Вычислимость
лекция 11

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

lbekl@yandex.ru

22.04.2009

Теорема Поста

Теорема.

$A \subseteq \mathbb{N}$ *разрешимо* $\iff$ A *и* $\mathbb{N} \setminus A$ *перечислимы.*

Доказательство.

Пусть определённые всюду функции f и g перечисляют A и $\mathbb{N} \setminus A$, соответственно. Вычисляем $f(0), g(0), f(1), g(1), f(2), g(2), \ldots$ до тех пор, пока не встретим данный нам x.

Теорема о графике

Теорема.

$f : \mathbb{N} \to \mathbb{N}$ *вычислима* $\iff$ *множество* $G_f \rightleftharpoons \{\langle x, y\rangle : f(x) = y\}$ *перечислимо.*

Доказательство.

$(\Rightarrow)$ Проверяем $\langle x, y\rangle \in G_f$ вычисляя $f(x)$.

$(\Leftarrow)$ Вычисляем $f(x)$ перебирая все возможные пары $\langle x, y\rangle$ и проверяя их на принадлежность G_f.

Разрешимость и перечислимость теорий

Опр.

Теория T (в конечной сигнатуре) *эффективно аксиоматизируема* $\iff$ множество аксиом T разрешимо.

Опр.

Теория T *разрешима*, если множество теорем T разрешимо.

Теорема.

Теория T эфф. аксиоматизируема $\iff$ множество теорем T перечислимо.

Доказательство.

$(\Rightarrow)$ Порождаем все возможные выводы из аксиом T.

$(\Leftarrow)$ Пусть $A_0, A_1, \ldots, A_n, \ldots$ — перечисление теорем T. Тогда множество формул A_0, $A_0 \wedge A_1$, $A_0 \wedge A_1 \wedge A_2, \ldots$ разрешимо и задаёт эквивалентную теорию.

Теорема.

Полная эфф. аксиоматизируемая теория разрешима.

Полные эфф. аксиоматизируемые теории:

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

Кодирование машин Тьюринга

Опр.

Машина $M = \langle Q, \Sigma, P, q_0, q_1 \rangle$ задаётся

- $Q = \{q_0, \ldots, q_s\}$ — внутр. состояния;
- $\Sigma = \{a_0, \ldots, a_r\}$ — рабочий алфавит;
- $P = \{p_0, \ldots, p_{s(r+1)}\}$ — набор команд.

q_1 — нач., q_0 — кон., $a_0 = \#$ — пробел.

Кодирование Q и Σ

Опр.

Алфавит программ есть $\Pi \rightleftharpoons \{\rightarrow, L, N, R, q, a, \mathbf{1}\}$.

Сопоставим элементам Q и Σ следующие коды в алфавите Π: $q_i \longmapsto q\mathbf{1}^i$; $\quad a_j \longmapsto a\mathbf{1}^j$.

Опр.

Слово $x \in \Sigma^*$ кодируется конкатенацией $Code(x)$ кодов всех его букв, например $Code(a_2 a_0 a_1) = a\mathbf{11}aa\mathbf{1}$.

Коды команд

Опр.

Код команды $q_i a_k \to q_j a_l \nu$, где $\nu \in \{L, N, R\}$, есть слово $q\mathbf{1}^i a\mathbf{1}^k \to q\mathbf{1}^j a\mathbf{1}^l \nu$ в алфавите Π.

Код команды $p \in P$ обозначим $Code(p)$.

Коды машин

Опр.

Код машины M есть конкатенация кодов всех её команд, то есть $Code(M) \rightleftharpoons Code(p_0) \ldots Code(p_{s(r+1)})$.

Утверждение.

Отображение $M \longmapsto Code(M)$ инъективно.

В частности, по $Code(M)$ однозначно восстанавливаются рабочий алфавит, множество внутренних состояний, команды и т.д.

Утверждение.

Множество кодов всевозможных машин Тьюринга (выбранного нами формата) есть разрешимое подмножество Π^*.

Функция, вычислимая машиной Тьюринга

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

Опр.

M чисто 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.

Опр.

