

# Математические основы Computer Science

## Часть 1: Теория алгоритмов. Лекция 1.

Дмитрий Ицыксон

ПОМИ РАН

20 сентября 2009

# Содержание курса

## 1 Теория алгоритмов

- Вычислимые функции, разрешимые и перечислимые множества.
- Универсальный алгоритм.
- Перечислимое неразрешимое множество.
- Теорема Клини о неподвижной точке.
- Теорема Успенского-Райса.
- Машины Тьюринга и программы с конечным числом переменных.
- Предикатные формулы, неразрешимость исчисления предикатов.
- Выразимость в арифметике. Арифметичность вычислимых функций.
- Вычисления с оракулом. Арифметическая иерархия.
- Теоремы Тарского и Геделя.

## 2 Вероятностный метод в комбинаторике.

## 3 ...

## Литература к первой части курса

- 1 Н.К. Верещагин, А. Шень. Вычислимые функции.
- 2 Н.К. Верещагин, А. Шень. Языки исчисления

## О понятии «алгоритм»...

- Существует точное математическое определение алгоритма.
- Но мы его изучим позже :).
- Алфавит  $\Sigma$  — конечное множество символов.
- $\Sigma^*$  — множество строчек над алфавитом  $\Sigma$ .
- Алгоритм:
  - строка  $\mapsto$ 

[	строка
	не останавливается
  - Алгоритм можно записать.
  - Алгоритм можно исполнять по шагам.
- $\mathbb{N} = \{0, 1, 2, \dots\}$

## Разрешимые множества

**Определение.** Множество  $S \subset \mathbb{N}$  называется разрешимым, если существует такой алгоритм  $\mathcal{A}$ , что

- $\forall x \in S, \mathcal{A}(x) = 1$ ;
- $\forall x \notin S, \mathcal{A}(x) = 0$ .

- 1 Множество четных чисел разрешимо.
- 2 Множество простых чисел разрешимо.
- 3 Любое конечное множество разрешимо.
- 4 Множество рациональных чисел, меньших  $\epsilon$ , разрешимо.
- 5 Множество таких  $n$ , что в числе  $\pi$  есть  $n$  девяток подряд разрешимо.

## Перечислимые множества

**Определение 1.** Множество  $S \subset \mathbb{N}$  называется перечислимым, если существует такой (полуразрешающий) алгоритм  $\mathcal{A}$ , что

- $\forall x \in S, \mathcal{A}(x) = 1$ ;
- $\forall x \notin S, \mathcal{A}(x)$  не останавливается.

**Определение 2.** Множество  $S \subset \mathbb{N}$  называется перечислимым, если существует такой (перечисляющий) алгоритм  $\mathcal{B}$ , который на пустом входе выводит через запятую все элементы множества  $S$ .

- (2)  $\implies$  (1).  $\mathcal{A}(x)$  запускает  $\mathcal{B}$  и выдает 1, если  $\mathcal{B}$  печатает  $x$ .
- (1)  $\implies$  (2).
  - $\mathcal{A}^k(x)$  печатает  $x$ , если  $\mathcal{A}(x)$  останавливается ровно за  $k$  шагов.
  - $\mathcal{B}$  запускает:  $\mathcal{A}^1(0); \mathcal{A}^2(0), \mathcal{A}^1(1); \mathcal{A}^3(0), \mathcal{A}^2(1), \mathcal{A}^1(2); \mathcal{A}^4(0), \mathcal{A}^3(1), \mathcal{A}^2(2), \mathcal{A}^1(3) \dots$

## Перечислимость и разрешимость

**Теорема.**  $S$  — разрешимо  $\implies S$  — перечислимо.

**Доказательство.** Заменить ответ 0 на бесконечный цикл.

**Теорема.** (Пост) Если  $S$  и  $\mathbb{N} \setminus S$  перечислимы, то  $S$  — разрешимо.

**Доказательство.** Запустить параллельно полуразрешающие алгоритмы для  $S$  и  $\mathbb{N} \setminus S$ . Если остановится первый из них, то выдать 1, если остановится второй, то выдать 0.

