

ТЕОРИЯ АЛГОРИТМОВ

Основные понятия и определения теории алгоритмов

ПЛАН ЛЕКЦИИ

“ОСНОВНЫЕ ПОНЯТИЯ И ОПРЕДЕЛЕНИЯ ТЕОРИИ АЛГОРИТМОВ”

1. Представление алгоритмов на интуитивном уровне
2. Определения понятия “алгоритм”
3. Основные разделы теории алгоритмов
4. Математические приложения теории алгоритмов
5. Современные направления теории алгоритмов
6. Цели и задачи теории алгоритмов
7. Аспекты применения теории алгоритмов

1. Основные понятия и определения теории алгоритмов

1.1. Представление алгоритмов на интуитивном уровне (1)

Варка манной каши

- Взять 500 мл воды.
- Довести до кипения.
- Соль и сахар добавит по вкусу.
- Всыпать, помешивая, 100 Г манной крупы.
- Довести до кипения, периодически помешивая.
- Варить, помешивая, 10 минут.

Вычитания десятичных чисел

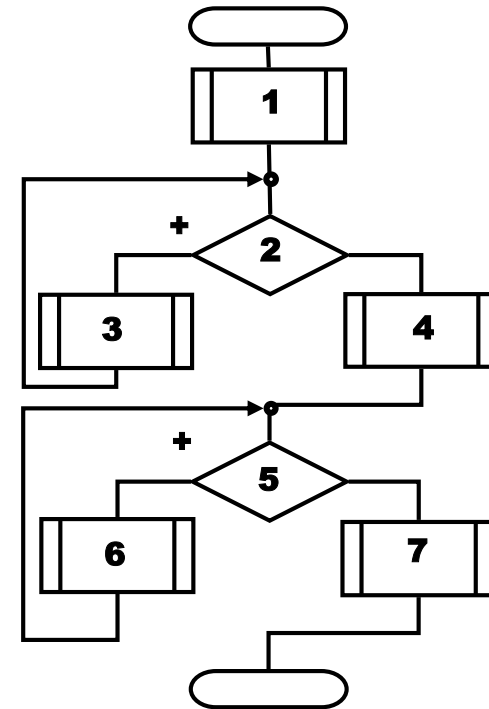
- Записать числа таким образом, чтобы запятые в записях уменьшаемого и вычитаемого оказались в одной позиции.
- Выровнять число разрядов в в записях, добавив, по необходимости нули в целые части слева, а в дробные части справа.
- Выполнить вычитание, так как вычитают натуральные числа
- Поставить запятую в записи результата на позицию, соответствующую позициям запятых уменьшаемого и вычитаемого.

1. Основные понятия и определения теории алгоритмов

1.1. Представление алгоритмов на интуитивном уровне (2)

Переход через двухполосную дорогу

1. Дойдите до ближайшего края дороги, остановитесь и посмотрите налево.
2. Транспортное средство в опасной близости?
3. Стойте и смотрите влево.
4. Дойдите до середины дороги, остановитесь и посмотрите направо.
5. Транспортное средство в опасной близости?
6. Стойте и смотрите вправо.
7. Идите прямо до края дороги



1. Основные понятия и определения теории алгоритмов

1.2. Определения понятия “алгоритм” (1)

*Дональд Эрвин Кнут (D.E. Knuth) обратил внимание на номограмму
ALGOriithm и LOGOrithm*

*Этимология слова “алгоритм” восходит к имени собственному
Abu Ja’far Mohamed ibn Mûsâ Khowârizmî*

*что буквально означает: “Отец Джафара, Магомет, сын Моисея, уроженец
Ховаризма (Хорезма)”*

Неформальное определение алгоритма

Алгоритм – набор систематических инструкций по выполнению *в строго определённом порядке* необходимых действий для решения *всех задач* какого-либо заданного класса.

Формализованное определение

Алгоритм – это заданное на некотором языке *конечное предписание*, задающее конечную последовательность выполнимых элементарных операций для решения задачи, *общее для класса* возможных исходных данных.

1. Основные понятия и определения теории алгоритмов

1.2. Определения понятия “алгоритм” (2)

Пусть D – область (множество) *исходных данных* задачи, а R – множество *возможных результатов*, тогда мы можем говорить, что алгоритм осуществляет отображение $D \rightarrow R$.

