

Конспект по теории вычислимости
IV семестр, 2021 год
Современное программирование, факультет математики и
компьютерных наук, СПбГУ
(лекции Пузыниной Светланы Александровны)

Тамарин Вячеслав

February 13, 2021

Contents

1	Вычислимость. Система вычислимости по Клини	3
1.1	Рекурсивные функции	3
1.1.1	Простейшие функции	3
1.1.2	Операторы	3
1.1.3	Функции	4
1.1.4	Оператор ограниченной минимизации	6
1.1.5	Предикаты	6
1.1.6	Теоремы про рекурсии	8
1.2	Равносильность МТ и ЧРФ	10

Исходный код на https://github.com/tamarinvs19/theory_university

**Некоторые доказательства были опущены на лекции, но написаны мной. Они выделены
оранжевыми символами:**

□ Исправляйте, дополняйте, меняйте. Чем меньше недоказанных утверждений, тем лучше! ■

Index

k -местная частичная функция, 3

общерекурсивная функция, 4

оператор минимизации, 4

оператор ограниченной минимизации, 6

оператор примитивной рекурсии, 3

оператор суперпозиции, 3

предикаты, 7

примитивно рекурсивная функция, 4

простейшие функции, 3

частично рекурсивная функция, 4

Chapter 1

Вычислимость. Система вычислимости по Клини

1.1 Рекурсивные функции

Лекция 1: †

11 feb

Определение 1

Пусть функция $f: \mathbb{N}^k \rightarrow \mathbb{N}$, $k \in \mathbb{N}$, где $\mathbb{N} = \{0, 1, 2, \dots\}$. Такая функция называется **k -местной частичной функцией**. Если $k = 0$, то $f = \text{const}$.

1.1.1 Простейшие функции

Простейшими будем называть следующие функции:

- Нуль местный нуль — функция без аргументов, возвращающая 0;
- Одноместный нуль — $0(x) = 0$;
- Функция следования — $s(x) = x + 1$;
- Функция выбора (проекция) — $I_n^m(x_1, \dots, x_n) = x_m$

1.1.2 Операторы

Определим три оператора:

- Функция f **получается оператором суперпозиции** из функций h и g , где

$$h(y_1, \dots, y_m), g_i(x_1, \dots, x_n); 1 \leq i \leq n,$$

если

$$f = h(g_1(x_1, \dots, x_n), \dots, g_m(x_1, \dots, x_n)).$$

Оператор обозначается **S**.

- Функция $f^{(n+1)}_1$ **получается оператором примитивной рекурсии** из $g^{(n)}$ и $h^{(n+2)}$, если

$$\begin{cases} f(x_1, \dots, x_n, 0) = g(x_1, \dots, x_n) \\ f(x_1, \dots, x_n, y + 1) = h(x_1, \dots, x_n, y, f(x_1, \dots, x_n, y)) \end{cases}$$

¹Здесь и далее $f^{(n)}$ обозначается функция, принимающая n аргументов, то есть n -местная

Оператор обозначается **R**.

- Функция f задается **оператором минимизации (M)**, если она получается из функции g следующим образом:

$$f(x_1, \dots, x_n) = \mu y [g(x_1, \dots, x_n, y) = 0] = \begin{cases} y & g(x_1, \dots, x_n, y) = 0 \wedge g(x_1, \dots, x_n, i)^2 \neq 0 \forall i < y \\ \uparrow^3 & \text{else} \end{cases}$$

Пример 1.1.1.

$$x - y = \begin{cases} x - y, & x \geq y \\ \uparrow, & x < y \end{cases}$$

Можно задать по другому, чтобы g была **ПРФ**:

$$x - y = \mu y [|(x + z) - y| = 0].$$

1.1.3 Функции

Определение 2: Примитивно рекурсивная функция

Функция f называется **примитивно рекурсивной (ПРФ)**, если существует последовательность таких функций f_1, \dots, f_k , что все f_i либо простейшие, либо получены из предыдущих f_1, \dots, f_{i-1} с помощью одного из операторов **S** и **R** и $f = f_k$.

