Определение

Частичной функцией $f : X \to Y$ называется подмножество $f \subseteq X \times Y$ такое, что из $\langle x, y_1 \rangle \in f$ и $\langle x, y_2 \rangle \in f$ следует $y_1 = y_2$.

Пишем $f(x) = y$ вместо $\langle x, y \rangle \in f$;

$!f(x)$ вместо $\exists y\, f(x) = y$.

Областью определения частичной функции f называется множество $dom(f) := \{x \in X : \exists y \in Y\ \langle x, y \rangle \in f\}$.

Областью значений частичной функции f называется множество $rng(f) := \{y \in Y : \exists x \in X\ \langle x, y \rangle \in f\}$.

Частичная функция $f : X \to Y$ **вычислима**, если она вычисляется некоторым алгоритмом.

В частности, можно говорить о вычислимых функциях $f : \Sigma^* \to \Sigma^*$, $f : \mathbb{N}^k \to \mathbb{N}$ и т.д.

$\mathcal{A}$ на входе $x \in X$ заканчивает работу, если $!f(x)$ и выдает $f(x)$

$\mathcal{A}$ незакан.. раб. (зацикливается), если $f(x)$ неопр. $x \notin dom(f)$)

Тезис Чёрча–Тьюринга

Тезис

Любая вычислимая в интуитивном смысле частичная функция $f : \Sigma^* \to \Sigma^*$ вычислима на машине Тьюринга.

Замечание

Это утверждение не является математическим, но говорит об адекватности математической модели (вычислимости по Тьюрингу) **реальному** явлению (вычислимости).

Все попытки построения более общих вычислительных моделей неизбежно приводили к тому же самому классу вычислимых функций.

Физический тезис Чёрча–Тьюринга

Текущему уровню знаний не противоречит и более сильный

Тезис

Всякая функция $f : \Sigma^* \to \Sigma^*$, вычислимая на (идеализированном) **физически реализуемом** устройстве, вычислима на машине Тьюринга.

Замечание

Физический тезис предполагает возможность аналогового вычисления, квантово–механические эффекты и т.д.

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.

- Команды имеют вид $\boxed{qa \to rb\nu}$, где $q, r \in Q$, $a, b \in \Sigma$ и $\nu \in \{L, N, R\}$.
  «прочтя символ a в состоянии q перейти в состояние r, заменить содержимое ячейки на b и сместиться влево (L), остаться на месте (N) или сместиться вправо (R) на одну ячейку, в зависимости от значения ν»
- Требуется, чтобы в программе P была ровно одна команда с левой частью qa для каждого $q \in Q \setminus \{q_0\}$ и $a \in \Sigma$.

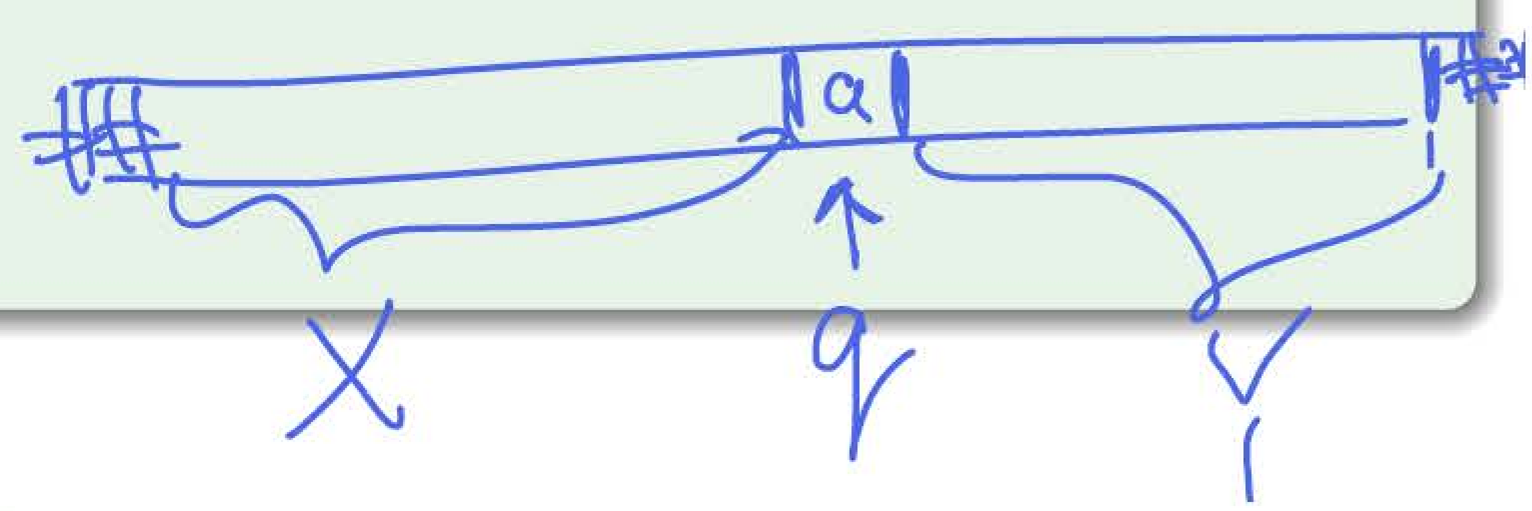
Соглашение: команды вида $qa \to qaN$, приводящие к зацикливанию, можно не указывать.