Алгоритм называется *частичным алгоритмом*, если предоставляет результат только для некоторых $d \in D$, и *полным алгоритмом*, если применение алгоритма даёт правильный результат для всех $d \in D$.

Определение алгоритма по А.Н. Колмогорову

Алгоритм – это всякая система вычислений, выполняемых по строго определенным правилам, которая после какого-либо числа шагов заведомо приводит к решению поставленной задачи.

Определение алгоритма по А.А. Маркову

Алгоритм – это точное предписание, определяющее вычислительный процесс, идущий от варьируемых исходных данных к искомому результату.

1. Основные понятия и определения теории алгоритмов

1.2. Определения понятия “алгоритм” (3)

Имеется множество формальных определений понятия “алгоритм”, которое связано со специальными математическими конструкциям: машина Поста(E.L Post), машина Тьюринга(A.M. Turing), рекурсивно-вычислимые функции Чёрча(A. Church).

При этом постулируется тезис об эквивалентности такого формализма и понятия “алгоритм”

Алгоритмической системой называется *общий способ задания* алгоритма.

1. Основные понятия и определения теории алгоритмов

1.3. Общие требования к алгоритму

Несмотря на множество различных определений понятия, имеет место ряд требований, предъявляемых к алгоритму.

Алгоритм должен:

- удовлетворять требованию конечности записи — содержать конечное количество элементарно выполнимых предписаний;
- удовлетворять требованию конечности действий — выполнять конечное количество шагов при решении задачи;
- удовлетворять требованию универсальности — быть единым для всех допустимых исходных данных;
- удовлетворять требованию правильности — приводить к правильному по отношению к поставленной задаче решению.

1. Основные понятия и определения теории алгоритмов

1.3. Основные разделы теории алгоритмов(1)

Объект исследования: алгоритмы.

Методы исследования: математическая логика, алгебраические системы, теория множеств, теория нумерации, комбинаторика, теория групп, математический анализ, теория абстрактных автоматов et c.

Результаты: позволяет пояснить ряд фундаментальных понятий – доказуемость, вычислимость, сложность и случайность.

Р А З Д Е Л Ы

1. Общие понятия и определения теории алгоритмов

Введены понятия:

- конструктивного объекта А.Н. Колмогоровым: слова в алфавите, матрицы, вектора, массивы, (Б, к)-деревья, комплексы (графы), ансамбли;
- итеративного процесса;
- локальной операции.

1. Основные понятия и определения теории алгоритмов

1.3. Основные разделы теории алгоритмов (2)

2. Теория представительных вычислительных моделей

В данном разделе изучают:

- машины А. Тьюринга;
- машины Э. Поста;
- машины А.Н Колмогорова;
- машины А.А. Маркова;
- машины А. Шёнхаге (A. Schönhage) и др.

3. Теория исчислений

Исчисление это список порождающих (разрешающих) правил или правил вывода, позволяющая осуществлять переходы от одного конструктивного объекта к другим конструктивным объектам.

Пример житейский: домино, шахматы, конструктивный объект — игровая позиция.

1. Основные понятия и определения теории алгоритмов

1.3. Основные разделы теории алгоритмов (3)

4. Теория представительных порождающих моделей

Формальные грамматики, нормальные алгоритмы Маркова.

5. Теория связей между алгоритмами и численными

6. Исследование временных и ёмкостных показателей сложности порождения и вычисления

Поскольку вычисления и порождения в физическом смысле характеризуются длительностью и объёмом, возникают *нормы* и *изоморфизм*.

7. Исследование вычислимых функций и породимых множеств

Рассматриваются разрешимые и перечислимые множества.

8. Исследование μ -рекурсивных функций

μ -рекурсивная функция совпадает по смыслу с вычислимой теоретико-числовой функцией, которая определяется как числовая функция, получаемая из фиксированного набора простейших исходных функций с помощью применения в произвольном порядке простейших операций, так же выбираемых из некоего фиксированного набора.

1. Основные понятия и определения теории алгоритмов

1.3. Основные разделы теории алгоритмов (4)

9. **Исследование возможностей арифметического и диофантова представления любого перечислимого множества**

Терм – выражение (арифметическое или полиномиальное) полином с натуральными коэффициентами и натуральными переменными.

