Вопросы к экзамену по алгоритмам
СПб ВШЭ, 2 курс, осень 2020, первый модуль

Собрано 18 декабря 2020 г. в 18:43

Курсивом помечено то, что было разобрано на практике. Кроме конспектов полезно смотреть разборы задач из практик и домашних заданий (иногда там написано иначе/понятнее/подробнее).

Теория чисел

1. Решето Эратосфена с временем $\mathcal{O}(n \log \log n)$, оптимизация в константу раз.
2. *Решето Эратосфена с памятью* $\mathcal{O}(\sqrt{n})$.
3. Решето Эратосфена с временем $\mathcal{O}(n)$.
4. *Подсчёт мультипликативных функций на* $[1, n]$ *за* $\mathcal{O}(n)$*:* φ*, число делителей, сумма делителей.*
5. Нахождение обратного по (простому и произвольному) модулю: возведение в степень, алгоритм Евклида, *обратные в* $\mathbb{F}_p$ *к* $1, \ldots, k$ *за* $\mathcal{O}(k)$.
6. Первообразный корень: проверка за $\mathcal{O}(\text{FACT} + \log^3 p)$, поиск.
7. Дискретный логарифм за $\mathcal{O}(\sqrt{p})$. Корень k-й степени по простому модулю.
8. Китайская теорема об остатках, случай не взаимно простых модулей. Использование в длинной арифметике.
9. Асимметричное шифрование. RSA: алгоритм кодирования, декодирования, сложность вычислений. Протокол Диффи—Хеллмана.

Линейная алгебра и метод четырёх русских

10. Метод Гаусса в $\mathbb{R}$, $\mathbb{F}_p$ за $\mathcal{O}(n^3)$ и в $\mathbb{F}_2$ за $\mathcal{O}(n^3/w)$. Нахождение решения для треугольной матрицы за $\mathcal{O}(n^2)$.
11. Реализация метода Гаусса для невырожденной квадратной матрицы.
12. Реализация метода Гаусса для произвольной матрицы $m \times n$. Свободные переменные. Базис решений.
13. Разложение вектора в базисе: методом Гаусса и с помощью ортогонализации Грама—Шмидта.
14. Метод Гаусса и погрешность. Матрица Гильберта. Способы борьбы с погрешностью. Метод простой итерации.
15. Вычисление определителя, обратной матрицы за $\mathcal{O}(n^3)$.
16. Метод Гаусса в евклидовых кольцах.
17. *Проверка принадлежности точки параллелепипеду. Расстояние от точки до подпространства. Нахождение решения с минимальной евклидовой нормой.*

---

18. Битовое сжатие. Умножение матриц над $\mathbb{F}_2$ за $\mathcal{O}(n^3/w)$.
19. Метод четырёх русских. Умножение матриц $\mathbb{F}_2^{n \times n} \times \mathbb{Z}^{n \times n}$ над $\mathbb{Z}$ за $\mathcal{O}(n^3/\log n)$, над $\mathbb{F}_2$ за $\mathcal{O}(n^3/(w \log n))$.
20. *Метод четырёх русских. Наибольшая общая подпоследовательность над бинарным алфавитом за* $\mathcal{O}(n^2/\log^2 n)$.

Быстрое преобразование Фурье (FFT) и длинная арифметика

21. База: извлечение корня из комплексного числа, единственность интерполяционного многочлена. Схема умножения многочленов за $\mathcal{O}(n \log n)$.
22. Рекурсивное вычисление DFT над $\mathbb{C}$ за $\mathcal{O}(n \log n)$.
23. Нерекурсивная эффективная реализация FFT за $\mathcal{O}(n \log n)$. Разворот всех битовых записей чисел за $\mathcal{O}(n)$.

24. Связь прямого и обратного DFT. Вычисление обратного DFT за $\mathcal{O}(n \log n)$.
25. Два вещественных DFT в одном комплексном.
26. Умножение чисел за $\mathcal{O}(n \log n)$, выбор системы счисления.
27. *FFT по простому модулю.*
28. *Возведение в степень. Поиск с ошибками. Поиск с ошибками и шаблоном (знаками «?»).*

---

29. Длинная арифметика: хранение; сложение, вычитание и деление на короткое за $\mathcal{O}(n/k)$, умножение за $\mathcal{O}((n/k)^2)$. Выбор k.
30. Бинарная арифметика: умножение за $\mathcal{O}(nm/k)$, деление за $\mathcal{O}((n-m)m/k)$, НОД за $\mathcal{O}(\max(n,m)^2/k)$.
31. Деление чисел за $\mathcal{O}(n^3/k^2)$ (бинпоиск), за $\mathcal{O}(n^2 \log n)$ (бинпоиск + FFT), за $\mathcal{O}(n^2/k)$ (бинарная арифметика), за $\mathcal{O}(n^2/k)$ (в столбик с бинпоиском), за $\mathcal{O}(n^2/k^2)$ (в столбик без бинпоиска — только алгоритм без доказательства).
(+) 32. Деление чисел за $\mathcal{O}(n^2/k^2)$ (в столбик без бинпоиска).
33. Деление многочленов за $\mathcal{O}(n^2)$ (наивно), за $\mathcal{O}(n \log^2 n)$ («разделяй и властвуй»).

