

# Элементы теории алгоритмов

§ 34. Уточнение понятия алгоритма

§ 35. Алгоритмически неразрешимые задачи

§ 36. Сложность вычислений

§ 37. Доказательство правильности программ

# Элементы теории алгоритмов

## § 34. Уточнение понятия алгоритма

# Зачем уточнять определение?

Алгоритм – точный **набор инструкций** для **исполнителя**.



Всегда ли существует алгоритм?

**Конструктивное доказательство**: построить алгоритм.



А если не удалось?

- задача о квадратуре круга
- задача о трисекции угла
- задача об удвоении куба
- вечный двигатель
- ...

нестрогие  
понятия



Как доказать, что алгоритма не существует?

# Зачем уточнять определение?

---

*Задача:* алгоритм как математический объект.

**Теория алгоритмов** (1930-е):

- доказательство алгоритмической неразрешимости задач
- анализ сложности алгоритмов
- сравнительная оценка качества алгоритмов



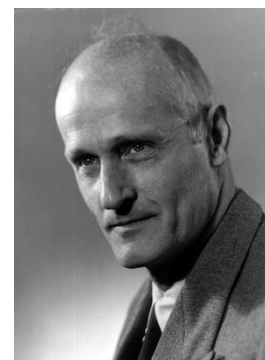
А. Тьюринг



Э. Пост



А. Чёрч



С. Клини



А. Марков

# Что такое алгоритм?

---

Первые алгоритмы – правила арифметических действий:

- объекты – числа
- шаги – операции с однозначными числами



Что считать шагом?

Все объекты можно закодировать как символьные строки:



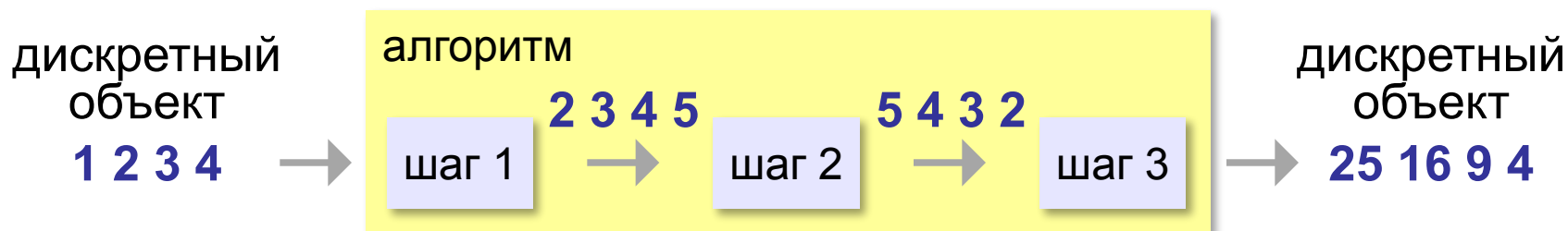
Можно рассматривать только алгоритмы обработки **строк**!

Из любого кода можно перевести в двоичный:



Можно рассматривать только алгоритмы обработки **битовых** строк!

# Как работает алгоритм?



- получает на вход дискретный объект
- в результате строит другой дискретный объект (или выдаёт сообщение об ошибке)
- обрабатывает объект по шагам
- на каждом шаге получается новый дискретный объект

# Как работает алгоритм?



Любой алгоритм определяет функцию!

т.е. правило преобразования входа в выход

Функция не определена  $\Leftrightarrow$  алгоритм зацикливается или завершается аварийно.

ввод  $a, b$   
вывод  $a * \text{sqrt}(b)$

→  $\times b < 0$

ввод  $a$   
нц пока да  
кц

→  $\times$  для всех  $a$

# Эквивалентные алгоритмы

---

Задают одну и ту же функцию:

если  $a < b$  то

$M := a$

иначе

$M := b$

все



$M := b$

если  $a < b$  то

$M := a$

все



# Универсальные исполнители

---

Алгоритм привязан к исполнителю  $\Rightarrow$  идея: построить универсального исполнителя.

Для любого алгоритма для любого исполнителя можно построить эквивалентный алгоритм для **универсального исполнителя**.

- если есть алгоритм для универсального исполнителя, то задача разрешима
- если доказано, что нет алгоритма для универсального исполнителя, задача неразрешима



Любой алгоритм может быть представлен как программа для универсального исполнителя!

# Универсальные исполнители

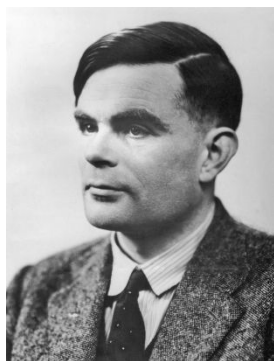
**Алгоритм** – это программа для универсального исполнителя.

