{0, 1\}$, не продолжаемая до тотальной вычислимой:

$$f(x) \Rightarrow \begin{cases} 1, & \text{если } F(x, x) = 0; \\ 0, & \text{если } !F(x, x) \neq 0; \\ \text{неопр.}, & \text{иначе.} \end{cases}$$

- $K \Rightarrow \{x \in \mathbb{N} : !F(x, x)\}$ перечислимое, неразрешимое.

Установленные факты

- Универсальная вычислимая функция $F(e, x)$.
- Частичная вычислимая $f : \mathbb{N} \rightarrow \{0, 1\}$, не продолжаемая до тотальной вычислимой:

$$f(x) \Rightarrow \begin{cases} 1, & \text{если } F(x, x) = 0; \\ 0, & \text{если } !F(x, x) \neq 0; \\ \text{неопр.}, & \text{иначе.} \end{cases}$$

- $K \Rightarrow \{x \in \mathbb{N} : !F(x, x)\}$ перечислимое, неразрешимое.

Пара неотделимых перечеислимых множеств

Опр.

Пара множеств $X, Y \subseteq \mathbb{N}$ *неотделима*, если

- $X \cap Y = \emptyset$
- не существует *разрешимого* множества $C \subseteq \mathbb{N}$ такого, что $X \subseteq C$ и $Y \cap C = \emptyset$.

Теорема.

Существует неотделимая пара перечеислимых
множеств.

Доказательство.

Пусть $f : \mathbb{N} \rightarrow \{0, 1\}$ — вычислимая функция без тотального вычислимого продолжения. Положим $X \Rightarrow \{x \in \mathbb{N} : f(x) = 0\}$ и $Y \Rightarrow \{x \in \mathbb{N} : f(x) = 1\}$.

По теореме о графике X, Y перечислимы.

Если разрешимое C отделяет X и Y , то функция

$$g(x) \Rightarrow \begin{cases} 0, & \text{если } x \in C; \\ 1, & \text{иначе.} \end{cases}$$

продолжает f на всё \mathbb{N} .

Главные универсальные функции

Опр.

Вычислимая универсальная функция $F : \mathbb{N}^2 \rightarrow \mathbb{N}$ называется *главной*, если для любой вычислимой $g : \mathbb{N}^2 \rightarrow \mathbb{N}$ найдётся тотальная вычислимая функция $s : \mathbb{N} \rightarrow \mathbb{N}$ такая, что

$$\forall e, x \ g(e, x) \simeq F(s(e), x).$$

Теорема.

Вычислимая универсальная функция $F : \mathbb{N}^2 \rightarrow \mathbb{N}$, построенная по универсальной машине Тьюринга U , является главной.

Замечание.

Вычислимую функцию $g(e, x)$ можно понимать как (возможно, не универсальный) язык программирования, где e — программа вычисления функции $x \mapsto g(e, x)$.

Функция s есть *интерпретатор*, сопоставляющий программе e языка g машину Тьюринга $s(e)$, вычисляющую ту же функцию.

Доказательство.

Пусть $\Delta = \{1\}$ и МТ M вычисляет $\underline{g(e, x)}$ в унарной записи, то есть $M_\Delta(\langle e, x \rangle) \simeq \underline{g(e, x)}$.

Сопоставим МТ M машину $\underline{M[n]}$, которая для данного входа \bar{x} вычисляет $\langle n, x \rangle$, а далее работает как M . Преобразование $n \mapsto \text{Code}(M[n])$ является тотальной вычислимой функцией.

Имеем

$$M_{\Delta}(\overline{\langle e, x \rangle}) \simeq M[e]_{\Delta}(\bar{x}) \simeq U_{\Delta}(\text{Code}(M[e])\bar{x}).$$

Вспомним, что $F(i, n) \rightleftharpoons |U_{\Delta}(\text{word}_{\Pi}(i)\bar{n})|$.

