Вычислимость
лекция 10

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

lbekl@yandex.ru

16.04.2009

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.

Опр.

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

Пример.

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

$$\begin{array}{rcl@{\qquad}rcl} q_1\# & \mapsto & q_1\#R & q_20 & \mapsto & q_21R \\ q_10 & \mapsto & q_11R & q_21 & \mapsto & q_20R \\ q_11 & \mapsto & q_10R & q_2\# & \mapsto & q_0\#L \end{array}$$

Конфигурации

Предположение: лента содержит лишь конечное число символов, отличных от $\#$.

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 $\mathrm{neg} : \{0,1\}^* \longrightarrow \{0,1\}^*$, заменяющую в данном слове 0 на 1 и 1 на 0. Чтобы вернуть головку в начало модифицируем M:

$$
\begin{aligned}
q_1\# &\mapsto q_1\#R \\
q_10 &\mapsto q_21R \\
q_11 &\mapsto q_20R \\
q_20 &\mapsto q_21R \\
q_21 &\mapsto q_20R \\
q_2\# &\mapsto q_3\#L \\
q_30 &\mapsto q_30L \\
q_31 &\mapsto q_31L \\
q_3\# &\mapsto q_0\#N
\end{aligned}
$$

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)

Вычислимые функции $\mathbb{N}^k \to \mathbb{N}$

Для $f : \mathbb{N}^k \to \mathbb{N}$ определим $\bar{f} : \{0,1\}^* \to \{0,1\}^*$:

$\bar{f}(x) = y$, если $x = 1^{n_1}0 \ldots 01^{n_k}$ и $y = 1^m$ для некоторых $n_1, \ldots, n_k, m \in \mathbb{N}$ и $f(n_1, \ldots, n_k) = m$.

Опр.

$f : \mathbb{N}^k \to \mathbb{N}$ вычислима по Тьюрингу, если вычислима $\bar{f} : \{0,1\}^* \to \{0,1\}^*$.

Вычислимые функции $\mathbb{N}^k \to \mathbb{N}$

Для $f : \mathbb{N}^k \to \mathbb{N}$ определим $\bar{f} : \{0,1\}^* \to \{0,1\}^*$:

$\bar{f}(x) = y$, если $x = 1^{n_1}0 \ldots 01^{n_k}$ и $y = 1^m$ для некоторых $n_1, \ldots, n_k, m \in \mathbb{N}$ и $f(n_1, \ldots, n_k) = m$.

Опр.

$f : \mathbb{N}^k \to \mathbb{N}$ вычислима по Тьюрингу, если вычислима $\bar{f} : \{0,1\}^* \to \{0,1\}^*$.

Примеры

- Арифметические операции $+$ и $\times$ вычислимы.
- Композиция вычислимых функций вычислима.
- Многочлены с натуральными коэффициентами вычислимы.

Вычислимые биекции

Утверждение.

Существует вычислимая биекция $\mathbb{N} \times \mathbb{N} \leftrightarrow \mathbb{N}$.

Канторовский пересчёт пар: $\langle 0,0\rangle$, $\langle 0,1\rangle$, $\langle 1,0\rangle$, $\langle 2,0\rangle$, $\langle 1,1\rangle$, $\langle 0,2\rangle$, $\ldots$

$c(x,y) :=$ номер пары $\langle x,y\rangle$

Подсчёт

Лемма.

$c(x, y) = \frac{1}{2}(x + y)(x + y + 1) + x$

Доказательство.

$c(x, y) = n + x$, где $n = 1 + 2 + \cdots + (x + y - 1)$

Обратные функции

Из биективности c однозначно определены функции l, r такие что $c(l(x), r(x)) = x$ для всех $x \in \mathbb{N}$.

Также имеем $l(c(x, y)) = x, \quad r(c(x, y)) = y$.

Почему функции l и r вычислимы?

Кодирование кортежей длины n

Определим по индукции вычислимые биективные функции $c_n : \mathbb{N}^n \to \mathbb{N}$ для $n \geq 2$:

$$\begin{aligned} c_2(x_1, x_2) &:= c(x_1, x_2) \\ c_{n+1}(x_1, \ldots, x_{n+1}) &:= c(c_n(x_1, \ldots, x_n), x_{n+1}) \end{aligned}$$

Обратные функции π_i^n определяются равенствами: $c_n(\pi_1^n(x), \ldots, \pi_n^n(x)) = x$ для всех $x \in \mathbb{N}$.

Кодирование кортежей конечной длины

Утверждение.

Существует вычислимая биекция $C : \mathbb{N}^{<\omega} \to \mathbb{N}$.

$C(\langle x_1, \ldots, x_n \rangle) := c(n, c_n(x_1, \ldots, x_n))$.

В каком смысле можно говорить о вычислимости функции C?

Кодирование слов в алфавите Σ

Утверждение.

Для любого непустого алфавита Σ *существует вычислимая биекция* $\Sigma^* \leftrightarrow \mathbb{N}$.

Доказательство.

Пусть $\Sigma = \{0, \ldots, m-1\}$ и $m \geq 2$.
Сопоставим $\Lambda \mapsto 0$ и

$$a_1 a_2 \ldots a_n \longmapsto \sum_{i=1}^{n} (a_i + 1) m^{n-i}$$

Утверждение.

Всякое $x > 0$ *однозначно представляется в виде*

$$x = (a_0 + 1) + (a_1 + 1)m + \cdots + (a_n + 1)m^n,$$

где $0 \leq a_i < m$ *для всех* i.