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

- если $x \notin dom(f)$, то начав работу в конфигурации $q_1\#x$, машина M не останавливается;
- если $x \in dom(f)$, то машина M останавливается, на ленте написано слово $y = f(x)$, слева и справа от него стоят символы не из Δ^*, а головка остановилась внутри или непосредственно перед y.

Обозначения

Опр.

$M_\Delta(x)$ есть результат работы M на слове $x \in \Delta^*$.

Опр.

$M_\Delta : \Delta^* \to \Delta^*$ — частичная функция, вычислимая M.

Замечание.

M_Δ определена для любой машины M с рабочим алфавитом $\Sigma \supset \Delta$.

Утверждение.

Для любой МТ M и Δ можно указать машину M' вычисляющую функцию M_Δ чисто.

- Преобразуем M так, чтобы M не печатала $\#$ (добавив «двойник» пробела).
- Добавим к программе M инструкции, определяющие по завершении работы M слово $M_\Delta(x)$ и удаляющие весь мусор слева и справа до символов $\#$.

Универсальная машина Тьюринга

Опр.

Универсальная машина U_Δ с рабочим алфавитом, содержащим $\Pi \cup \Delta \cup \{\$\}$, для любой МТ M и слова $x \in \Delta^*$ (чисто) вычисляет результат работы машины M на входе x, то есть частичную функцию

$$Code(M)\$x \longmapsto M_\Delta(x).$$

Другими словами:

- Если U_Δ начинает работу в конфигурации $q_1\#Code(M)\$x$ для $x \in \Delta^*$, то заключительная конфигурация $q_0\#M_\Delta(x)$;
- Иначе U_Δ зацикливается.

Алгоритм работы машины U_Δ:

- Читаем входное слово вплоть до первого пробела и проверяем, что оно имеет вид $Code(M)\$x$ для $x \in \Delta^*$. Если нет, зацикливаемся.
- Эмулируем работу M на входе x, пользуясь частью ленты справа от $\$$ для записи кодов конфигураций M.

- В случае завершения работы M на входе x с результатом y выделяем слово $Code(y)$ из кода заключительной конфигурации M.
- Преобразуем $Code(y)$ в y.

Универсальные функции

Опр.
$\mathrm{Com}(X, Y)$ есть множество всех частичных вычислимых функций из X в Y.

Опр.
$\mathrm{TCom}(X, Y)$ есть множество всех тотальных (всюду определённых) вычислимых функций из X в Y.

Условное равенство

Пусть f, g — частичные функции.

Опр.

$f(x) \simeq g(x)$ означает, что $dom(f) = dom(g)$ и $\forall x{\in}dom(f)\ f(x) = g(x)$.

Пример.

$x \cdot 1/x \simeq 1/x \cdot x$.

Пример.

$U_\Delta(Code(M)\$x) \simeq M_\Delta(x)$.

Пусть $\mathcal{F}$ — счётное семейство част. функций $f : X \to Y$, например $\mathcal{F} = \mathrm{Com}(\mathbb{N}, \mathbb{N})$.

Опр.

Универсальной функцией для $\mathcal{F}$ называем такую функцию $F : \mathbb{N} \times X \to Y$, что

- Для любого $e \in \mathbb{N}$ функция $f(x) \rightleftharpoons F(e, x)$ принадлежит $\mathcal{F}$.
- $\forall f{\in}\mathcal{F}\ \exists e{\in}\mathbb{N}\ \forall x{\in}X\ \ f(x) \simeq F(e, x)$.

Замечание.

- Универсальная функция F существует для любого счётного семейства $\mathcal{F}$.
- F определяет некоторую нумерацию $\mathcal{F}$: $\mathcal{F} = \{f_0(x), f_1(x), \dots\}$, где $f_i(x) \rightleftharpoons F(i, x)$.

Опр.

Число i называется *индексом* функции f_i относительно данной универсальной функции F.

Теорема.

Семейство $\mathrm{Com}(\mathbb{N}, \mathbb{N})$ *обладает* *вычислимой универсальной функцией* $F \in \mathrm{Com}(\mathbb{N} \times \mathbb{N}, \mathbb{N})$.

Доказательство.