## Вычислимые функции

**Определение.** Функция  $f : M \rightarrow \mathbb{N}$ ,  $M \subset \mathbb{N}$  называется вычислимой, если существует такой алгоритм  $\mathcal{A}$ , что

- $\forall x \in M, \mathcal{A}(x) = f(x)$ ;
- $\forall x \notin M, \mathcal{A}(x)$  не останавливается.

**Лемма.**  $S$  — перечислимо  $\iff S$  — это область определения вычислимой функции.

**Доказательство.**  $\Rightarrow$  Полуразрешающий алгоритм для  $S$  задает вычислимую функцию.

$\Leftarrow$  Заменить ответ функции на 1.

**Лемма.**  $S$  — перечислимо  $\iff S$  — это область значений вычислимой функции.

**Доказательство.**  $\Rightarrow$  Если полуразрешающий алгоритм остановился на  $x$ , то выдать  $x$ .

$\Leftarrow$   $\mathcal{A}^k(x)$  печатает  $\mathcal{A}(x)$ , если  $\mathcal{A}(x)$  останавливается ровно за  $k$  шагов. Запустить  $\mathcal{A}^1(0); \mathcal{A}^2(0), \mathcal{A}^1(1); \mathcal{A}^3(0), \mathcal{A}^2(1), \mathcal{A}^1(2); \mathcal{A}^4(0), \mathcal{A}^3(1), \mathcal{A}^2(2), \mathcal{A}^1(3) \dots$

## Вычислимость и перечислимость

**Теорема.** Функция  $f : M \rightarrow \mathbb{N}$  вычислима  $\iff$  ее график  $\{(x, f(x)) \mid x \in M\}$  перечислим.

**Доказательство.**  $\implies$  Функция  $x \mapsto (x, f(x))$  вычислима, график  $f$  — это ее область значений.

$\impliedby$  Перечисляем график  $f$ , как только напечаталась пара  $(x, y)$ , выдаем  $y$ .

**Теорема.**  $f : M \rightarrow \mathbb{N}$  — вычислимая функция,  $S$  — перечислимо. Тогда 1)  $f(M \cap S)$  — перечислимо; 2)  $f^{-1}(S)$  — перечислимо.

**Доказательство.** 1)  $f|_{M \cap S}$  — вычислима,  $f(M \cap S)$  — это множество значений  $f|_{M \cap S}$ .

2) Параллельно перечисляем  $S$  и график  $f$ , как только нашлись  $(x, y)$  из графика, а  $y \in S$ , печатаем  $x$ .

## Перечислимые — проекции разрешимых

**Теорема.** Множество  $S$  — перечислимо  $\iff \exists$  разрешимое множество пар  $B$ , что  $S = \{x \in \mathbb{N} \mid \exists y : (x, y) \in B\}$ .

**Доказательство.**  $\Leftarrow$  Полуразрешающий алгоритм:

- 1 Вход:  $x$ .
- 2 Перебираем все  $y \in \{0, 1, 2, 3, \dots\}$ , если  $(x, y) \in B$ , то выдать 1.

$\Rightarrow$  Пусть  $\mathcal{A}$  — это полуразрешающий алгоритм для  $S$ .  
Определим  $B = \{(x, k) \mid \mathcal{A}(x) \text{ останавливается ровно за } k \text{ шагов}\}$ .

## Вопросы

- Существуют ли неразрешимые множества?
  - Да: алгоритмов счетное число, а подмножеств континуум.
  - **Неконструктивное доказательство**
- Существуют ли неперечислимые множества?
  - Да: алгоритмов счетное число, а подмножеств континуум.
- Существуют ли перечислимые неразрешимые множества?

## Универсальный алгоритм

- Каждому алгоритму соответствует строка — его текст.
- Все строки можно перенумеровать в алфавитном порядке: каждый алгоритм получает номер.
- $\#A$  — номер алгоритма  $A$
- $\langle n \rangle$  — алгоритм с номером  $n$ .
- Универсальный алгоритм  $\mathcal{U}(n, x) = \langle n \rangle (x)$

## Диагональная функция

- $\#A$  — номер алгоритма  $A$ ,  $\langle n \rangle$  — алгоритм с номером  $n$ .
- Универсальный алгоритм  $\mathcal{U}(n, x) = \langle n \rangle(x)$
- $u(n) = \mathcal{U}(n, n)$  — диагональная функция.
- $u(n)$  — вычислимая функция.
- $u(n)$  определено не для всех  $n$ .
- **Лемма.**  $u(n)$  нельзя доопределить до всюду определенной вычислимой функции.