Конфигурации

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

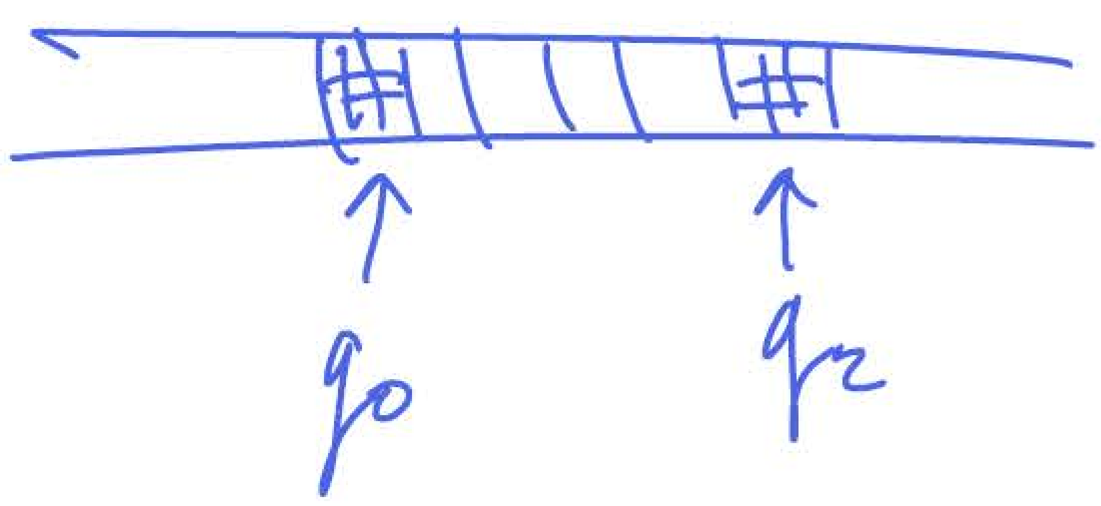
Конфигурация машины M определяется содержимым ленты, состоянием и положением головки. Конфигурация записывается словом вида $XqaY$, где

- $XaY \in \Sigma^*$ есть содержимое ленты,
- $q \in Q$ есть состояние M,
- головка обозревает символ a.