Пусть $\Delta = \{1\}$. Обозначим $\overline{n} \rightleftharpoons 11\ldots1$ (n раз). Заметим, что $|\overline{n}| = n$.

$f : \mathbb{N} \to \mathbb{N}$ вычислима $\iff$ вычислима функция $\overline{f} : \Delta^* \to \Delta^*$, определяемая по формуле $\overline{f}(\overline{n}) \rightleftharpoons \overline{f(n)}$.

Пусть M вычисляет $\overline{f}$, то есть

$$\forall x \in \Delta^* \ M_\Delta(x) \simeq \overline{f}(x).$$

Рассмотрим выч. биекцию $\mathrm{word}_\Pi : \mathbb{N} \to \Pi^*$. Для некоторого $i \in \mathbb{N}$ имеем $Code(M) = \mathrm{word}_\Pi(i)$. Значит, для всех $x \in \Delta^*$

$$\overline{f}(x) \simeq M_\Delta(x) \simeq U_\Delta(\mathrm{word}_\Pi(i)\$x).$$

В качестве универсальной функции $F : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ возьмём

$$F(i, n) \rightleftharpoons |U_{\Delta}(\mathrm{word}_{\Pi}(i)\$\overline{n})|.$$

Замечание.
Аналогично, для каждого k строятся вычислимые универсальные функции для классов $\mathrm{Com}(\mathbb{N}^k, \mathbb{N})$, обозначаемые F^k.

Вычислимая функция, не продолжаемая до вычислимой тотальной

Пусть $f, g : X \to Y$ — частичные функции.

Опр.

g *продолжает* f, если $f \subseteq g$, то есть

$dom(f) \subseteq dom(g)$ и $\forall x{\in}dom(f)\; f(x) = g(x)$.

Теорема.

Найдётся такая $f \in \mathrm{Com}(\mathbb{N}, \mathbb{N})$, *что никакая* $g \in \mathrm{TCom}(\mathbb{N}, \mathbb{N})$ *не продолжает* f.

Доказательство.

Диагональный метод Кантора.

Пусть $f(x) \simeq F(x, x) + 1$, где F — универсальная функция.

Функция f вычислима, т.к. такова F.

Допустим $f \subseteq g$ и $g \in \mathrm{TCom}(\mathbb{N}, \mathbb{N})$. Тогда найдётся $i \in \mathbb{N}$

$$\forall x{\in}\mathbb{N}\; g(x) \simeq F(i, x).$$

Т.к. $!g(i)$, получаем

$$F(i, i) = g(i) = F(i, i) + 1,$$

противоречие.

Упражнение

Построить вычислимую функцию $f : \mathbb{N} \to \{0, 1\}$*, не имеющую тотального вычислимого продолжения.*

Перечислимое неразрешимое множество

Положим $K \rightleftharpoons dom(f)$, где f из предыдущей теоремы, т.е. $K = \{x \in \mathbb{N} : !F(x, x)\}$.

Теорема.

$K \subseteq \mathbb{N}$ *перечислимо, но не разрешимо.*

Доказательство.

K перечислимо, поскольку K есть область определения вычислимой функции f.

Допустим K разрешимо. Тогда функция

$$g(x) \rightleftharpoons \begin{cases} f(x), & \text{если } x \in K; \\ 0, & \text{иначе.} \end{cases}$$

вычислима и является продолжением f на всё $\mathbb{N}$.

Проблема остановки

Проблема = массовая проблема

Пусть фиксирован алфавит Δ и $\# \notin \Delta$.

Задача: по данной программе (коду машины Тьюринга) M и исходным данным $x \in \Delta^*$ узнать, завершает ли работу M на входе x.

Теорема.

Проблема остановки алгоритмически неразрешима.

Доказательство.

В случае разрешимости проблемы остановки мы могли бы построить разрешающий алг. для K:

- По данному x вычислить $y = \mathrm{word}_\Pi(x)$.
- Проверить, является ли y кодом МТ с алфавитом, содержащим Δ. Если нет, то $x \notin K$.
- Иначе проверить, завершает ли работу машина M с кодом y на входе $\overline{x}$. Если да, то $x \in K$, иначе $x \notin K$.