Полиномиальное отношение определяется между двумя термами.

На базе полиномиальных отношений применением любого числа логических операций (объединения, пересечения, дополнения и проецирования) и кванторов выполняется построение арифметических отношений.

Если используются эксклюзивно кванторы существования или операции проецирования, то отношение называется *диофантовым* отношением.

1. Основные понятия и определения теории алгоритмов

1.3. Основные разделы теории алгоритмов (5)

10. Исследование возможностей построения неразрешимого породимого множества

Всякое множество, распознаваемое на конкретной вычислительной модели со временем, не большим T , и ёмкостью, не большей S , может быть порождено некой порождающей моделью, со временем и ёмкостью cT и cS соответственно, где c – константа, не зависящая от распознаваемого элемента.

Пусть задано исчисление Γ для выбранной порождающей модели. Тогда для задачи “по словам a , b и числу k определить, существует ли в Γ вывод b из a ($a \Rightarrow + b$), в котором длины всех промежуточных результатов не превосходят величины ck^2 , где c не зависит от a , b и k ”.

Сэвич В.Дж. (W.J. Savitch), доказал, что множество, порождаемое с ёмкостью S , можно распознать с ёмкостью S^2 .

Приложение – построение интерпретирующих автоматов.

Советские учёные Ю.Л. Ершов, Г.М. Корпелевич, О.Б. Лупанов показали, что существуют автоматы, при переходе на которых от порождения к распознаванию происходит экспоненциальный рост объёма числа состояний вычислительного устройства

1. Основные понятия и определения теории алгоритмов

1.3. Основные разделы теории алгоритмов (6)

11. Изучение проблемы сводимости Поста

Было замечено, что проблемы разрешения, заведомо нерешимые, сводятся, в некотором смысле, друг к другу.

Сводимость проблемы B к проблеме A означает, по Посту, наличие некоторого способа, который позволяет эффективно ответить на вопрос “ $Y \in Q?$ ”, пользуясь ответом “ $X \in P$ ”.

12. Изучение относительных алгоритмов

Последние называются ещё “алгоритмами с оракулом”. Вопросы взаимодействия процедур и функций

13. Исследование вычислимых операций

Изучение специальных способов задания операций и схем программ

1. Основные понятия и определения теории алгоритмов

1.3. Основные разделы теории алгоритмов (7)

14. Изучение программ как объекта вычисления и порождения

Исследуются:

- способы программирования;
- универсальные алгоритмы и универсальные функции;
- гёделевские модели;
- вычислительные структуры.

Гёделевость (К. Gödel) модели программирования означает, что имеется способ преобразования (трансляции) программ любого способа программирования в программы заданного способа программирования.

15. Теория нумерации

16. Теория инвариантности (машинной независимости) сложных вычислений

17. Теория сложности и энтропии конструктивных объектов

18. Теория вычислительных моделей

Служит базой для построения архитектуры вычислительных систем

1. Основные понятия и определения теории алгоритмов

1.4. Математические приложения теории алгоритмов (1)

1. Исследование массовых проблем

Алгоритмическая проблема – построение алгоритма с заданными свойствами.

Единичная проблема – состоит в требовании предъявить объект, который удовлетворяет определённым условиям, называемый решением проблемы.

Массовая проблема – состоит в серии (часто бесконечной) единичных проблем и требовании *решить все* эти проблемы.

Пример *единичной* проблемы:

Для уравнения $x^2 - x - 1 = 0$ найти рациональное приближение к корню с точностью 10^{-6} .

Пример *массовой* проблемы:

Для уравнения $x^2 - x - 1 = 0$ найти рациональное приближение к корню с точностью 10^{-n} при любом n .

1. Основные понятия и определения теории алгоритмов

1.4. Математические приложения теории алгоритмов (2)

Формулировка алгоритмической массовой проблемы:

- Породимое множество X – множество вопросов или единичных проблем.
- Породимое множество Y – множество ответов или единичных решений.
- Подмножество $E \subset X$ – ограничения на вопросы.
- Подмножество $R \subset X \otimes Y$ – отношение “вопрос – ответ”.
- Требуется: найти алгоритм из X в Y , преобразующий каждый вопрос $\alpha \in E$, в ответ $\beta \in Y$ со свойством $\langle \alpha, \beta \rangle \in R$.