## **Модель вычислений:**

- *«процессор»* (система команд и способ их выполнения)
- *«память»* (способ хранения данных)
- *язык программирования* (способ записи программ);
- *способ ввода* данных
- *способ вывода* результата

# Универсальные исполнители

---



А. Тьюринг

**машина  
Тьюринга**



Э. Пост

**машина  
Поста**



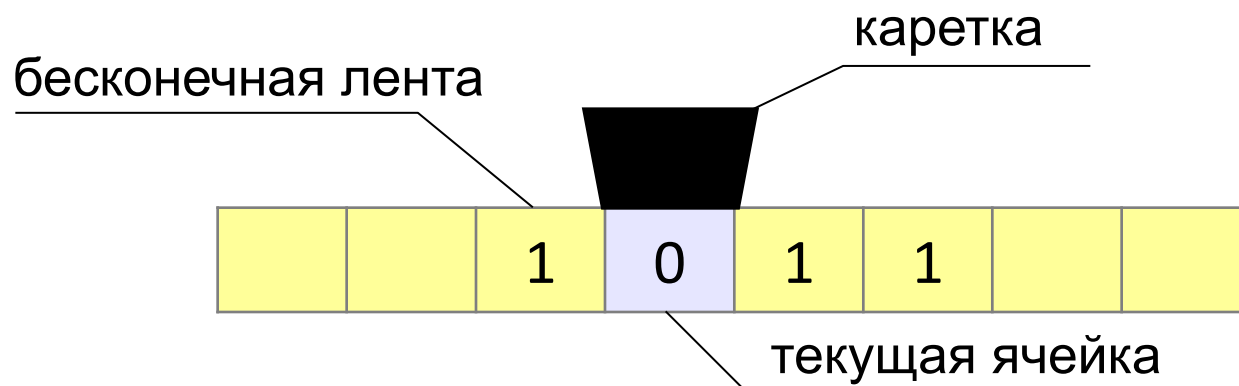
А. Марков

**нормальные  
алгоритмы  
Маркова**



Все универсальные исполнители эквивалентны!

# Машина Тьюринга



А. Тьюринг

- бесконечная лента («**память**»)
- каретка (**запись и чтение**)
- программируемый автомат («**процессор**»)

**алфавит:**  $A = \{a_1, a_2, \dots, a_N\}$        $A = \{0, 1, \square\}$

пробел

# Что такое автомат?

**Автомат** – это устройство, работающее без участия человека.

**Состояние** – промежуточная задача, которую решает автомат.

$$Q = \{q_1, q_2, \dots, q_M\}$$

начальное  
состояние

$q_0$  – остановка автомата

# Программа для машины Тьюринга

**Программа** состоит из команд:

- записать символ  $a_i$  в текущую ячейку
- переместить каретку  $\rightarrow \leftarrow$  • (не перемещать)
- перейти в состояние  $q_j$

$$A = \{0, 1, \square\}$$

$$1 \rightarrow q_1$$

- записать 1
- переместиться вправо
- перейти в состояние  $q_1$

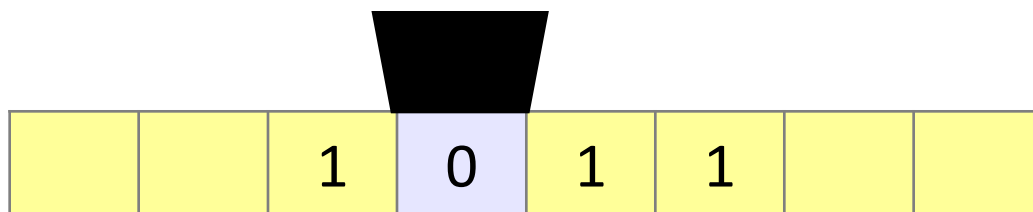
$$0 \cdot q_0$$

- записать 0
- не перемещать каретку
- останов ( $q_0$ )

# Программа для машины Тьюринга

**Задача.** На ленте записано число в двоичной системе счисления. Каретка находится где-то над числом. Требуется увеличить число на единицу.

**алфавит:**  $A = \{0, 1, \square\}$



**СОСТОЯНИЯ:**  $q_1$  – поиск правого конца слова

подзадачи  $q_2$  – увеличение числа на 1

# Программа для машины Тьюринга

$q_1$  : поиск конца слова

- если 0, то  $\rightarrow$
- если 1, то  $\rightarrow$
- если  $\square$ , то  $\leftarrow$  и **переход в  $q_2$**

ТОЛЬКО  
изменения!

	$q_1$
0	$\rightarrow$
1	$\rightarrow$
$\square$	$\leftarrow q_2$

$q_2$  : увеличение числа на 1

- если 0, то записать 1 и стоп ( $q_0$ )
- если 1, то записать 0 и  $\leftarrow$
- если  $\square$ , то записать 1 и стоп ( $q_0$ )

	$q_2$
0	1 • $q_0$
1	0 $\leftarrow$
$\square$	1 • $q_0$



Как объединить две программы?



# Программа для машины Тьюринга

	$q_1$		$q_2$
0	→	0	1
1	→	1	0
□	← $q_2$	□	1 • $q_0$

Связь подзадач через ячейку (□,  $q_1$ )!

Если алгоритмы А и Б можно запрограммировать на машине Тьюринга, то и любую их комбинацию тоже можно запрограммировать.

**Тезис Чёрча-Тьюринга:** Любой алгоритм (в интуитивном смысле этого слова) может быть представлен как программа для машины Тьюринга.