Отсюда $g(e, x) \simeq F(s(e), x)$, где

$$s(e) = \text{word}_{\Pi}^{-1}(\text{Code}(M[e])).$$

Теорема Райса–Успенского

Какие свойства вычислимых функций распознаваемы по программе?

Примеры практически интересных свойств частичных функций f :

- $\forall x !f(x)$ (тотальность);
- $f(x_0) = y_0$, где x_0, y_0 фиксированы;
- $f = g_0$, где функция g_0 фиксирована;
- «вычисление $f(x)$ на некотором x приводит к стиранию всех данных на HD компьютера».

Опр.

Пусть фиксирована универсальная вычислимая функция F . Обозначим через φ_e частичную функцию с индексом e , т.е. $\varphi_e(x) \simeq F(e, x)$.

Опр.

Нетривиальным свойством вычислимых функций называем любое подмножество $\mathcal{C} \subset \text{Com}(\mathbb{N}, \mathbb{N})$ такое, что $\mathcal{C} \neq \emptyset$ и $\mathcal{C} \neq \text{Com}(\mathbb{N}, \mathbb{N})$.

С каждым свойством \mathcal{C} вычислимых функций связывается множество всех программ, вычисляющих функции со свойством \mathcal{C} , то есть множество $I_{\mathcal{C}} \equiv \{e \in \mathbb{N} : \varphi_e \in \mathcal{C}\}$.

Теорема.

Если \mathcal{C} — нетривиальное свойство вычислимых функций, то множество $\{e \in \mathbb{N} : \varphi_e \in \mathcal{C}\}$ неразрешимо.

Доказательство.

- Можно считать, что нигде не определённая функция ζ не обладает свойством \mathcal{C} — иначе заменим \mathcal{C} на его дополнение.
- Т.к. $\mathcal{C} \neq \emptyset$, фиксируем вычислимую функцию $g_0 \in \mathcal{C}$.

- Построим тотальную вычислимую функцию $f : \mathbb{N} \rightarrow \mathbb{N}$ такую, что для всех $x \in \mathbb{N}$

$$x \in K \iff f(x) \in I_c.$$

- Если бы $I_c \equiv \{e \in \mathbb{N} : \varphi_e \in \mathcal{C}\}$ было разрешимо, то мы получили бы следующий разрешающий алгоритм для K : для данного x вычислить $y = f(x)$ и проверить $y \in I_c$.

Вычисляем $g(e, x)$ в соответствии со следующим алгоритмом:

- вычислить $\varphi_e(e)$;
- если $!\varphi_e(e)$, очистить ленту, а затем вычислить $g_0(x)$.

По свойству главности получаем тотальную вычислимую функцию f такую, что

$$\forall e, x \varphi_{f(e)}(x) \simeq g(e, x).$$

Тогда имеем:

- Если $e \in K$, то $\varphi_{f(e)}(x) \simeq g_0(x)$;
- Если $e \notin K$, то $\varphi_{f(e)} = \zeta$.

Отсюда $e \in K \iff \varphi_{f(e)} \in \mathcal{C} \iff f(e) \in I_{\mathcal{C}}$.

Следствие.

Следующие свойства вычислимых функций не распознаваемы по программе:

- тотальность,
- ограниченность,
- конечность области определения, и т.д.

Замечание.

Такие свойства как

- «вычисление $f(0)$ завершается менее, чем за 100 шагов»;
- «программа f содержит менее 100 символов» (при фиксированном алфавите)

являются разрешимыми свойствами программ.

Они не соответствуют никакому классу частичных функций.

Теоремы Гёделя о неполноте



Арифметика Пеано PA

Сигнатура: $0, S, +, \cdot, \text{exp}, \leq, =$

Стандартная модель: $(\mathbb{N}; 0, S, +, \cdot, \text{exp}, \leq, =)$, где $S(x) = x + 1$ и $\text{exp}(x) = 2^x$.