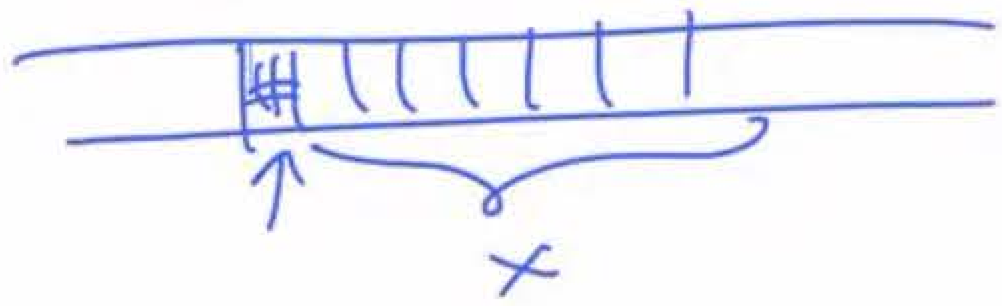


Машина M из примера (почти) вычисляет функцию $\text{neg} : \{0,1\}^* \to \{0,1\}^*$, заменяющую в данном слове 0 на 1 и 1 на 0. Чтобы вернуть головку в начало модифицируем M:

$$
\begin{array}{rcl}
q_1\# & \mapsto & q_1\#R \\
q_1 0 & \mapsto & q_2 1R \\
q_1 1 & \mapsto & q_2 0R \\
q_2 0 & \mapsto & q_2 1R \\
q_2 1 & \mapsto & q_2 0R \\
\hline
q_2\# & \mapsto & q_3\#L \\
q_3 0 & \mapsto & q_3 0L \\
q_3 1 & \mapsto & q_3 1L \\
q_3\# & \mapsto & q_0\#N
\end{array}
$$



Функция, вычислимая машиной Тьюринга



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

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.

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

Замечание

На множестве Σ^* определить «умножение», как конкатенацию слов. Получится моноид с пустым словом ε в качестве единицы. Степень определяется естественным образом.

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

$\bar{f}(x) = y$, если $x = 1^{n_1}0\dots01^{n_k}$ и $y = 1^m$ для некоторых $n_1, \dots, n_k, m \in \mathbb{N}$ и $f(n_1, \dots, n_k) = m$.

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

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 $l(c(x,y)) = x$, $r(c(x,y)) = y$.

Почему функции l и r вычислимы?

Кортежи произвольной длины

Кортежи произвольной длины тоже можно закодировать:

$$c_3(x_1, x_2, x_3) = c(c(x_1, x_2), x_3)$$

$$\dots$$

$$c_{n+1}(x_1, \dots, x_{n+1}) = c(c_n(x_1, \dots, x_n), x_{n+1})$$

Разрешимые множества

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

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

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

$\chi_{\mathbb{N}\setminus A}(x) = 1 - \chi_A(x)$

$A \cap B$ χ_A, χ_B – вычисл

$\chi_{A \cap B}(x) = \chi_A(x) \cdot \chi_B(x)$

$\cup$

Утверждение

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

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

Множество A, удовлетворяющее любому из пунктов следующей теоремы, называется перечислимым.

Теорема 23.1

Для любого $A \subseteq \mathbb{N}$ следующие утверждения 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. $A = \{x \mid \exists y\ \langle x, y\rangle \in B\}$ для некоторого разрешимого $B \subseteq \mathbb{N} \times \mathbb{N}$ (A — проекция разрешимого множества).

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

$\boxed{A = \mathrm{dom}(f)}$

$2 \Rightarrow 5$:
Пусть машина M_f вычисляет f. Рассмотрим

$$\mathbb{N}\times\mathbb{N} \supseteq B := \{\langle x, y\rangle : M_f \text{ на входе } x \text{ ост. за } y \text{ шагов}\}.$$

χ_B

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

Найти f, $\mathrm{range}(f) = A$

$5 \Rightarrow 4$:
Допустим $A \neq \varnothing$, выберем $a_0 \in A$.
Определим $f : \mathbb{N} \to \mathbb{N}$ так:

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

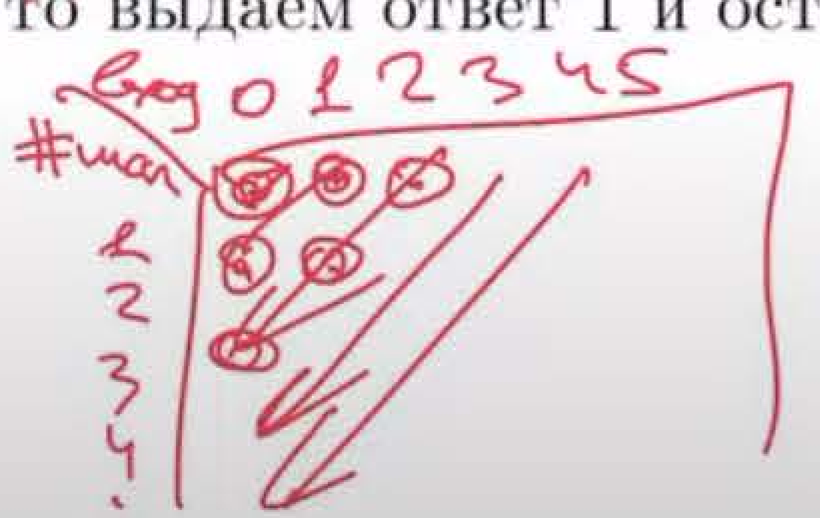
$A = \varnothing \iff B = \varnothing$

$A = \mathrm{rng}(f)$

$3 \Rightarrow 1$:
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

$\chi^*_{A\cup B}(x)$

$\to x$ 1 шаг χ^*_A | 2 ш

1 шаг χ^*_B | 2 ш

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

A, B — перечислимы

$A \cap B$ $\qquad f \quad \operatorname{rng}(f) = A$

$g \quad \operatorname{dom}(g) = B$

$\operatorname{dom}(h) = A\cap B \quad h(x) = g(f(x))$

χ^*_A

χ^*_B

$A \cup B$

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

Утверждение

Всякое диофантово множество перечислимо.

Теорема Матиясевича

Теорема 23.2

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.

K — переч. через $\boxed{P_K(m, x_1, \ldots, x_n)}$ — имеет реш $\Leftrightarrow m \in K$

Теорема Поста

Теорема 24.1 (Пост)

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

($\Rightarrow$) Очевидно.

($\Leftarrow$) Случай, когда A или $\mathbb{N} \setminus A$ пусты очевиден.
Пусть определённые всюду функции f и g перечисляют A и $\mathbb{N} \setminus A$, соответственно. Т.е. $\operatorname{rng}(f) = A$ и $\operatorname{rng}(g) = \mathbb{N} \setminus A$. Тогда χ_A можно вычислить так:

Вычисляем $f(0), g(0), f(1), g(1), f(2), g(2), \ldots$ до тех пор, пока не встретим данный нам x и выводим 0 или 1, в зависимости от того на какой функции остановились.

Теорема о графике

Теорема 24.2

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

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

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

$f(x)$ – опр. – процесс закончи[тся] и выдать y.

$f(x)$ – неопр

$\langle x,0\rangle$ 1 $\langle x,1\rangle$ 1 $\langle x,2\rangle$ 1

$\langle x,0\rangle$ 2 $\langle x,1\rangle$ 2

$\langle x,0\rangle$ 3

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

Теория T разрешима, если множество теорем T разрешимо.

Теорема 24.3

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

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

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

$T \vdash B \quad \exists n \quad A_n - B$

$A_0 \wedge \ldots \wedge A_n \in 1$

$C = A_0$

$C = A_0 \wedge A_1$

$A_0 \wedge \ldots \wedge A_n \to A_n \leftarrow$ акс

A_n

Теорема 24.4

Полная эфф. аксиоматизируемая теория разрешима.

Полные эфф. аксиоматизируемые теории:

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

Подробнее про элементарную геометрию:
http://www.mathnet.ru/php/presentation.phtml?presentid=9380

Универсальная машина Тьюринга это МТ, которая умеет «моделировать» любую другую МТ.

Теорема 24.5
Универсальная МТ существует.

Неформальный аргумент: существуют компиляторы и интерпретаторы полных по Тьюрингу языков программирования.

Идея: Каждой МТ M сопоставляется код $Code(M)$ в некотором алфавите Π. Универсальная МТ (обозначим ее U_Δ) работает так, что если ей на вход подать слово $Code(M)\$x$, где $x \in \Delta^*$, а $\$$ — специальный символ, выдает то же что M на входе x.