Пример 1.1.2. Докажем, что $f(x, y) = x + y$ — **ПРФ**. По **R** можем получить f так:

$$\begin{cases} f(x, 0) &= x = I_1^1(x) = g \\ f(x, y + 1) &= (x + y) + 1 = s(f(x, y)) = S(I_3^3(x, y, f(x, y))) = h \end{cases}$$

Теперь построим последовательность функций f_i , где последним элементом будет f , полученный с помощью **R**:

$$I_1^1, s, I_3^3, h = S(s, I_3^3), f.$$

Определение 3: Частично рекурсивная функция

Функция f называется **частично рекурсивной функцией (ЧРФ)**, если существует последовательность функций f_1, \dots, f_k , таких что f_i либо простейшая, либо получается из предыдущих с помощью одного из операторов **S**, **R**, **M**.

Замечание. Частично рекурсивная функция может быть не везде определена. Но примитивно рекурсивная определена везде.

Замечание. Существуют частично рекурсивные функции, которые всюду определены, но при этом не являются **ПРФ**.

Определение 4

Общерекурсивная функция — всюду определенная частично рекурсивная.

Пример 1.1.3. $\mu y [x + y + 1 = 0]$ — нигде не определена, но получается из последовательности других функций с помощью операторов.

Лемма 1. Следующие функции являются **ПРФ**:

1. $\text{const}^{(n)}$

2. $x + y$

3. $x \cdot y$

4. x^y , где 0^0 можем определить, как хотим

5. $\text{sg}(x) = \begin{cases} 1 & x = 0 \\ 0 & x \neq 0 \end{cases}$

6. $\overline{\text{sg}}(x) = \begin{cases} 1 & x = 0 \\ 0 & x \neq 0 \end{cases}$

7. $x \div 1 = \begin{cases} 0 & x = 0 \\ x - 1 & x > 0 \end{cases}$

8. $x \div y = \begin{cases} 0 & x < y \\ x - y & \text{else} \end{cases}$

9. $|x - y|$



1. Сначала можем получить нужное число последовательной суперпозицией функции следования (получили константу от одной переменной), затем проецируем I_1^n , чтобы получить n переменных.

2. Доказали выше в примере 1.1.2.

3. $f(x, y) = xy$ определим так:

$$\begin{cases} f(x, 0) &= 0 \\ f(x, y + 1) &= f(x, y) + x \end{cases}$$

а складывать мы умеем.

4. $f(x, y) = x^y$:

$$\begin{cases} f(x, 0) &= 1 = s(0) \\ f(x, y + 1) &= f(x, y) * y \end{cases}$$

Умножать тоже можно по пролому пункту.

5. $\text{sg}(x) = \begin{cases} 1 & x = 0 \\ 0 & x \neq 0 \end{cases}$

$$\begin{cases} \text{sg}(0) &= 0 \\ \text{sg}(x + 1) &= 1 = s(0) \end{cases}$$

6. Аналогично

7. $f(x) = x \div 1$

$$\begin{cases} f(0) &= 0 \\ f(x + 1) &= x = I_1^1(x) \end{cases}$$

$$8. f(x, y) = x \dot{-} y$$

$$\begin{cases} f(x, 0) &= x = I_1^1(x) \\ f(x, y + 1) &= f(x, y) \dot{-} 1 \end{cases}$$

$$9. f(x, y) = |x - y| = (x \dot{-} y) + (y \dot{-} x)$$

Замечание. Обычное вычитание не является **ПРФ**, так как не везде определено на \mathbb{N} .

1.1.4 Оператор ограниченной минимизации

Определение 5: Оператор ограниченной минимизации

Функция $f^{(n)}$ задается **оператором ограниченной минимизации** из функций $g^{(n+1)}$ и $h^{(n)}$, если

$$\mu y \leq h(\bar{x}) [g(\bar{x}, y) = 0]^a.$$

Это означает, что

$$f(\bar{x}) = \begin{cases} y & g(\bar{x}, y) = 0 \wedge y \leq h(\bar{x}) \wedge g(\bar{x}, i) \neq 0^b \forall i < y \\ h(\bar{x}) + 1 & \text{else} \end{cases}.$$

^aЗдесь и далее $\bar{x} = x_1, \dots, x_n$.