Доказательство.

$$x = \sum_{i=1}^{n} (a_i + 1)m^{n-i} = \sum_{i=1}^{n} a_i m^{n-i} + \sum_{i=1}^{n} m^i$$

$$= \sum_{i=1}^{n} a_i m^{n-i} + \frac{m^{n+1} - 1}{m - 1}$$

Решение относительно $a_1, \ldots, a_n$ существует и единственно, если

$$0 \leq x - \frac{m^{n+1} - 1}{m - 1} < m^{n+1}.$$

Это равносильно

$$\frac{m^{n+1} - 1}{m - 1} \leq x < \frac{m^{n+1} - 1}{m - 1} + m^{n+1} = \frac{m^{n+2} - 1}{m - 1}.$$

Разрешимые множества

Опр.

Множество $A \subseteq \mathbb{N}^k$ разрешимо, если вычислима характеристическая функция $\chi_A : \mathbb{N}^k \to \{0, 1\}$, где

$$\chi_A(x) = \begin{cases} 1, & \text{если } x \in A \\ 0, & \text{иначе.} \end{cases}$$

Примеры

Разрешимы:

- множества $\varnothing$, $\mathbb{N}$;
- конечные множества;
- множество чётных чисел;
- множество простых чисел;
- $\{\langle m, n\rangle : m \text{ и } n \text{ взаимно просты}\}$;

...

Свойства замкнутости

Утверждение.

Класс разрешимых подмножеств $\mathbb{N}$ *замкнут относительно булевых операций* $\cap$, $\cup$, $\setminus$.

Разрешимые подмножества $\mathbb{N}$ образуют булеву алгебру.

Перечислимые множества

Опр.

Частичной характеристической функцией $A \subseteq \mathbb{N}^k$ называем $\chi_A^* : \mathbb{N}^k \to \{0, 1\}$, где

$$\chi_A^*(x) = \begin{cases} 1, & \text{если } x \in A; \\ \text{не определено}, & \text{иначе.} \end{cases}$$

Теорема.

Для любого $A \subseteq \mathbb{N}$ *следующие утв. равносильны:*

1. *функция* χ_A^* *вычислима;*
2. $A = \mathrm{dom}(f)$ *для некоторой вычислимой* f*;*
3. $A = \mathrm{rng}(f)$ *для некоторой вычислимой* f*;*
4. $A = \varnothing$ *или* $A = \mathrm{rng}(f)$ *для некоторой вычислимой* f *такой что* $\mathrm{dom}(f) = \mathbb{N}$*;*
5. $A = \{x : \exists y \, \langle x, y \rangle \in B\}$ *для некоторого разрешимого* $B \subseteq \mathbb{N} \times \mathbb{N}$*.*

Доказательство

Утверждения $1 \Rightarrow 2$ и $4 \Rightarrow 3$ очевидны.

$1 \Rightarrow 5$:
Пусть машина M_f вычисляет f. Рассмотрим

$$B \rightleftharpoons \{\langle x, y\rangle : M_f \text{ на входе } x \text{ ост. за } y \text{ шагов}\}.$$

Тогда $x \in \mathrm{dom}(f) \iff \exists y\, \langle x, y\rangle \in B$ и
B разрешимо.

$5 \Rightarrow 4$:

Допустим $A \neq \varnothing$, выберем $a_0 \in A$.

Определим $f : \mathbb{N} \to \mathbb{N}$ так:

$$f(x) \rightleftharpoons \begin{cases} l(x), & \text{если } \langle l(x), r(x) \rangle \in B \\ a_0, & \text{иначе.} \end{cases}$$

$3 \Rightarrow 1$:
Пусть M_f вычисляет f. Вычисляем $\chi^*_A(x)$ для данного x:

Для каждого $n = 0, 1, 2, \ldots$ выполним:

- сопоставим n пару $l = l(n)$ и $r = r(n)$;
- проделаем r шагов вычисления M_f на входе l;
- если получен результат $y = x$, то выдаем ответ 1 и останавливаемся (иначе рассматриваем следующее n).

Свойства перечислимых множеств

Опр.

Множество A, удовлетворяющее любому из пунктов доказанной теоремы, называется *перечислимым*.

- Всякое разрешимое множество перечислимо.
- Класс перечислимых подмножеств $\mathbb{N}$ замкнут относительно операций $\cap$, $\cup$.

Диофантовы уравнения

Пусть $P(x_1, \ldots, x_n)$ – многочлен с целыми коэффициентами.

Утверждение.

Множество всех решений уравнения $P(x_1, \ldots, x_n) = 0$ *в натуральных числах разрешимо (как подмножество* $\mathbb{N}^n$*).*

Диофантовы множества

Опр.

Множество вида
$\{m \in \mathbb{N} : P(m, x_1, \ldots, x_n) = 0$ имеет решение в $\mathbb{N}\}$
называется *диофантовым*.

Утверждение.

Всякое диофантово множество перечислимо.

Теорема Матиясевича

Теорема.

Всякое перечислимое множество диофантово.

Из этой теоремы вытекает решение 10-й проблемы Гильберта:

Следствие.

Множество всех диофантовых уравнений $P(x_1, \ldots, x_n) = 0$, которые имеют решение в $\mathbb{N}$, неразрешимо.

Доказательство: возьмем диофантово представление перечислимого неразрешимого множества.