Пример формулировки алгоритмической массовой проблемы

Для уравнения $a \cdot x^2 + b \cdot x + c = 0$ при любом натуральном значении n найти пару действительных рациональных корней с точностью до 10^{-n} .

$$X = \mathbb{N}^+ \otimes \mathbb{N}^3; Y = \mathbb{Q},$$

$$E = \{ \langle a, b, c, n \rangle \mid b^2 - 4 \cdot a \cdot c \}$$

$$R = \{ \langle \langle a, b, c, n \rangle, r \rangle \mid \text{abs}(r - x_0) < 10^{-n} \},$$

где \mathbb{N} – множество натуральных чисел, \mathbb{Q} – множество рациональных чисел

1. Основные понятия и определения теории алгоритмов

1.4. Математические приложения теории алгоритмов (3)

2. **Конструктивная семантика**

Лежит в основании теории компиляции программ

3. **Анализ формализованных языков логики и арифметики**

Лежит в основании предикатных языков

4. **Вычислительный анализ**

5. **Нумерованные структуры**

6. **Построение псевдослучайных последовательностей**

7. **Алгоритмический подход к понятию количества информации**

8. **Оценка сложности решения отдельных задач**

9. **Влияние на алгоритмическую практику**

- алгоритмы и возможности формализации;
- неалгоритмическое описание вычислимых функций (непроцедурные – ЛИСП);
- вычислительные и порождающие модели (конечные автоматы и формальные грамматики)

1. Основные понятия и определения теории алгоритмов

1.5. Современные направления теории алгоритмов

Ныне сформированы следующие отрасли теории алгоритмов

1. Классическая теория алгоритмов:

- формулировка задач в терминах формальных языков;
- понятие задачи разрешения, введение сложностных классов;
- исследование класса NP -полных задач.

2. Теория асимптотического анализа алгоритмов:

- критерии оценки алгоритмов;
- методы получения асимптотических оценок;
- асимптотический анализ трудоемкости или времени выполнения.

3. Теория практического анализа вычислительных алгоритмов

- получение явных функции трудоёмкости;
- интервальный анализ функций;
- построение практических критериев качества алгоритмов;
- методики выбора рациональных алгоритмов.

1. Основные понятия и определения теории алгоритмов

1.6. Цели и задачи теории алгоритмов

На современном этапе целями и задачами теории алгоритмов являются

- Дальнейшая формализация понятия “алгоритм” и исследование формальных алгоритмических систем;
- формальное доказательство алгоритмической неразрешимости ряда задач;
- классификация задач, определение и исследование сложностных классов;
- асимптотический анализ сложности алгоритмов;
- исследование и анализ рекурсивных алгоритмов;
- получение явных функций трудоёмкости в целях сравнительного анализа алгоритмов;
- разработка критериев сравнительной оценки качества алгоритмов.

1. Основные понятия и определения теории алгоритмов

1.7. Аспекты применения теории алгоритмов (1)

Теоретический аспект теории алгоритмов позволяет

- определить алгоритмическую разрешимость задачи;
- определить возможность сведения алгоритмически неразрешимых задач к задаче останова машины Тьюринга;
- определить для алгоритмической разрешимой задачи – факт принадлежности этой задачи к классу NP –полных задач;
- оценить для члена класса NP –полных задач временных затрат для получения точного решения для больших размерностей исходных данных.

1. Основные понятия и определения теории алгоритмов

1.7. Аспекты применения теории алгоритмов (2)

Практический аспект, основывающийся на разделах асимптотического и практического анализа позволяют осуществить:

- рациональный выбор из известного множества алгоритмов решения данной задачи с учетом особенностей их применения (например, при ограничениях на размерность исходных данных или объема дополнительной памяти);
- получение временных оценок решения сложных задач;
- получение достоверных оценок невозможности решения некоторой задачи за определенное время, что важно для криптографических методов;
- разработку и совершенствование эффективных алгоритмов решения задач в области обработки информации на основе практического анализа.