# Программа для машины Тьюринга

начальное  
состояние

новая  
метка

переход

НОВОЕ  
СОСТОЯНИЕ

( 0,  $q_1$ , 0,  $\rightarrow$ ,  $q_1$  )

( 1,  $q_1$ , 1,  $\rightarrow$ ,  $q_1$  )

(  $\square$ ,  $q_1$ ,  $\square$ ,  $\leftarrow$ ,  $q_2$  )

( 0,  $q_2$ , 1,  $\bullet$ ,  $q_0$  )

( 1,  $q_2$ , 0,  $\leftarrow$ ,  $q_2$  )

(  $\square$ ,  $q_2$ , 1,  $\bullet$ ,  $q_0$  )

	$q_1$
0	$0 \rightarrow q_1$
1	
$\square$	

	$q_2$
0	$1 \bullet q_0$
1	$0 \leftarrow q_2$
$\square$	$1 \bullet q_0$

# Программы для машины Тьюринга

	$q_1$
0	←
1	←
□	→ $q_0$

	$q_1$
0	→ $q_0$
1	→ $q_0$
□	←

	$q_1$	$q_2$
0	$q_2$	□ ←
1	$q_2$	□ ←
□	←	$q_0$

**?** Что делает программа?

**?** Когда зацикливается?

# Программы для машины Тьюринга

---

*Задача 1.* Уменьшить двоичное число на 1.

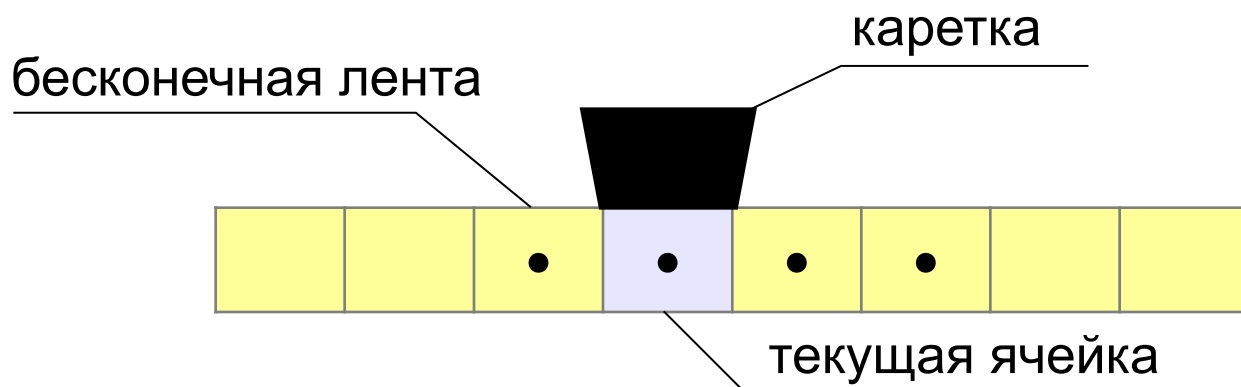
*Задача 2.* Увеличить на единицу число, записанное в десятичной системе счисления.

*Задача 3.* Уменьшить на единицу число, записанное в десятичной системе счисления.

*Задача 4.* Сложить два числа в двоичной системе, разделенные на ленте знаком «+».

*Задача 5.* Сложить два числа в десятичной системе, разделенные на ленте знаком «+».

# Машина Поста



Э. Пост

**!** Алфавит сокращён до двух символов!

- ← переместить каретку на 1 ячейку влево
- переместить каретку на 1 ячейку вправо
- 0** стереть метку в рабочей ячейке (записать **0**)
- 1** поставить метку в рабочей ячейке (записать **1**)
- ?  $n_0, n_1$  если в рабочей ячейке нет метки, перейти к строке  $n_0$ , иначе перейти к строке  $n_1$
- стоп** остановить машину

# Программа для машины Поста

1. ←
2. ? 1, 3
3. стоп

**?** Что делает?  
Зацикливается?

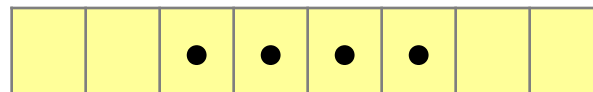
команда с переходом

← 3

строки  
нумеруются

сдвинуть каретку влево  
и перейти на строку 3

**?** Как записывать числа?



4 в унарной системе!

**!** Машины Поста и Тьюринга эквивалентны!

# Программы для машины Поста

1	1
2	→
3	→ 1

1	←
2	? 3, 4
3	1 1
4	стоп

1	? 2, 3
2	1 4
3	→ 1
4	стоп

**?** Что делает программа?

**?** При каких состояниях ленты?

## Программы для машины Поста

---

*Задача 1.* Напишите программу для машины Поста, которая увеличивает (уменьшает) число в единичной системе счисления на единицу. Каретка расположена слева от числа.

*Задача 2.* Напишите программу для машины Поста, которая складывает два числа в единичной системе счисления. Каретка расположена над пробелом, разделяющим эти числа на ленте.



# Нормальные алгоритмы Маркова (НАМ)

**НАМ** – правила обработки символьных строк с помощью подстановок.



А. Марков

**а** → **н**  
**ух** → **ло**  
**м** → **с**

**муха** → **мухн** → **млон** → **слон**

→ **0**

добавить 0 в начало строки

**о** → **а**

заменить и стоп



Корова → ?

**Ка**рова

# Нормальные алгоритмы Маркова (НАМ)

*Задача.* Удалить из строки, состоящей из букв  $a$  и  $b$ , первый символ. Например, строка  $abba$  должна бы преобразована в  $bba$ .

«Очевидное» решение:

~~$a \rightarrow \cdot$~~   
 ~~$b \rightarrow \cdot$~~



Что плохо?