^bАналогично, подразумевается, что функция определена в этих точках

Утверждение. Пусть $g^{(n-1)}, h^{(n)}$ — примитивно рекурсивные функции, $f^{(n)}$ получается из g и h с помощью ограниченной минимизации, то f тоже **ПРФ**.

□ Заметим, что f можно получить следующим образом:

$$f(\bar{x}) = \sum_{y=0}^{h(\bar{x})} \prod_{i=0}^y \text{sg}(g(\bar{x}, i)).$$

Внутреннее произведение равно единице только тогда, когда все $g(\bar{x}, i) \neq 0$. Если для некоторого y обнуляется $g(\bar{x}, y)$, то все произведения, начиная с $y + 1$, будут равны нулю, поэтому просуммируются только y единиц. Если же такого y нет, получим сумму из $h(\bar{x}) + 1$ единиц. Именно это и нужно.

Проверим, что можно получить $a(\bar{x}, y) = \sum_{i=0}^y g(\bar{x}, i)$ и $m(\bar{x}, y) = \prod_{i=0}^y g(\bar{x}, i)$ с помощью примитивной рекурсии:

$$\begin{cases} a(\bar{x}, 0) &= g(\bar{x}, 0) \\ a(\bar{x}, y + 1) &= a(\bar{x}, y) + g(\bar{x}, y + 1) \end{cases} \quad \begin{cases} m(\bar{x}, 0) &= g(\bar{x}, 0) \\ m(\bar{x}, y + 1) &= m(\bar{x}, y) \cdot g(\bar{x}, y + 1) \end{cases}$$

Замечание. $0(x)$ можно исключить из определения простейших функций, так как она получается с помощью **R** для нульмерного **0** и $I_2^2(x, y)$:

$$0(y) = \begin{cases} 0(0) &= 0 \\ 0(y + 1) &= I_2^2(y, 0) \end{cases}$$

1.1.5 Предикаты

Определение 6

Предикат — условие задающее подмножество: $R \subset \mathbb{N}^k$.

Предикат называется **примитивно рекурсивным (общерекурсивным)**, его характеристическая функция примитивно рекурсивная (общерекурсивная).

$$\chi_R(\bar{x}) = \begin{cases} 1, & \bar{x} \in R \\ 0, & \bar{x} \notin R \end{cases}.$$

Утверждение.

- Если R, Q — примитивно рекурсивные (общерекурсивные) предикаты, то $P \vee Q, P \wedge Q, P \rightarrow Q, \neg P$ тоже примитивно рекурсивные (общерекурсивные).
- Предикаты $=, \leq, \geq, <, >$ тоже примитивно и общерекурсивны.



- Проверим, что характеристические функции примитивно / общерекурсивны:

$$\begin{aligned} \chi_{P \vee Q}(\bar{x}) &= \chi_P(\bar{x}) \vee \chi_Q(\bar{x}) \\ \chi_{P \wedge Q}(\bar{x}) &= \text{sg}(\chi_P(\bar{x}) + \chi_Q(\bar{x})) \\ \chi_{P \rightarrow Q}(\bar{x}) &= \overline{\text{sg}}(\chi_P(\bar{x}) + \overline{\text{sg}}(\chi_Q(\bar{x}))) \\ \chi_{\neg P}(\bar{x}) &= \overline{\text{sg}}(\chi_P(\bar{x})) \end{aligned}$$

- Аналогично выразим, через простейшие:

$$\begin{aligned} \chi_{x=y}(x) &= \overline{\text{sg}}(|x - y|) = \begin{cases} 1, & x = y \\ 0, & x \neq y \end{cases} \\ \chi_{x < y}(x) &= \text{sg}(x \div y) \end{aligned}$$

Остальные можем выразить также или через уже проверенные $<$ и \neg .