Условное равенство

Пусть f, g — частичные функции.

$f(x) \simeq g(x)$ означает, что либо $x \in \mathrm{dom}(f) \cap \mathrm{dom}(g)$ и $f(x) = g(x)$, либо $x \notin \mathrm{dom}(f)$ и $x \notin \mathrm{dom}(g)$.
$f \simeq g \iff \forall x (f(x) \simeq g(x))$

$$x \cdot \frac{1}{x} \simeq \frac{1}{x} \cdot x$$

Для МТ M и универсальной МТ U_Δ можно записать:

$$\forall x \in \Delta^* \; (U_\Delta(Code(M)\$x) \simeq M_\Delta(x))$$

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

Универсальной функцией для $\mathcal{F}$ называем такую функцию $F : \mathbb{N} \times X \to Y$, что
- Для любого $e \in \mathbb{N}$ функция $F_e(x) := F(e, x)$ принадлежит $\mathcal{F}$.
- $\forall f{\in}\mathcal{F}\ \exists e{\in}\mathbb{N}\ \forall x{\in}X\ f(x) \simeq F(e, x)$.

Последнее условие можно записать так

$$\forall f{\in}\mathcal{F}\ \exists e{\in}\mathbb{N}\ f(x) \simeq F_e(x).$$

Замечание
- Универсальная функция F существует для любого счётного семейства $\mathcal{F}$.
- F определяет некоторую нумерацию $\mathcal{F}$: $\mathcal{F} = \{F_0(x), F_1(x), \dots\}$.

Число i называется индексом функции F_i относительно данной универсальной функции F.

Теорема 24.6
Семейство $\mathrm{Com}(\mathbb{N}, \mathbb{N})$ обладает вычислимой универсальной функцией $F \in \mathrm{Com}(\mathbb{N} \times \mathbb{N}, \mathbb{N})$.

Пусть $\Delta = \{1\}$. Обозначим $\overline{n} := 11\dots1$ (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 $\overline{f}(\overline{n}) := \overline{f(n)}$.

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

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

Рассмотрим выч. биекцию $\phi : \mathbb{N} \to \Pi^*$. Где Π это рабочий алфавит универсальной МТ. Для некоторого $i \in \mathbb{N}$ имеем $Code(M) = \phi(i)$. Значит, для всех $x \in \Delta^*$

$$\overline{f}(x) \simeq M_\Delta(x) \simeq U_\Delta(\phi(i)\$x).$$

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

$$F(i, n) := |U_\Delta(\phi(i)\$\overline{n})|.$$

Замечание 24.7
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.

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 24.8
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. F — вычислима.
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.

Перечислимое неразрешимое множество

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

Теорема 24.9
$K \subseteq \mathbb{N}$ перечислимо, но не разрешимо.