Аксиомы PA

1 $\neg S(a) = 0, \quad S(a) = S(b) \rightarrow a = b,$

2 $a + 0 = a, \quad a + S(b) = S(a + b),$

3 $a \cdot 0 = 0, \quad a \cdot S(b) = a \cdot b + a,$

4 $\exp(0) = S(0), \quad \exp(S(a)) = \exp(a) + \exp(a),$

5 $a \leq 0 \leftrightarrow a = 0,$

6 $a \leq S(b) \leftrightarrow (a \leq b \vee a = S(b)),$

7 (Схема аксиом индукции)

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

для любой формулы A .

Арифметика Робинсона

Опр.

Теория Q получается из PA заменой схемы индукции единственной аксиомой:

$$a \leq b \vee b \leq a.$$

Упражнение

Показать, что $PA \vdash Q$.

Решение

(1) Сначала покажем индукцией по x , что
 $\forall x (a \leq x \leftrightarrow a = x \vee S(a) \leq x)$.

(2) Затем покажем индукцией по x , что
 $\forall x (a \leq x \vee x \leq a)$.

Заметим, что из (1) следует $a \leq a$ и $a \leq S(a)$.

Вывод (1)

Базис: $a \leq 0 \leftrightarrow a = 0 \vee S(a) \leq 0$. Поскольку $S(a) \leq 0 \rightarrow S(a) = 0$, имеем $\neg S(a) \leq 0$.

Шаг: эквивалентно преобразуем

- 1 $a \leq S(x)$
- 2 $a \leq x \vee a = S(x)$ (аксиома)
- 3 $(a = x \vee S(a) \leq x) \vee a = S(x)$ (пр. инд.)
- 4 $S(a) = S(x) \vee S(a) \leq x \vee a = S(x)$ (аксиома)
- 5 $S(a) \leq S(x) \vee a = S(x)$

Вывод (1)

Базис: $a \leq 0 \leftrightarrow a = 0 \vee S(a) \leq 0$. Поскольку $S(a) \leq 0 \rightarrow S(a) = 0$, имеем $\neg S(a) \leq 0$.

Шаг: эквивалентно преобразуем

- 1 $a \leq S(x)$
- 2 $a \leq x \vee a = S(x)$ (аксиома)
- 3 $(a = x \vee S(a) \leq x) \vee a = S(x)$ (пр. инд.)
- 4 $S(a) = S(x) \vee S(a) \leq x \vee a = S(x)$ (аксиома)
- 5 $S(a) \leq S(x) \vee a = S(x)$

Вывод (2)

Базис: $a \leq 0 \vee 0 \leq a$ поскольку $0 \leq a$.

Шаг:

- 1 $a \leq x \vee x \leq a$ (пр. инд.)
- 2 $x \leq a \rightarrow (a = x \vee S(x) \leq a)$ (1)
- 3 $a \leq x \vee a = x \vee S(x) \leq a$
- 4 $a \leq x \rightarrow a \leq S(x)$ (аксиома)
- 5 $a = x \rightarrow a \leq S(x)$ (из (1))
- 6 $a \leq S(x) \vee S(x) \leq a$

Первая теорема Гёделя о неполноте

Теорема.

Если теория T

- в арифметическом языке,
- эффективно аксиоматизируема,
- $\mathbb{N} \models T$,

то T неполна, то есть существует предложение A такое, что $T \not\vdash A$ и $T \not\vdash \neg A$.

Следствие.

PA неполна.

Теорема Гёделя–Россера

Теорема.

Если

- теория T содержит Q ,
- T эффективно аксиоматизируема,
- T непротиворечива,

то T неполна.

Замечание.

Теорема Гёделя–Россера применима к теориям в произвольном языке, которые содержат Q в смысле интерпретируемости.

Следствие.

ZFC неполна.

Вторая теорема Гёделя о неполноте

Теорема.

Если

- T содержит PA ,
- T эффективно аксиоматизируема,
- T непротиворечива,

то $T \not\vdash \text{Con}(T)$, где $\text{Con}(T)$ – арифметическая формула, выражающая непротиворечивость T .