Лемма 2. Следующие функции являются примитивно рекурсивными:

1. $\left\lfloor \frac{x}{y} \right\rfloor$, считаем, что $\left\lfloor \frac{x}{0} \right\rfloor = x$
2. $\text{Div}(x, y) = \begin{cases} 1, & y \mid x \\ 0, & \text{else} \end{cases}$
3. $\text{Prime}(x) = \begin{cases} 1, & x \in \mathbb{P} \\ 0, & \text{else} \end{cases}$
4. $f(x) = p_x$, где p_x — x -тое простое число, $p_0 := 2$
5. $\text{ex}(i, x)$ — степень простого числа p_i разложения x , $\text{ex}(i, 0) := 0$



1. $f(x, y) = \left\lfloor \frac{x}{y} \right\rfloor$. Найдем минимальное k , что $f'(x, y, k) = yk > x$. Чтобы получить $f(x, y) = \min(k \mid f'(x, y, k)) - 1$. Используем оператор минимизации:

$$f(x, y) = \mu k [\neg f'(x, y, k) = 0] - 1.$$

$$2. \text{Div}(x, y) = \left\lfloor \frac{x}{y} \right\rfloor \cdot y = x$$

3. Определим $\text{Div}'(x, y) = (y \leq 1) \vee (\neg \text{Div}(x, y))$, эта функция проверяет, что y не является нетривиальным делителем x .

Теперь, используя ограниченную минимизацию, выразим $\text{Prime}(x)$:

$$\text{Prime}(x) = \left(\mu y \leq h(x) [\text{Div}'(x, y) = 0] \right) = x, \text{ где } h(x) = x - 1.$$

То есть мы посмотрели на все меньшие числа, если среди них найдется нетривиальный делитель, то число не простое.

4. Пусть $f'(x) =$ количество простых $\leq x$.

$$\begin{cases} f'(0) &= 0 \\ f'(x+1) &= \text{Prime}(x+1) + f(x) \end{cases}$$

Теперь можно вычислить $f(x)$: для этого определим функцию $g(x, y) = (f'(y) = x)$,

$$f(x) = \mu y [\neg f'(x, y) = 0].$$

5. Чтобы найти степень вхождения простого числа p_i в x , сначала находим это простое число по номеру, затем находим минимальное k , что x не делится на p_i^k и вычитаем единицу.



1.1.6 Теоремы про рекурсии

Теорема 1.1.1 (Канторовская нумерация). Пусть $\pi: \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$:

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

- Тогда для любого z существует единственное представление $z = \pi(x, y)$.
- Причем функции $x(z), y(z)$ примитивно рекурсивные.



- Запишем $\pi(x, y) = \binom{x+y}{2} + y$. Заметим, что для $n > m$ верно

$$\binom{n}{2} - \binom{m}{2} \geq \binom{n}{2} - \binom{n-1}{2} = n - 1.$$

Предположим, что $x + y > x' + y'$ и $\pi(x, y) = \pi(x', y')$. Тогда

$$y' - y = \binom{x+y}{2} - \binom{x'+y'}{2} \geq x + y - 1 \geq x' + y'.$$

Но $y \geq 0$, $x' \geq 0$, поэтому единственный возможный вариант, когда они равны нулю, а $x + y = x' + y' + 1$. Проверим на равенство $\pi(x, y)$ и $\pi(x', y')$:

$$\begin{aligned} \pi(x, y) &= \frac{1}{2}x(x+1) = \frac{1}{2}(y'+1)(y'+2) = \frac{1}{2}y'(y'+1) + y' + 1 \\ \pi(x', y') &= \frac{1}{2}y'(y'+1) + y' \end{aligned}$$

Равенства нет.