Допустим K разрешимо. Тогда функция

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

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

Проблема остановки

Проблема = массовая проблема

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

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

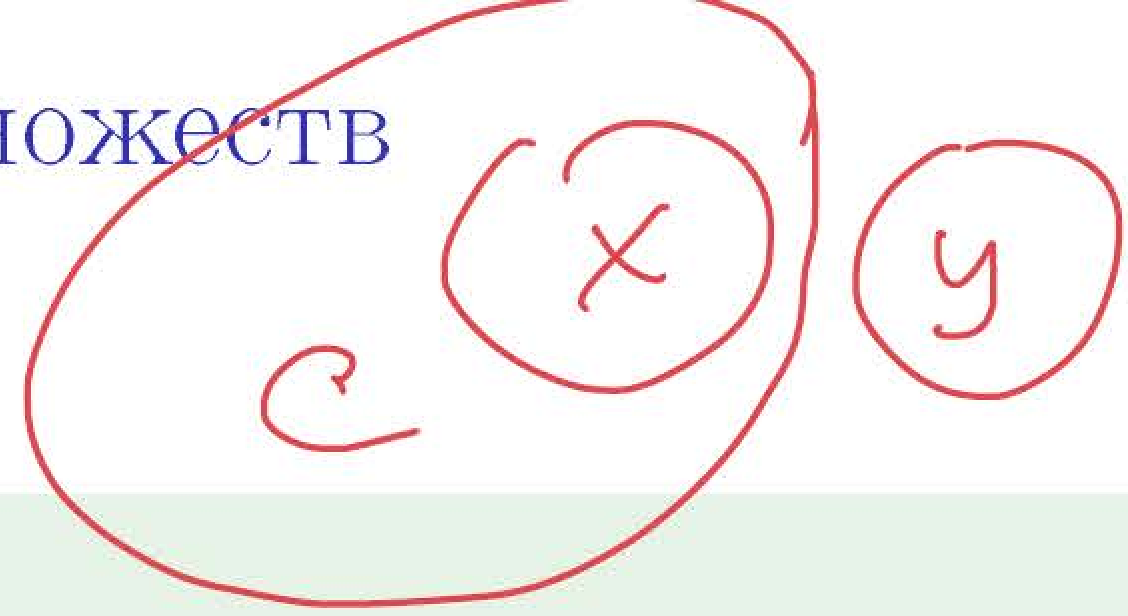
Теорема 24.10

Проблема остановки алгоритмически неразрешима.

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

- По данному x вычислить $y = \phi(x)$.
- 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 $x \notin K$.

Пара неотделимых перечислимых множеств



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

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

Теорема 25.1

Существует неотделимая пара перечислимых множеств.

Доказательство.

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

По теореме о графике X, Y перечислимы. $X \cap Y = \varnothing$

Если разрешимое C отделяет X и Y, то функция

$$g(x) := \begin{cases} 0, & \text{если } x \in C; \\ 1, & \text{иначе.} \end{cases} \quad = 1 - \chi_C(x)$$

продолжает f на всё $\mathbb{N}$.

Установленные факты

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

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

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

Главные универсальные функции

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

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

Теорема 25.3

Главная вычислимая универсальная функция $F : \mathbb{N}^2 \to \mathbb{N}$ существует.

На самом деле, универсальная МТ задает главную унив. функцию.

М – вычисляет g $\quad$ s на вход даём $\underline{\underline{e}}$

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.

<u>Вариации Шена</u>

$F(x, y)$ – ун. выч ф-ция

$\downarrow$

$T(x, y, z)$ – ун выч ф-ция для $Com(\mathbb{N}^3, \mathbb{N})$

$\downarrow$

F

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». +

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

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

$I_C = \phi$ $\quad$ $I_C = \mathbb{N}$

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

Теорема 25.4

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

Доказательство.

- Можно считать, что нигде не определённая функция ζ не обладает свойством $\mathcal{C}$ — иначе заменим $\mathcal{C}$ на его дополнение.
- Т.к. $\mathcal{C} \neq \varnothing$, фиксируем вычислимую функцию $f_0 \in \mathcal{C}$.
- Построим тотальную вычислимую функцию $s : \mathbb{N} \to \mathbb{N}$ такую, что для всех $x \in \mathbb{N}$
$$x \in K \iff s(x) \in I_{\mathcal{C}}.$$
- Если бы $I_{\mathcal{C}} := \{e \in \mathbb{N} : F_e \in \mathcal{C}\}$ было разрешимо, то мы получили бы следующий разрешающий алгоритм для K: для данного x вычислить $y = s(x)$ и проверить $y \in I_{\mathcal{C}}$.

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

- вычислить $F_e(e)$;
- если $!F_e(e)$, очистить ленту, а затем вычислить $f_0(x)$. $\in C$

По свойству главности получаем тотальную вычислимую функцию s такую, что
$$\forall e, x \; F_{s(e)}(x) \simeq g(e, x).$$

Тогда имеем:

- Если $e \in K$, то $F_{s(e)}(x) \simeq f_0(x)$; $\in C$ $\quad$ $s(e) \in I_C$
- Если $e \notin K$, то $\boxed{F_{s(e)} = \zeta}$ $\quad$ $\zeta \notin C$ $\quad$ $s(e) \notin I_C$

Отсюда $e \in K \iff F_{s(e)} \in \mathcal{C} \iff s(e) \in I_{\mathcal{C}}$.

m-сводимость

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

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

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

Свойства:

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

Пусть F — главная универсальная вычислима функция.
$A = \{e \mid F_e(0) \neq 0\}$. Что можно сказать про множество A?