~~$b \rightarrow \cdot$~~   
 ~~$a \rightarrow \cdot$~~

Правильное решение:

маркер

$*a \rightarrow \cdot$   
 $*b \rightarrow \cdot$   
 $\rightarrow *$

$abba$

$baab$

$*abba$

$*baab$

$bba$

$aab$



НАМ, машины Поста и Тьюринга эквивалентны!

# Нормальные алгоритмы Маркова

алфавит:  $A = \{0, 1\}$

$0 \rightarrow 00$

$1 \rightarrow 11$

$*0 \rightarrow 0*$

$*1 \rightarrow 1*$

$* \rightarrow =.$

$\rightarrow *$

$*0 \rightarrow 00*$

$*1 \rightarrow 11*$

$* \rightarrow .$

$\rightarrow *$



Что делает НАМ?

# Нормальные алгоритмы Маркова

---

*Задача 1.* Напишите НАМ, который «сортирует» цифры двоичного числа так, чтобы сначала стояли все нули, а потом – все единицы.

*Задача 2.* Напишите НАМ, который удаляет последний символ строки, состоящей из цифр 0 и 1. Какую операцию он выполняет, если рассматривать строку как двоичную запись числа?

*Задача 3.* Напишите НАМ, который умножает двоичное число на 2, добавляя 0 в конец записи числа.

# Элементы теории алгоритмов

## § 35. Алгоритмически неразрешимые задачи

# Вычислимые функции



Любой алгоритм определяет функцию!

т.е. правило преобразования входа в выход

**Вычислимая функция** – это функция, для вычисления которой существует алгоритм.

может задаваться разными алгоритмами:

**а** → **0**

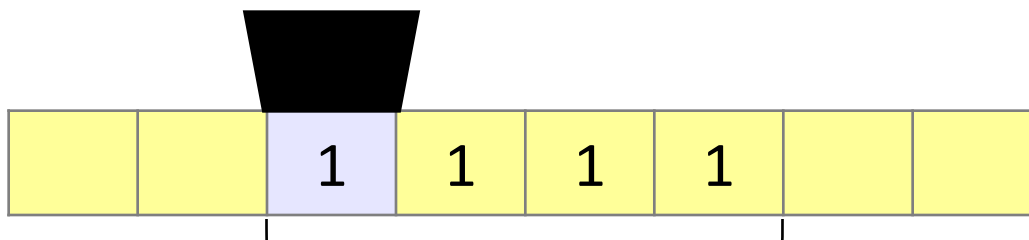
**б** → **1**

**б** → **1**

**а** → **0**

# Вычислимые функции

$$f(n) = \begin{cases} 1, & \text{если } n \text{ – чётное} \\ 0, & \text{если } n \text{ – нечётное} \end{cases}$$



в унарной системе счисления

	$q_1$	$q_2$	$q_3$	$q_4$
1	$\rightarrow q_2$	$\rightarrow q_1$	$\leftarrow q_4$	$\square \leftarrow$
$\square$	$\leftarrow q_3$	$\leftarrow q_4$		$q_0$

- $q_1$  – чётное число единиц
- $q_2$  – нечётное число единиц
- $q_3$  – оставить 1 единицу
- $q_4$  – стереть все единицы



Почему пусто?

# Вычислимые функции

$$f(n) = \begin{cases} 1, & \text{если } n \text{ – чётное} \\ 0, & \text{если } n \text{ – нечётное} \end{cases}$$

11 → ""  
1 → .  
→ 1.

**?** Как написать НАМ?

Пример (В.А. Успенский):

$$h(n) = \begin{cases} 1, & \text{если в записи числа } \pi \text{ есть } n \text{ стоящих подряд} \\ & \text{девяток в окружении других цифр} \\ 0, & \text{если такой цепочки нет} \end{cases}$$

перебор 800 знаков:

$$h(n) = 1 \text{ для } n = 1, 2, 6.$$

**!** Если  $h(n)=0$ , перебор не остановится!

**Вычислимость неизвестна!**

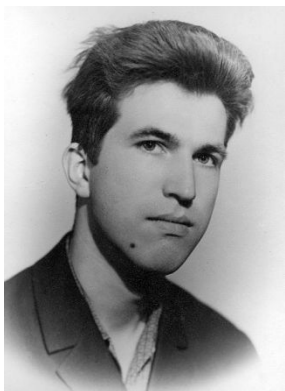


# Алгоритмически неразрешимые задачи

**Алгоритмически неразрешимая задача** – это задача, соответствующая невычислимой функции.

⇒ общего решения задачи нет, его бесполезно искать!

**10-я проблема Гильберта** (1900): найти метод, который позволяет определить, имеет ли заданное алгебраическое уравнение с целыми коэффициентами решение в целых числах.



Ю.В. Матиясевич

$$x^2 + y^3 + 2 = 0 \quad \Rightarrow (5; -3) \text{ и } (-5; -3)$$



1970: общего алгоритма **нет!**

# Алгоритмически неразрешимые задачи

**Г.В. Лейбниц, XVII в.:** разработать алгоритм, позволяющий установить, можно ли вывести формулу Б из формулы А в рамках заданной системы аксиом («*проблема распознавания выводимости*»).



