

Логика и алгоритмы, лекция 26

лектор: Кудинов Андрей Валерьевич

1 июня 2021 г.

План лекции:

- Универсальная машина Тьюринга
- Главность универсальной МТ
- m -сводимость и m -полнота
- Теорема Клини о неподвижной точке
- Арифметика Пеано

Кодирование машин Тьюринга

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

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

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

$$P : \underbrace{Q \setminus \{q_0\}} \times \Sigma \rightarrow \dots$$

Кодирование Q и Σ

Алфавит программ есть $\Pi := \{\rightarrow, \underline{L}, \underline{N}, \underline{R}, q, a, \underline{1}\}$.

Сопоставим элементам Q и Σ следующие коды в алфавите Π :

$$\text{Code } q_i \mapsto \underline{q1^i}; \quad \text{Code } a_j \mapsto \underline{a1^j}.$$

Слово $x \in \Sigma^*$ кодируется конкатенацией $\text{Code}(x)$ кодов всех его букв, например $\text{Code}(a_2 a_0 a_1) = a11aa1$.

$$\text{Code}(a^0 a^1 \dots a^n) = \text{Code}(a^0) \cdot \text{Code}(a^1) \cdot \dots \cdot \text{Code}(a^n)$$

Коды команд

Код команды $q_i a_k \rightarrow q_j a_l \nu$, где $\nu \in \{L, N, R\}$, есть слово $q1^i a1^k \rightarrow q1^j a1^l \nu$ в алфавите Π .

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

Коды машин

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

Утверждение

Отображение $M \mapsto Code(M)$ 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^* .

$$\text{Code}(M) \in \Pi^*$$

Функция, вычислимая машиной Тьюринга

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

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

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



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

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

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

M_Δ : $\Delta^* \rightarrow \Delta^*$ — частичная функция, вычислимая M .

Замечание 26.1

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

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

$$\text{Code}(M)\$x \mapsto M_\Delta(x).$$

Другими словами:

- Если U_Δ начинает работу в конфигурации $q_1 \# \text{Code}(M) \$ x$ 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 .

Главность универсальной МТ

$F(n, x)$ - главная УВФ, если $\forall g: \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$
 $\in \text{Com}(\mathbb{N}, \mathbb{N})$, $\exists s: \mathbb{N} \rightarrow \mathbb{N}$ - тотальная выч.
 $\forall n \forall x \ F(s(n), x) \simeq g(n, x)$

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

$$\langle \overline{e} \ \$ \ \overline{x} \rangle \mapsto \overline{g(e, x)}$$

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

На входе $\langle \overline{M} \rangle$ и n
 $\text{Code}(M[n])$ Код

на выходе $M[n]$
 На входе \underline{x} $\frac{c(n, x)}{M}$

Пусть $\phi_{\Pi} : \mathbb{N} \rightarrow \Pi^*$, произвольная вычислимая тотальная биекция, такая что обратная биекция тоже вычислима.

Имеем

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

Вспомним, что универсальная функция $F(i, n) := |U_{\Delta}(\phi_{\Pi}(i)\$ \bar{n})|$.

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

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

m-СВОДИМОСТЬ

Говорят, что множество A натуральных чисел m -сводится к другому множеству B натуральных чисел, если существует всюду определённая вычислимая функция $f : \mathbb{N} \rightarrow \mathbb{N}$ с таким свойством:

$$x \in A \iff f(x) \in B$$

для всех $x \in \mathbb{N}$. Обозначение: $A \leq_m B$.

Свойства:

- \leq_m — рефлексивно и транзитивно;
- B — разрешима (перечислима) и $A \leq_m B \Rightarrow A$ — разрешима (перечислима);
- B — **неразреш.** (**неперечис.**) и $A \leq_m B \iff$ A — **неразреш.** (**неперечис.**);
- $A \leq_m B \iff \mathbb{N} \setminus A \leq_m \mathbb{N} \setminus B$;
- A — разрешима и $B \neq \emptyset, \mathbb{N} \Rightarrow A \leq_m B$.

Пусть F — главная универсальная вычислима функция.

$A = \{e \mid F_e(0) \neq 0\}$. Что можно сказать про множество A ?

По Т. Райса-Уэлча. A — неразрешимо

χ_A^* — вычислима, значит A — не вычислимо

$A = \{e \mid F_e(0) \neq 0\}$ — тотальность

A — неразрешимо

A — неперечислимо

m -полные множества

Множество A называется m -полным (в классе перечислимых множеств), если для любого перечислимого множества B верно, что $B \leq_m A$.

Теорема 26.2

Для главной УВФ $F(e, x)$ множество $K = \{e \mid F(e, e) \text{ определено}\}$ является m -полным.

K — перечислимо.