По Т. Райса-Усп. A — неразрешимо

χ^*_A — вычислима, значит A — перечислимо

$A = \{e \mid F_e$ — тотально$\}$ A — неразрешимо

A — неперечислимо

m-полные множества

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

Теорема 26.2

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

K — перечислимо.
Предположим, что A — перечислимо. Рассмотрим функцию

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

вычисл

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

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

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

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

— вычислима

$g(n,x) = \chi^*_A(n)$

Покажем, что

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

$\Downarrow$

$\forall x\ g(n,x) = 1$

$\Downarrow$

$F_{f(n)}$ — всюду опр.

$n \notin A$ $f(n) \notin K$

$\Downarrow$

$\forall x\ g(n,x)$ неопр

$\Downarrow$

$F_{f(n)}$ — нигде неопр

$x \in A \iff f(x) \in K$ $A \leqslant_m K$

Теорема Клини о неподвижной точке

Теорема 26.3 (Клини)

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

$n \equiv m \iff F_n \simeq F_m$

Лемма $\forall f$ - вычисл ф-ю $\exists s$ - тотально выч ф-ция т.ч. s продолжае f (по модулю $\equiv$) т.е. $\forall n \in \mathrm{dom} f \; (f(n) \equiv s(n))$

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

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

$s(n) \equiv f(n)$ для $n \in \mathrm{dom} f$

Теорема 26.3 (Клини)

Пусть F — главная УВФ для класса $\mathrm{Com}(\mathbb{N},\mathbb{N})$, а h — всюду определённая вычислимая функция одного аргумента. Тогда существует такое число m, что $\boxed{F_n = F_{h(n)}}$, 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 отличающегося от f на всех точках Упр

По лемме $\exists f_0$ - тотальн выч ч $\forall n \in \mathrm{dom} f$ $f_0(n) \equiv f(n)$

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

1) t - тотально вычислима

2) $t(n) \neq f(n)$

$f(n)$ - неопр. $t(n)$ опр

$f(n)$ - опр. $t(n) = h(f_0(n)) \neq f_0(n)$

$\Rightarrow t(n) \neq f(n)$

Программа печатающая свой номер (текст)

Следствие 26.4

ГУВФ

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

$g(n,x) = n$ - вычислима

$\exists s$ - тот выч т.ч. $\forall x (F(s(n),x) \simeq g(n,x))$

По Т. Клини $\exists k$ т.ч. $\forall x (F(s(k),x) \simeq F(k,x))$

$F(k,x) = F(s(k),x) = g(k,x) = k$

Арифметика Пеано PA

Сигнатура: 0, S, $+$, $\cdot$, Exp, $\leq$, $=$

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

$\forall x \leq n \ \exists y \leq t$

Аксиомы PA

1. $\neg S(a) = 0$, $\quad S(a) = S(b) \to a = b$,
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. $\mathrm{Exp}(0) = S(0)$, $\quad \mathrm{Exp}(S(a)) = \mathrm{Exp}(a) + \mathrm{Exp}(a)$,
5. $a \leq 0 \leftrightarrow a = 0$,
6. $a \leq S(b) \leftrightarrow (a \leq b \vee a = S(b))$,
7. (Схема аксиом индукции)
   $A[a/0] \wedge \forall x\, (A[a/x] \to A[a/S(x)]) \to \forall x\, A[a/x]$,
   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 $\mathsf{PA} \vdash Q$.

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 $S(a) \leq 0 \to S(a) = 0$, имеем $\neg S(a) \leq 0$.