1936: в общем виде задача **неразрешима!**



удалось получить отрицательные результаты



А. Чёрч

# Алгоритмически неразрешимые задачи

---

**Проблема останова:** по тексту любой программы  $P$  и ее входным данным  $X$  определяет, завершается ли программа  $P$  при входе  $X$  за конечное число шагов или закликивается.

**Проблема эквивалентности:** по двум заданным алгоритмам определить, будут ли они выдавать одинаковые результаты для любых допустимых исходных данных.



Невозможно полностью автоматизировать отладку программ!

# Элементы теории алгоритмов

## § 36. Сложность вычислений

# Что такое сложность вычислений?

## Задачи теории алгоритмов:

- существует ли алгоритм решения задачи?
- можно ли им воспользоваться?

## Шахматы:

- алгоритм существует (конечное число позиций)
- полный перебор нереален

## Требования к алгоритму:

- быстродействие
- минимальный расход  
памяти

временная  
сложность

пространственная  
сложность



Обычно эти требования противоречивы!

# Временная сложность

$T$  – количество элементарных операций универсального исполнителя (компьютера)



$T$  зависит от размера входных данных  $n$ !

Временная сложность алгоритма – функция  $T(n)$ .

*Задача 1.* Вычислить сумму первых трёх элементов массива (при  $n \geq 3$ ).

```
Sum := A[1] + A[2] + A[3]
```

$$T(n) = 3$$

2 сложения  
+ запись в  
память

*Задача 2.* Вычислить сумму всех элементов массива.

```
Sum := 0
нц для i от 1 до n
    Sum := Sum + A[i]
кц
```

$$T(n) = 2n + 1$$

$n$  сложений,  $n+1$   
операций записи

# Временная сложность

Задача 3. Отсортировать все элементы массива по возрастанию методом выбора.

```
нц для i от 1 до n-1
  nMin := i;
  нц для j от i+1 до n
    если A[i] < A[nMin] то nMin := j все
  кц
  если nMin <> i то
    c := A[i]; A[i] := A[nMin]; A[nMin] := c
  все
кц
```

Число сравнений:  $T_c(n) = (n-1) + (n-2) + \dots + 2 + 1 = \frac{n(n-1)}{2} = \frac{1}{2}n^2 - \frac{1}{2}n$

Число перестановок:  $T_p(n) \leq n-1$

зависит от  
данных

# Сравнение алгоритмов по сложности

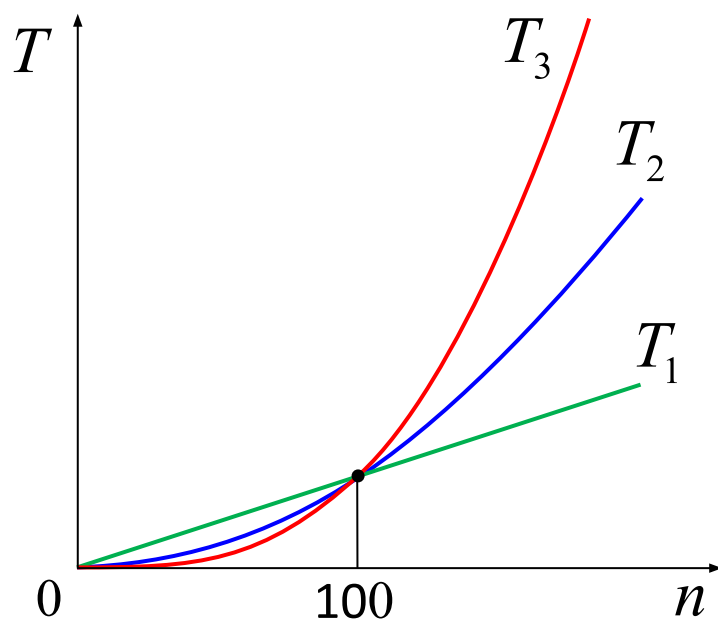
$$T_1(n) = 10000 \cdot n$$

$$T_2(n) = 100 \cdot n^2$$

$$T_3(n) = n^3$$



Какой алгоритм выбрать?



при  $n < 100$ :

$$T_3(n) < T_2(n) < T_1(n)$$

при  $n > 100$ :

$$T_3(n) > T_2(n) > T_1(n)$$



Нужно знать размер данных!



# Асимптотическая сложность

**Асимптотическая сложность** – это оценка скорости роста количества операций при больших значениях  $N$ .

линейная

постоянная

сложность  $O(N)$   $\Leftrightarrow T(N) \leq c \cdot N$  для  $N \geq N_0$

сумма элементов массива:

$$T(N) = 2 \cdot N - 1 \leq 2 \cdot N \text{ для } N \geq 1 \Rightarrow$$

квадратичная

сложность  $O(N^2)$   $\Leftrightarrow T(N) \leq c \cdot N^2$  для  $N \geq N_0$

сортировка методом выбора:

$$T_c(N) = \frac{1}{2} N^2 - \frac{1}{2} N \leq \frac{1}{2} N^2 \text{ для } N \geq 0 \Rightarrow O(N^2)$$