Предположим, что A — перечислимо. Рассмотрим функцию

$$g(n, x) = \begin{cases} \text{неопред.}, & \text{если } n \in A; \\ 1, & \text{если } n \notin A; \end{cases}$$

1 — ложь

По главность F найдется тотальная функция $f : \mathbb{N} \rightarrow \mathbb{N}$, т.ч.

$$g(n, x) \simeq F(f(n), x).$$

$$g(n, x) = \begin{cases} \text{неопред.}, & \text{если } n \notin A; \\ 1, & \text{если } n \in A; \end{cases}$$

$$g(n, x) \simeq F(f(n), x).$$

— вычисли

$$g(n, x) = \chi_A^*(n)$$

Покажем, что

$$n \in A \iff f(n) \in K$$

$$\begin{array}{c} \Downarrow \\ \forall x \, g(n, x) = 1 \\ \Downarrow \\ F_{f(n)} \text{ — всюду } \\ \text{вып.} \end{array} \quad \begin{array}{c} \Uparrow \\ \end{array}$$

$$\begin{array}{c} n \notin A \quad f(n) \notin K \\ \Downarrow \\ \forall x \, g(n, x) \text{ неоп.} \\ \Downarrow \\ F_{f(n)} \text{ — нигде } \\ \text{неоп.} \end{array} \quad \begin{array}{c} \Uparrow \\ \end{array}$$

$$\underline{x \in A \iff f(x) \in K} \quad A \leq_m K$$

Теорема Клини о неподвижной точке

Теорема 26.3 (Клини)

Пусть F — главная УВФ для класса $\text{Com}(\mathbb{N}, \mathbb{N})$, а h — всюду определённая вычислимая функция одного аргумента. Тогда существует такое число n , что $F_n \cong F_{h(n)}$, то есть n и $h(n)$ — номера одной функции.

$$n \equiv m \Leftrightarrow F_n \cong F_m$$

Лемма $\forall f$ - вычисл. ф-ция $\exists s$ - тотально вычисл. ф-ция т.ч.
 s продолжение f (по модулю \equiv) т.е. $\forall n \in \text{dom } f \quad (f(n) \equiv s(n))$

Док-во $g(n, x) \cong F(f(n), x)$ - вычисл. $\Rightarrow \exists s$ т.ч.

$$F(s(n), x) \cong g(n, x) \cong F(f(n), x) \\ s(n) \equiv f(n) \text{ где } n \in \text{dom } f$$

Теорема Клини о неподвижной точке

Теорема 26.3 (Клини)

Пусть F — главная УВФ для класса $\text{Com}(\mathbb{N}, \mathbb{N})$, а h — всюду определённая вычислимая функция одного аргумента. Тогда существует такое число m , что $F_n = F_{h(n)}$, то есть n и $h(n)$ — номера одной функции.

$$n \equiv h(n)$$

Пусть

h не имеет неподв. точки в смысле \equiv

$$f(n) = F(n, n)$$

Заметим, что f не имеет всюду опр. продолжения от f на всех точках

Sup

По лемме $\exists f_0$ — тотальна в \mathcal{C} и $\forall n \in \text{dom } f \quad f_0(n) \equiv f(n)$

$$t(n) = h(f_0(n))$$

- 1) t — тотально вычислима
- 2) $t(n) \neq f(n)$

$$\begin{array}{l} f(n) - \text{не опр.} \quad t(n) - \text{опр.} \\ f(n) - \text{опр.} \quad t(n) = h(f_0(n)) \neq f(n) \\ \Rightarrow t(n) \neq f(n) \end{array}$$

Программа печатающая свой номер (текст)

Следствие 26.4

пусть

Существует n , такой что $F(\underline{n}, \underline{x}) = \underline{n}$ при любом x .

$g(n, x) = n$ — вычислим
 $\exists s$ — тот выч
по Т. Кини
 $\exists k$ т.ч. $\forall x (F(s(n), x) \simeq g(n, x))$
т.ч. $\forall x (F(s(k), x) \simeq F(k, x))$

$$\underline{F(k, x)} = F(s(k), x) = g(k, x) = \underline{k}$$

Программа печатающая свой номер (текст)

Следствие 26.4

Существует n , такой что $F(n, x) = n$ при любом x .

Дур $\exists n, m$
 $\forall x (F(n, x) = m \wedge F(m, x) = n)$

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 $\text{Exp}(x) = 2^x$.

$$\boxed{\forall x \leq n \quad \exists y \leq t}$$

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 $\text{Exp}(0) = S(0), \quad \text{Exp}(S(a)) = \text{Exp}(a) + \text{Exp}(a),$

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

Теория Q получается из PA заменой схемы индукции единственной аксиомой:

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

Упражнение 26.1

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 $\neg S(a) \leq 0$.

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

- ❶ $a \leq S(x)$
- ❷ $a \leq x \vee a = S(x)$ (аксиома)
- ❸ $(a = x \vee S(a) \leq x) \vee a = S(x)$ (пр. инд.)
- ❹ $S(a) = S(x) \vee S(a) \leq x \vee a = S(x)$ (аксиома)
- ❺ $S(a) \leq S(x) \vee a = S(x)$

Вывод (2)

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

Шаг:

- ❶ $a \leq x \vee x \leq a$ (пр. инд.)
- ❷ $x \leq a \rightarrow (a = x \vee S(x) \leq a)$ (1)
- ❸ $a \leq x \vee a = x \vee S(x) \leq a$
- ❹ $a \leq x \rightarrow a \leq S(x)$ (аксиома)
- ❺ $a = x \rightarrow a \leq S(x)$ (из (1))
- ❻ $a \leq S(x) \vee S(x) \leq a$