Программа курса

«Основные алгоритмы»

ФУПМ. 2022 г.

Содержание

1 Введение. Верхние и нижние оценки сложности алгоритмов, жадные алгоритмы

Литература: [ДПВ12; 05; КЛР02; Шен04; КФ12]

1. Язык Си как исполнители алгоритмов.
2. Сложность по времени и по памяти. Верхние и нижние оценки. Примеры:
   - Задача о поиске максимума последовательности: верхняя и нижняя оценки (последняя — через связность графа)
   - Проверка числа n на простоту перебором делителей до $\sqrt{n}$ — экспоненциальный алгоритм (сложность измеряется по длине входа.).
3. [Краткий повтор] O, Ω, Θ обозначения — формальные определения.
   - $f(n) = \Theta(g(n))$ — отношение эквивалентности.
   - Если $P(n)$ — многочлен степени k, то $P(n) = \Theta(n^k)$.
   - Сумма чисел от 1 до n есть $\Theta(n^2)$.
   - $1^k + 2^k + \ldots + n^k = \Theta(n^{k+1})$.
   - Оценка суммы через интеграл (без доказательства).
4. Пример: задача о поиске треугольника максимальной площади, сторона которого лежит на оси Ox.
5. Жадные алгоритмы и индуктивные функции [Шен04].
   - функции максимума и суммы — индуктивные
   - индуктивное расширение на примере поиска максимума произведения
6. Онлайн-алгоритмы
7. Поиск максимального числа попарно непересекающихся отрезков

* Жадный алгоритм для 2-приближённого алгоритма для дискретной задачи о рюкзаке [КФ12].

2 Рекурсия и итерация.

Литература: [ДПВ12; Шен04]

Переход от алгоритмов, заданных рекурсивно, к алгоритмам, заданным итеративно, с использованием стека на примере алгоритма Евклида.

План лекции

- Расширенный алгоритм Евклида
- Алгоритм быстрого возведения в степень
- Числа Фибоначчи. Вычисление через
  - рекурсию
  - рекурсию с запоминанием
  - итерацию
  - возведение матрицы в степень
- Доказательство нижних оценок на время работы алгоритма Евклида через числа Фибоначчи.

3 Алгоритмы «разделяй и властвуй»

Литература: [ДПВ12; 05; КЛР02]

Деревья рекурсии. Доказательство Θ-оценок для алгоритмов:

- Алгоритм Карацубы
- Сортировка слиянием (быстрый повтор)
- Поиск k-ой порядковой статистики (детерминированный алгоритм)
- Алгоритм деления целых чисел (Divide, раздел 1.1 [ДПВ12])

Анализ рекуррентных соотношений. Доказательство основной теоремы о рекурсии

4 Дискретное преобразование Фурье

- ДПФ и БПФ
- Обратное преобразование, быстрое умножение многочленов
- Поиск вхождения паттерна в текст (Wildcard matching) с помощью многочленов
- ДПФ для обработки сигналов
- Итеративная схема вычисления БПФ

На семинар

- БПФ для многочленов над конечными полями

5 Нижние оценки

Литература: [05; КЛР02; 18]

Сортировки сравнениями. Модель разрешающих деревьев, доказательство нижних оценок.

План лекции

- Доказательство оценки $\Omega(n \log n)$ для сортировок сравнениями.
- Бинарный поиск. Нижняя оценка на поиск элемента в отсортированном массиве.
- Задача поиска $F^{-1}(x)$ для монотонной функции.
- Потенциальные функции. Нижняя оценка на поиск второго максимума в массиве.
- Быстрая сортировка (детерминированный алгоритм).
- Вероятностный алгоритм поиска k-ой порядковой статистики.
- Сортировка за линейное время.

  - Поразрядная сортировка (Radix sort)
  * Сортировка подсчётами

6 Вероятность-1

Литература: [18]

План лекции

- Элементарная теория вероятностей: определения
  - Пространство элементарных исходов U
  - Событие $A \subseteq U$
  - Функция вероятности
- Модель последовательного выбора
- Формула для объединения (ФВИ, без доказательства)
- Условная вероятность
  - Независимые события
  - Закон полной вероятности
  - Формула Байеса
  - Доказательство формулы Эйлера $\phi(n) = \prod_{p|n}(1 - \frac{1}{p})$ через вероятность

7 Вероятность-2

Литература: [18]