- Можно по-честному все посчитать и выразить $x(z)$, $y(z)$. Пусть

$$w = x + y$$

$$t = \frac{1}{2}w(w+1) = \frac{w^2 + w}{2}$$

$$z = t + y$$

Решим квадратное уравнение, чтобы выразить w через t (отрицательный корень можем сразу отбросить):

$$w = \frac{-1 + \sqrt{8t+1}}{2}.$$

Запишем неравенство:

$$t \leq z = t + y < t + (w+1) = \frac{(w+1)^2 + (w+1)}{2}.$$

Отсюда

$$w \leq \frac{-1 + \sqrt{8z+1}}{2} < w+1.$$

Тогда

$$w = \left\lfloor \frac{-1 + \sqrt{8z+1}}{2} \right\rfloor$$

$$t = \frac{w^2 + w}{2}$$

$$y = z - t$$

$$x = w - y$$

Таким образом, мы выразили через z обе координаты. Единственный момент — нужно извлекать корень, в натуральную степень возводить мы умеем, поэтому можем с помощью ограниченной минимизации перебрать все меньшие числа, возвести их в квадрат и сравнить с нашим числом.



Теорема 1.1.2 (Возвратная рекурсия). Зафиксируем s . Пусть

$$\begin{cases} f(\bar{x}, 0) &= g(x) \\ f(\bar{x}, y+1) &= h(\bar{x}, y, f(\bar{x}, t_1(y)), \dots, f(\bar{x}, t_s(y))) \end{cases}$$

где $t_i(g) \leq y \ \forall 1 \leq i \leq s, g^{(n)}, h^{(n+1+s)}, t_i^{(1)}$.

Тогда, если g, h, t_i — примитивно / общерекурсивные, то и f тоже.

□ Пока без доказательства.



Теорема 1.1.3 (Совместная рекурсия). Пусть $f_i, 1 \leq i \leq k$ — рекурсии,

$$\begin{cases} f_i(\bar{x}, 0) &= g_i(\bar{x}) \\ f_i(\bar{x}, y+1) &= h_i(\bar{x}, y, f_1(\bar{x}, y), \dots, f_k(\bar{x}, y)) \end{cases}$$

Если $g_i, h_i, 1 \leq i \leq k$ — примитивно / общерекурсивные, то f_i тоже.

□ Пока без доказательства. Полезно использовать канторову нумерацию.



Теорема 1.1.4 (Кусочное задание функции). Пусть R_0, \dots, R_k — отношения, такие что $\bigcup_{i=0}^k R_i = \mathbb{N}$ и для $i \neq j$ верно $R_i \cap R_j = \emptyset$. Для $|\bar{x}| = n$:

$$f(\bar{x}) = \begin{cases} f_0(\bar{x}) & \text{если } R_0(\bar{x}) \\ f_1(\bar{x}) & \text{если } R_1(\bar{x}) \\ \vdots & \vdots \\ f_k(\bar{x}) & \text{если } R_k(\bar{x}) \end{cases}$$

Если f_i, R_i — примитивно / общерекурсивны, то и f тоже.

□ Пока без доказательства. ■

1.2 Равносильность МТ и ЧРФ

Теорема 1.2.1. Функция вычисляется машиной Тьюринга тогда и только тогда, когда она частично рекурсивная.

□ Если $f(x_1, \dots, x_n) = y$, то считаем, что МТ получаем $1^{x_1}01^{x_2}0 \dots 01^{x_n}$ и должна выдать 1^y ; если f не определена, МТ должна заикливаться и наоборот.

2 \implies 1

- Для простых функций можем построить МТ напрямую.
- Для операторов **S, R, M**:

S: Пусть есть набор функций $h^{(n)}, g_1^{(m)}, \dots, g_n^{(m)} \longrightarrow f^{(m)}$, для каждой из которых есть машина Тьюринга M_h и M_{g_i} .

Хотим построить МТ M_S для S .

Сделаем это так:

- Копируем весь вход n раз:

$$\left(1^{x_1}01^{x_2} \dots 01^{x_n}*\right)^n.$$

- Запускаем M_{g_i} на соответствующей части полученного входа.

Если нужно что-то записать, то будем сдвигать всю правую часть на нужное число клеток, чтобы освободить для место.

МТ запускаем псевдопараллельно (по очереди даем поработать).

В каждой части после окончания работы оставляем только ответ:

$$1^{y_1} * 1^{y_2} \dots * 1^{y_n},$$

где $y_i = g_i(x_1, \dots, x_m)$.

- Запускаем на этом результате M_h .

R:

M:

1 \implies 2