# Асимптотическая сложность

кубическая

сложность  $O(N^3) \Leftrightarrow T(N) \leq c \cdot N^3$  для  $N \geq N_0$

сложность  $O(2^N)$

сложность  $O(N!)$

задачи оптимизации,  
полный перебор вариантов

**Факториал числа  $N$ :**  $N! = 1 \cdot 2 \cdot 3 \dots$

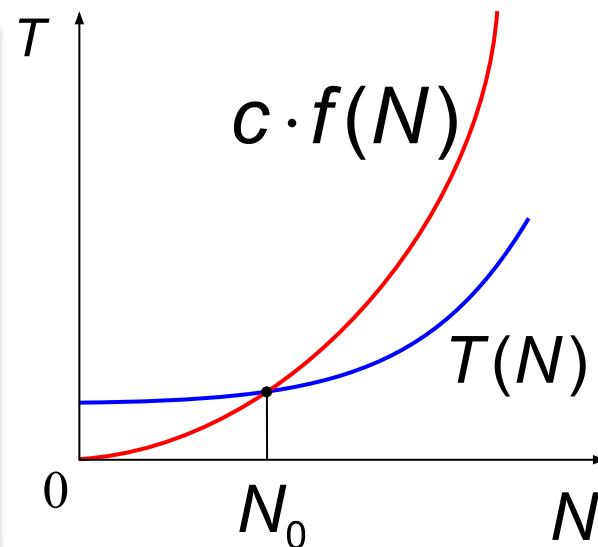
$N$	$T(N)$	время выполнения
	$N$	100 нс
	$N^2$	10 мс
	$N^3$	0,001 с
	$2^N$	$10^{13}$ лет

$N = 100,$   
1 млрд оп/с

# Асимптотическая сложность

Алгоритм относится к классу  $O(f(N))$ , если найдется такая постоянная  $c$ , что начиная с некоторого  $N = N_0$  выполняется условие

$$T(N) \leq c \cdot f(N)$$



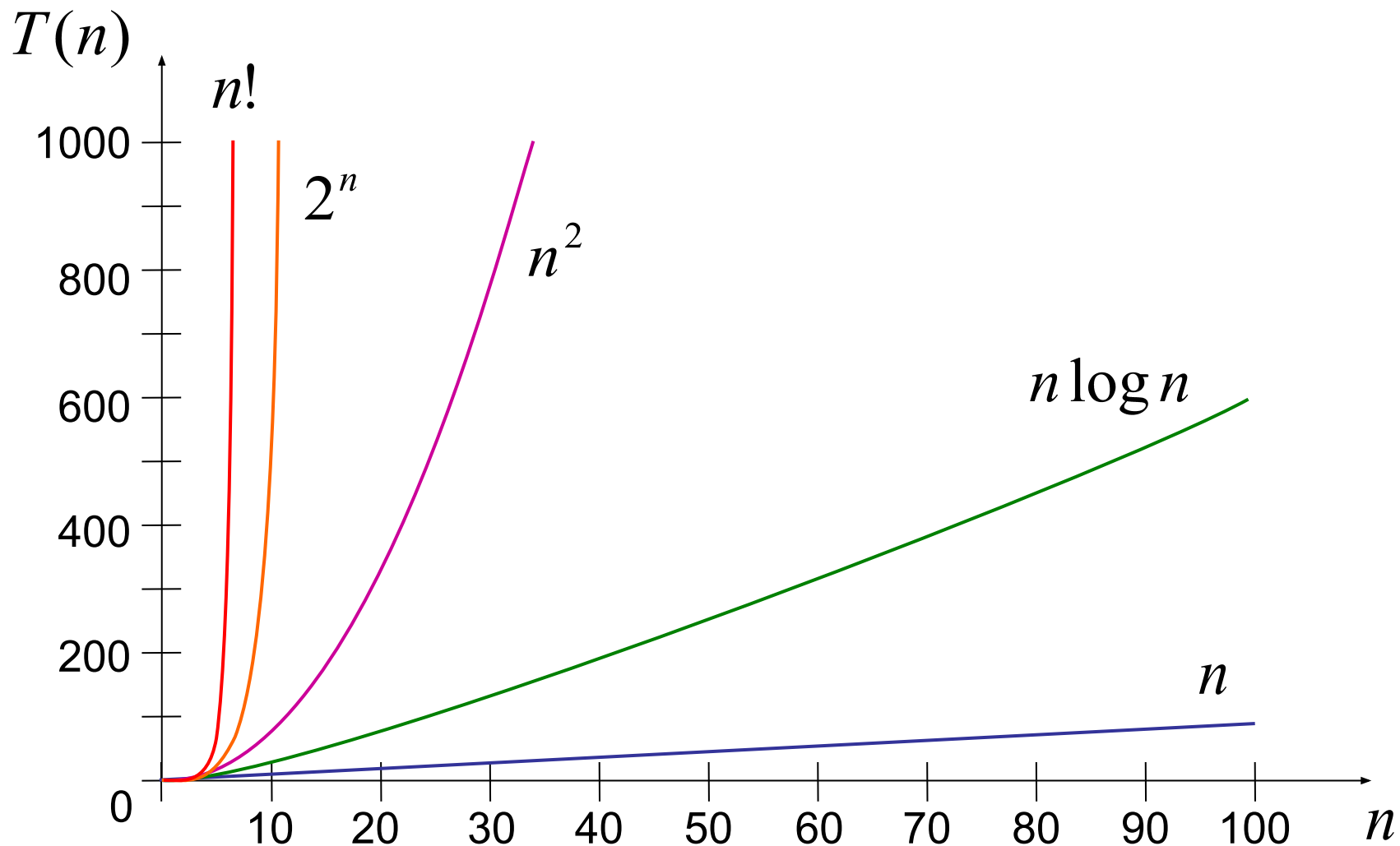
это верхняя оценка!

$$O(N) \Rightarrow O(N^2) \Rightarrow O(N^3) \Rightarrow O(2^N)$$

«Алгоритм имеет сложность  $O(N^2)$ ».