Шаг: эквивалентно преобразуем

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

Определение 1.1. *Арифметика Пеано* PA задаётся следующими нелогическими аксиомами:

1. аксиомы равенства для сигнатуры $0, S, +, \cdot, \exp, \leq, =$;
2. $\neg S(a) = 0, \quad S(a) = S(b) \to a = b$,
3. $a + 0 = a, \quad a + S(b) = S(a + b)$,
4. $a \cdot 0 = 0, \quad a \cdot S(b) = a \cdot b + a$,
5. $\exp(0) = S(0), \quad \exp(S(a)) = \exp(a) + \exp(a)$
6. $a \leq 0 \leftrightarrow a = 0$
7. $a \leq S(b) \leftrightarrow (a \leq b \vee a = S(b))$
8. (Схема аксиом индукции)
   $A[a/0] \wedge \forall x\, (A[a/x] \to A[a/S(x)]) \to \forall x\, A[a/x]$,
   для любой формулы A.

Стандартной моделью арифметики Пеано называем модель

$$(\mathbb{N}; 0, S, +, \cdot, \exp, \leq, =).$$

Следующие лемма и следствие очевидны.

Лемма 1.2. $\mathbb{N} \models$ PA.

Следствие 1.3. PA *непротиворечива.*

Определение 1.4. *Арифметика Робинсона* Q получается из PA заменой схемы индукции единственной аксиомой:

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

Замечание 1.5. Заметим, что из этой аксиомы следует $a \leq a$ (положим $b = a$) и $a \leq b \vee b < a$ (поскольку $\neg a \leq b \to \neg a = b$ в силу предыдущего).

Замечание 1.6. Теория Q задаётся конечным числом аксиом.

Упражнение 1.7. *Показать, что* PA $\vdash$ Q.

Решение. Последовательно докажем индукцией по x:

(i) $\forall x\, (a \leq x \leftrightarrow a = x \vee S(a) \leq x)$;

(ii) $\forall x\, (a \leq x \vee x \leq a)$.

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

Вывод утверждения (i):

Базис индукции: $a \leq 0 \leftrightarrow a = 0 \vee S(a) \leq 0$.
Импликации $a \leq 0 \to a = 0$ и $a = 0 \to a \leq 0$ получаем по аксиоме 6. Поэтому достаточно вывести $\neg S(a) \leq 0$. По аксиоме 6 формула $S(a) \leq 0$ влечет $S(a) = 0$, что противоречит аксиоме 2.

Шаг индукции: надо показать $a \leq S(x) \leftrightarrow S(a) \leq S(x) \vee a = S(x)$. Пользуясь предположением индукции строим следующую цепочку формул, каждая из которых эквивалентна предыдущей:

1. $a \leq S(x)$
2. $a \leq x \vee a = S(x)$ (по аксиоме 7)
3. $(a = x \vee S(a) \leq x) \vee a = S(x)$ (по предположению индукции)
4. $(S(a) = S(x) \vee S(a) \leq x) \vee a = S(x)$ (по аксиоме 2)
5. $S(a) \leq S(x) \vee a = S(x)$ (по аксиоме 7).

Вывод утверждения (ii):

Базис индукции: $a \leq 0 \vee 0 \leq a$. Мы получаем $0 \leq a$ очевидной индукцией по a.

Шаг индукции:

1. $a \leq x \vee x \leq a$ (предположение индукции)
2. $a \leq S(x) \vee x \leq a$ (по аксиоме 7)
3. $a \leq S(x) \vee (S(x) \leq a \vee x = a)$ (по утверждению (i))
4. $a \leq S(x) \vee (S(x) \leq a \vee a \leq S(x))$ (из $a \leq S(a)$)
5. $a \leq S(x) \vee S(x) \leq a$.

Таким образом, теория Q представляет собой конечную подтеорию арифметики PA.

Замечание 1.8. В теории Q не возможны доказательства по индукции, поэтому она не позволяет вывести сколько-нибудь содержательные свойства арифметических операций (см. упражнение ниже). Другими словами, Q является очень слабой подтеорией арифметики PA. Она играет роль минимально достаточной теории, для которой справедливы теоремы Гёделя о неполноте. Выбор такой теории, в отличие от PA, в значительной степени произволен. В частности, сам Р. Робинсон обозначал через Q несколько иную теорию (отличия, в основном, связаны с выбранным здесь вариантом языка арифметики).