### Доказательство.

- Пусть  $u'(n)$  — всюду определенное вычислимое дополнение  $u(n)$ .
- $d(n) = u'(n) + 1$  — всюду определенная вычислимая функция.
- $u(\#d) = d(\#d) = u'(\#d) + 1 = u(\#d) + 1$ .

## Перечислимое неразрешимое множество

- Область определения  $u(n)$  — перечислимое множество.
- Область определения  $u(n)$  — неразрешимое множество.
- $W = \{n \mid \langle n \rangle (n) \text{ останавливается} \}$ .
- $\mathbb{N} \setminus W$  — неперечислимое множество.
- $\{(n, x) \mid \langle n \rangle (x) \text{ останавливается} \}$  — неразрешимое множество.
- $\{n \mid \langle n \rangle (0) \text{ останавливается} \}$  — неразрешимое множество.

## Задача об остановке алгоритма

- Допустим, что все же существует алгоритм, который определяет, останавливается ли данный алгоритм на данном входе.
- Тогда можно было бы доказать Великую теорему Ферма так:
- Алгоритм:
  - ① Перебрать все  $x, y, z, n \in \{1, 2, 3, \dots\}$ ,  $n > 2$
  - ② Остановиться, если  $x^n + y^n = z^n$ .
- Узнаем, останавливается ли этот алгоритм на пустом входе.

## Вычислимое вещественное число

**Определение.**  $\alpha \in \mathbb{R}$  называется вычислимым вещественным числом, если существует пара всюду останавливающихся алгоритмов:

- Основа:  $\mathcal{A}(n)$  — сходящаяся последовательность рациональных чисел,  $\lim_{n \rightarrow \infty} \mathcal{A}(n) = \alpha$ .
- Регулятор сходимости:  $\mathcal{B}$ . Для всех  $n > \mathcal{B}(k)$  выполняется  $|\mathcal{A}(n) - \alpha| < \frac{1}{2^k}$ .
- Существует последовательность  $0 \leq a(n) \leq 1$ .
- $a(n) \in \mathbb{Q}$ ,  $a(n)$  возрастает.
- $a(n)$  — вычислима.
- $\lim_{n \rightarrow \infty} a(n)$  не является вычислимым числом.

## Последовательность Шпеккера

- Пусть  $W$  — это перечислимое неразрешимое множество.
- Пусть алгоритм  $\mathcal{A}$  печатает все элементы  $W$  без повторений.
- Алгоритм  $\mathcal{B}(k)$  выдает элемент, который печатает  $\mathcal{A}$  на  $k$ -м месте.
- $\mathcal{C}(n) = \sum_{k=1}^n \frac{1}{2^{\mathcal{B}(k)}}$ .
- $\alpha = 0.110110001\dots$
- $k$ -я цифра  $\alpha$  равна 1  $\iff k \in W$ .

## Задачи

- 1 Докажите, что всякое бесконечное перечислимое множество содержит бесконечное разрешимое подмножество.
- 2 Докажите, что непустое подмножество натуральных чисел разрешимо тогда и только тогда, когда оно есть множество значений всюду определенной неубывающей вычислимой функции с натуральными аргументами и значениями.
- 3 Приведите пример неразрешимого подмножества  $\mathbb{N} \times \mathbb{N}$ , такого что все его горизонтальные и вертикальные сечения (т.е. пересечения с  $\mathbb{N} \times \{x\}$  и с  $\{x\} \times \mathbb{N}$ ) разрешимы.
- 4 Постройте множество, которое не является перечислимым и его дополнение тоже не является перечислимым.
- 5 Докажите, что вещественное число  $\alpha$  является вычислимым тогда и только тогда, когда множества  $\{x \in \mathbb{Q} \mid x < \alpha\}$  и  $\{x \in \mathbb{Q} \mid x > \alpha\}$  являются разрешимыми.