Строки

34. Префикс-функция. Поиск подстроки в строке — алгоритм Кнута—Морриса—Пратта. *Нахождение всех периодов строки.*
35. Z-функция. Поиск подстроки в строке. *Нахождение всех периодов строки.*
36. *Количество подпалиндромов и максимальный подпалиндром за $\mathcal{O}(n)$ — алгоритм Манакера.*
37. Алгоритм Бойера—Мура поиска подстроки в строке.

---

38. Полиномиальный хеш строки. Хеш подстроки. Поиск подстроки в строке с $\mathcal{O}(1)$ дополнительной памяти — алгоритм Рабина—Карпа. *Нахождение всех периодов строки.*
39. Оценки вероятности коллизии полиномиального хеша в среднем и худшем случаях.
40. Хеши: количество различных подстрок за $\mathcal{O}(n^2)$. *Оценка вероятности ошибки и выбор модуля.*
41. *Антихеш-тест для модуля хеширования $m = 2^k$ — строка Туэ—Морса.*
42. *Хеши: нахождение наибольшей общей подстроки двух строк за $\mathcal{O}(n \log n)$, LCP за $\mathcal{O}(\log n)$, построение суффиксного массива за $\mathcal{O}(n \log^2 n)$.*
43. *Количество подпалиндромов и максимальный подпалиндром за $\mathcal{O}(n \log n)$ с помощью хешей.*

---

44. Построение суффиксного массива за $\mathcal{O}(n \log n)$. Реализация.
45. Вычисление LCP для суффиксного массива — алгоритм Касаи—Ли—Аримуры—Арикавы—Парка за $\mathcal{O}(n)$.
46. Суффиксный массив: поиск подстроки s в строке t за $\mathcal{O}(|s| \log |t|)$, за $\mathcal{O}(|s| + \log |t| \log |s|)$.
47. Суффиксный массив: поиск подстроки s в строке t за $\mathcal{O}(|s| + \log |t|)$.
48. *Суффиксный массив: нахождение наибольшей общей подстроки k строк за $\mathcal{O}(L)$.*

---

49. Бор, сжатый бор, хранение. Поиск словарных слов в тексте за $\mathcal{O}(|t| \max |s_i|)$.
50. Алгоритм Ахо—Корасик. Построение суффиксных ссылок двумя способами. Поиск словарных слов в тексте за $\mathcal{O}(|t| + L)$.
51. *Онлайн-словарь: при добавлении символа в конец текста пересчитать число вхождений словарных слов за $\mathcal{O}(1)$, обновить множество A вхождений за $\mathcal{O}(1 + |\Delta A|)$.*
52. Суффиксное дерево. Оценка на размер. *Построение за $\mathcal{O}(n^2)$.* Схема алгоритма Укконена построения за $\mathcal{O}(n)$ (основные идеи, инварианты).
53. Реализация алгоритма Укконена построения суффиксного дерева за $\mathcal{O}(n)$. Доказательство корректности и времени работы.
54. *Преобразование (суффиксное дерево) $\leftrightarrow$ (суффиксный массив + LCP) за $\mathcal{O}(n)$.*
55. *Суффиксное дерево: поиск подстроки s в строке за $\mathcal{O}(|s|)$, количество различных подстрок s за $\mathcal{O}(|s|)$, нахождение наибольшей общей подстроки k строк за $\mathcal{O}(L)$.*

Как попасть

Вы записываетесь в google-таблицу (она появится попозже), получаете время сдачи. В нужный момент вы приходите и сообщаете, что готовы сдавать. На это вы получаете *несколько* вопросов из списка и идёте **40 минут готовиться**.

Если вы опоздали более чем на 5 минут, вы попадаете в живую очередь, у вас самый низкий приоритет, но как только кто-то освободится, вас тоже послушают.

Чем можно пользоваться

На экзамен можно принести с собой один лист формата A4 с вашими рукописными записями на одной стороне. Этим листом можно пользоваться после получения вопросов во время подготовки, но нельзя во время ответа.

Другими словами: нельзя несколько листов, нельзя лист формата, отличного от A4, одна из сторон должна быть пустой, записи должны быть сделаны от руки (в том числе нельзя распечатать отсканированные рукописные записи).

На экзамене нельзя пользоваться любыми другими внешними источниками: другими людьми, компьютером, телефоном, литературой, конспектами, книгами, ...

Рассказ вопросов

Вы рассказываете материал по вопросам, которые вам выдали. У вас будет до 20-30 минут на ответ — напишите побольше (сколько успеете), чтобы можно было быстрее отвечать. Могут быть дополнительные вопросы по близким темам или по всему курсу.

После этого экзаменатор выставляет вам оценку по итогам вашего общения.

Возможно, здесь попозже появятся какие-то примерные границы того, за что вы получите какую оценку, но может и нет.