обычно — наиболее точная верхняя оценка!

# Асимптотическая сложность



# Алгоритмы поиска

## Линейный поиск

```
nX := 0
нц для i от 1 до n
  если A[i] = X то
    nX := i
  выход
все
кц
```



Сложность?

СЛОЖНОСТЬ  $O(n)$

# Алгоритмы поиска

## Двоичный поиск

```

L := 1; R := n + 1
нц пока L < R - 1
  c := div(L + R, 2)
  если X < A[c] то
    R := c
  иначе
    L := c
все
кц

```

**?** Какой алгоритм поиска лучше?

$$\log_2 n$$

$$n = 2^m$$

**?** Сколько шагов?

$$T(n) = m + 1$$

$$T(n) = \log_2 n + 1$$

СЛОЖНОСТЬ  $O(\log n)$

основание роли не играет

$$\log_a n = \frac{1}{\log_b a} \cdot \log_b n$$

# Алгоритмы сортировки

## Метод «пузырька»

```
нц для i от 1 до n-1
  нц для j от n-1 до i шаг -1
    если A[j] > A[j+1] то
      c := A[j]; A[j] := A[j+1]; A[j+1] := c;
    все
  кц
кц
```

сравнений:  $T_c(n) = (n-1) + (n-2) + \dots + 2 + 1 = \frac{n(n-1)}{2} = \frac{1}{2}n^2 - \frac{1}{2}n$

присваиваний при перестановках:

$$T_p(n) = 3 \cdot \frac{n(n-1)}{2} = \frac{3}{2}n^2 - \frac{3}{2}n$$

сложность  $O(n^2)$

# Алгоритмы сортировки

## Сортировка подсчётом

```
цел С[1:МАХ]
нц для і от 1 до МАХ
    С[і] := 0
кц
```

```
нц для і от 1 до  $n$ 
    С[А[і]] := С[А[і]] + 1
кц
```

```
к := 1
нц для і от 1 до МАХ
    нц для j от 1 до С[і]
        А[к] := і
        к := к + 1
    кц
кц
```



Все значения [1, МАХ]!

обнулить массив  
счётчиков

подсчитать, сколько  
каких чисел

заполнить массив  
заново

сложность  $O(n)$



За счёт чего?



# Алгоритмы сортировки



При использовании операций «сравнить» и «переставить» сложность не может быть меньше  $O(n \cdot \log n)$ !

**Сортировка слиянием** (*Merge sort*)

$O(n \cdot \log n)$

**Пирамидальная сортировка** (*Heap sort*)

$O(n \cdot \log n)$

**Быстрая сортировка** (*Quick sort*)

$n)$

в среднем  $O(n \cdot \log n)$

в худшем случае  $O(n^2)$

# Элементы теории алгоритмов

## § 37. Доказательство правильности программ

# Как доказать правильность программы?

**Тестирование** – проверка работы программы с помощью набора тестовых данных, для которых известен правильный результат.

**?** Может ли тестирование доказать правильность?

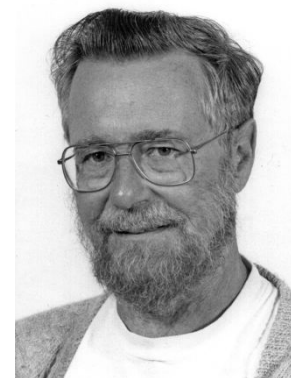
*«Отладка может показать лишь наличие ошибок и никогда их отсутствие».*

Поиск максимума из трёх:

если  $a > b$  то  $M := a$  иначе  $M := b$  все  
если  $b > c$  то  $M := b$  иначе  $M := c$  все

Тесты проходят:  $(a, b, c) = (1, 2, 3), (1, 3, 2), (2, 1, 3)$  и  $(2, 3, 1)$

**Тесты не проходят:**  $(3, 1, 2), (3, 2, 1)$



Э.В.  
Дейкстра

# Доказательное программирование

требования к  
входным данным



алгоритм



требования к  
результату

**ВХОД:**  $\mathbf{a} = a_0, \mathbf{b} = b_0$

$\mathbf{b} := \mathbf{a} + \mathbf{b}$

$\mathbf{b} = a_0 + b_0$

$\mathbf{a} := \mathbf{b} - \mathbf{a}$

$\mathbf{a} = a_0 + b_0 - a_0 = b_0$

$\mathbf{b} := \mathbf{b} - \mathbf{a}$

$\mathbf{b} = a_0 + b_0 - b_0 = a_0$

ДОКАЗАТЕЛЬСТВО

**ВЫХОД:**  $\mathbf{a} = b_0, \mathbf{b} = a_0$

если  $\mathbf{a} > \mathbf{b}$  то  $\mathbf{M} := \mathbf{a}$  иначе  $\mathbf{M} := \mathbf{b}$  все

если  $\mathbf{b} > \mathbf{c}$  то  $\mathbf{M} := \mathbf{b}$  иначе  $\mathbf{M} := \mathbf{c}$  все

$$M = \begin{cases} b, & b > c \\ c, & c \geq b \end{cases}$$

алгоритм  
неверный!