- Случайная величина
- Математическое ожидание: два определения
- Техника работы с индикаторными случайными величинами
  - Оценка времени работы быстрой сортировки
- Вероятностный метод: максимум не меньше среднего
  - В графе есть разрез, в который входит хотя бы половина рёбер
- Неравенство Маркова
  - Приложение к числу повторов алгоритма
- Приложения
  - Поиск минимального разреза (полная вероятность)
  * Оценка глубины случайного двоичного дерева поиск
  * Парадокс дней рождений, взлом MD-5

8 RSA

- Остатки примеров на вероятность
- Криптосистема RSA
- Вероятностные тесты проверки простоты
  - Тест Ферма
  * Тест Миллера-Рабина

9 Алгоритмы на графах I. Поиск в глубину

Литература: [ДПВ12; 05; КЛР02]

Поиск в глубину. Связь времени открытия и времени закрытия вершин с правильными скобочными последовательностями. Переход от рекурсивного варианта алгоритма к итеративному с помощью стека.

Алгоритмы на основе поиска в глубину:

- Топологическая сортировка
- Сильно-связные компоненты
- Поиск Эйлерова цикла
- Проверка на двудольность
- Поиск мостов

10 Алгоритмы на графах II. Кратчайшие пути

Литература: [ДПВ12; 05; КЛР02]

План лекции

- Поиск в ширину
- Алгоритм Беллмана-Форда
- Алгоритм Дейкстры

11 Алгоритмы на графах III. Остовные деревья

Литература: [ДПВ12; 05; КЛР02]

План лекции

- Алгоритм Крускала
- Алгоритм Прима
- Union-Find (?) если была, попробуем рассказать оценку через $\log *$

12 От кратчайших путей к динамическому программированию

Литература: [ДПВ12; 05; КЛР02]

План лекции

- Алгоритм Флойда-Уоршелла
- Обзор алгоритмов поиска кратчайших путей и
- Линейный алгоритм поиска кратчайших расстояний в топологически сортированном графе.
- Задача о наибольшей возрастающей подпоследовательности (быстрый повтор)
- Задача про рюкзак
- Динамика на деревьях

* Сюжет с матрицами

  – возведения матрицы в степень — связь с количеством путей в графе

  - смена кольца на $(\vee, \wedge)$ — проверка на связность и транзитивное замыкание
  - смена кольца на $(\min, +)$ — поиск кратчайших путей

На семинар

- Задача о расстоянии редактирования (Edit distance)

13 Потоки

- Задача о максимальном потоке и минимальном разрезе
- Увеличивающие пути, остаточная сеть, метод Форда-Фалкерсона, теорема Эдмондса-Карпа
- Теорема о равенстве максимального потока и величины минимального разреза. (Дальше будет связь с двойственностью)
- Сводимость задачи о максимальном парасочетании к задаче о максимальном потоке

14 Линейное программирование

Литература: [ДПВ12]

- Задачи линейного программирования
- Двойственность
  - Задача о кратчайшем s-t пути и двойственная к ней
  - Максимальный поток и минимальный разрез
- Вычисление булевой схемы
- О приближённом решении ЦЛП через округление «непрерывной» ЛП

Примеры

– Задача о распределении ресурса (ЛП и ДП)
– Задача о поиске минимального остовного дерева через ЛП

Список литературы

[ДПВ12] *Дасгупта С.*, *Пападимитриу Х.*, *Вазирани У.* Алгоритмы. — М.: МЦНМО, 2012.

[05] Алгоритмы: построение и анализ. / Т. Кормен [и др.]. — 2-е. — М.: Вильямс, 2005.

[КЛР02] *Кормен Т.*, *Лейзерсон Ч.*, *Ривест Р.* Алгоритмы: построение и анализ. — М.: МЦНМО, 2002.

[Шен04] *Шень А. Х.* Программирование: теоремы и задачи. — М.: МЦНМО, 2004.

[КФ12] *Кузюрин Н. .*, *Фомин С. .* Эффективные алгоритмы и сложность вычислений. — 2012.

[18] Лекции по дискретной математике / М. Вялый [и др.]. — Черновик: https://publications.hse.ru/mirror/pubs/share/direct/393719078.pdf, 2018.

[ЖФФ12] *Журавлёв Ю. И.*, *Флёров Ю. А.*, *Федько О. С.* Дискретный Анализ. Комбинаторика. Алгебра логики. Теория графов. — М.: МФТИ, 2012.

[ЖФВ07] *Журавлёв Ю. И.*, *Флёров Ю. А.*, *Вялый М. Н.* Дискретный Анализ. Основы высшей алгебры. — М.: МЗ-пресс, 2007.

[Lei96] *Leighton T.* Notes on Better Master Theorems for Divide-and-Conquer Recurrences // Lecture notes, MIT. — 1996.