# Алгоритм Евклида

$a := m; b := n$

нц пока  $b \neq 0$

$r := \text{mod}(a, b)$

$a := b; b := r$

кц

вывод  $a$

$b = 0$

$$\text{НОД}(a, b) = \text{НОД}(m, n)$$

$$a = b \cdot p + r$$

$$\begin{aligned} \text{НОД}(a, b) &= \text{НОД}(b, r) \\ &= \text{НОД}(m, n) \end{aligned}$$

$$a = \text{НОД}(a, 0) = \text{НОД}(a, b) = \text{НОД}(m, n)$$

После любого шага цикла:

$\text{НОД}(a, b) = \text{НОД}(m, n)$  инвариант цикла

# Инвариант цикла

**Инвариант цикла** – это соотношение между значениями переменных, которое остается справедливым после завершения любого шага цикла.

*«Программиста бьют по рукам, если он посмеет написать оператор цикла, не найдя перед этим его инварианта».*



А.П. Ершов

# Инвариант цикла

## Сумма элементов массива:

```
Sum := 0
нц для i от 1 до n
    Sum := Sum + A[i]
кц
```

$$\text{Sum} = A[1] + A[2] + \dots + A[i]$$

## Поиск в массиве:

```
Min := A[1]
нц для i от 2 до n
    если A[i] < Min то
        Min := A[i]
    все
кц
```

$$\text{Min} = \min(A[1], A[2], \dots, A[i])$$

# Инвариант цикла

## Сортировка методом «пузырька»:

нц для  $i$  от 1 до  $n-1$

нц для  $j$  от  $n-1$  до  $i$  шаг  $-1$

если  $A[j] > A[j+1]$  то

$c := A[j]; A[j] := A[j+1]; A[j+1] := c;$

все

кц

кц

$i$ -й элемент по  
порядку стоит в  
позиции от  $i$  до  $j$

$i$  первых элементов  
установлены на свои места



# Быстрое возведение в степень $a^n = ?$

Задача – построить цикл с помощью инварианта.

**Правила:**

$$a^k = a^{k-1} \cdot a$$

при нечётных  $k$

$$a^k = (a^2)^{k/2}$$

при чётных  $k$

$$a^7 = a^6 \cdot [a]$$

$$a^n = b^k \cdot p \quad \leftarrow \text{инвариант}$$



Задача – свести  $k$  к нулю!

$$k = 0 \Rightarrow a^n = p$$

# Быстрое возведение в степень

```

b := a; k := n; p := 1
нц пока k <> 0
  если mod(k, 2) = 0 то
    k := div(k, 2)
    b := b*b
  иначе
    k := k-1
    p := b*p
все
кц
вывод p

```

$$a^n = b^k \cdot p$$

$$a^k = (a^2)^{k/2}$$

$$a^k = a^{k-1} \cdot a$$

$$a^n = b^k \cdot p$$



Как можно изменить начальные условия?

# Доказательное программирование

**Спецификация** – точная и полная формулировка задачи, содержащая информацию, необходимую для построения алгоритма её решения.



Ч.Э. Хоар

программа

$\{Q\} S \{R\}$

предусловие

постусловие

*«Если выполнение программы **S** началось в состоянии, удовлетворяющем **Q**, то гарантируется, что оно завершится через конечное время в состоянии, удовлетворяющем **R**».*

# Спецификации алгоритмов

---

## Алгоритм Евклида:

$$Q: m \geq n > 0$$

$$R: a = \text{НОД}(m, n)$$

## Суммирование элементов массива:

$$Q: n > 0$$

$$R: \text{Sum} = \sum_{i=1}^n A[i] = A[1] + A[2] + \dots + A[n]$$

**Корректная программа** – это программа, соответствующая спецификации.

**Надёжная программа** – это программа, которая корректна и, кроме того, не завершается аварийно при недопустимых входных данных.

# Доказательное программирование

---

## Правила преобразования:

- если  $\{Q\}S\{P\}$  и  $P \Rightarrow R$ , то  $\{Q\}S\{R\}$
- если  $R \Rightarrow Q$  и  $\{Q\}S\{P\}$ , то  $\{R\}S\{P\}$
- если  $\{Q\}S_1\{P\}$  и  $\{P\}S_2\{R\}$ , то  $\{Q\}S_1S_2\{R\}$
- ...

**Верификация** – доказательство правильности готовых программ (сложно!).



Проще сразу доказывать правильность отдельных блоков (циклов, процедур)!

# Конец фильма

---

**ПОЛЯКОВ Константин Юрьевич**

д.т.н., учитель информатики

ГБОУ СОШ № 163, г. Санкт-Петербург

[kpolyakov@mail.ru](mailto:kpolyakov@mail.ru)

**ЕРЕМИН Евгений Александрович**

к.ф.-м.н., доцент кафедры мультимедийной

дидактики и ИТО ПГГПУ, г. Пермь

[eremin@pspu.ac.ru](mailto:eremin@pspu.ac.ru)

# Источники иллюстраций

---

1. [en.wikipedia.org](http://en.wikipedia.org)
2. [ru.wikipedia.org](http://ru.wikipedia.org)
3. иллюстрации художников издательства «Бином»
4. авторские материалы