Вопросы к экзамену по алгоритмам
SPb HSE, 2-й курс, декабрь 2021

Общая информация

- Кроме конспектов полезно смотреть разборы задач из практик.
- *Курсивом* помечено то, что было разобрано на практике.
- (a) темы на 3 (оценка 4-5).
- (b) темы на 4 (оценка 6-7).
- (c) темы на 5 (оценка 8-9).
- (+) факультативные темы (оценка 10) – нужно заботать 3 любых темы из 6.

Строки, хеширование, сжатие данных

(a) 1. Универсальное семейство хеш-функций. Пример семейства.
(b) 2. Универсальное семейство хеш-функций. Время в хеш-таблице на списках.
(c) 3. 2-независимость, k-независимость. Пример 2-независимого семейства.
(b) 4. Фильтр Блюма.
(a) 5. Совершенное хеширование. Одноуровневая схема.
(b) 6. Совершенное хеширование. Двухуровневая схема.
(a) 7. *Хеширование множеств [211115].*
(b) 8. *Хеширование пар (способ полиномиальным хешированием).*
(a) 9. Сжатие данных. Th «нельзя сжать идеально», Th «можно сжать хорошо». 7-битное.
(b) 10. Сжатие данных. Хаффман. Хранение словаря.
(c) 11. Сжатие данных. Арифметическое кодирование.
(a) 12. Сжатие данных. BWT (только прямое)
(a) 13. Сжатие данных. RLE, связь с BWT, обратное RLE.
(b) 14. Сжатие данных. MTF, связь с BWT.
(b) 15. Сжатие данных. *Обратное MTF.*
(c) 16. Сжатие данных. *Обратное BWT за* $\mathcal{O}(n)$.
(b) 17. Сжатие данных. LZSS на практике (как сжимать 16gb? минимизировать количество бит?)
(c) 18. Сжатие данных. Словарное кодирование, простейший пример. LZW.
(c) 19. Сжатие данных. Связь сжатия и предсказаний. Алгоритм сжатия на основе предсказаний.
(a) 20. Ахо-Корасик. Пусть уже известны суффссылки. Поиск словарных слов в тексте.
(b) 21. Ахо-Корасик. *Для каждого словарного слова определить число вхождений.*
(a) 22. Ахо-Корасик. Полный автомат, ленивая динамика.
(b) 23. Ахо-Корасик. Версия с $\mathcal{O}(\sum |s_i|)$ памяти для произвольного алфавита.
(b) 24. Суффдерево. Алгоритм Укконена. Построение за $\mathcal{O}(n)$.
(c) 25. Суффдерево. Алгоритм Укконена. Оценка времени работы.
(c) 26. Суффдерево. Алгоритм Укконена. Подробности реализации.
(a) 27. Решение задач суффдеревом: число различных подстрок.
(b) 28. Решение задач суффдеревом: поиск общей подстроки.
(b) 29. Решение задач суффдеревом: LZSS за $\mathcal{O}(n)$.

Теория чисел

(a) 30. ТЧ. Решето Эратосфена. Алгоритм. Время работы $\mathcal{O}(n \log\log n)$. Оптимизация константы.
(b) 31. ТЧ. Решето Эратосфена. Версия за $\mathcal{O}(n)$.
(c) 32. ТЧ. *Решето Эратосфена с памятью* $\mathcal{O}(\sqrt{n})$.
(a) 33. ТЧ. Подсчёт мультипликативных функций на $[1, n]$ за $\mathcal{O}(n)$: количество делителей
(b) 34. ТЧ. Подсчёт мультипликативных функций на $[1, n]$ за $\mathcal{O}(n)$: φ, сумма делителей.
(a) 35. ТЧ. Расширенный алгоритм Евклида. Рекурсивно.
(b) 36. ТЧ. Расширенный Евклид. Время работы, нерекурсивная версия, диофантовы уравнения.
(c) 37. ТЧ. Расширенный Евклид. *Свойств коэффициентов.* Решение $ax + by = c, |x| + |y| \to \min$.
(a) 38. ТЧ. Обратное по простому и произвольному модулю. 2 алгоритма.
(b) 39. ТЧ. Обратное по простому и произвольному модулю. Сравнение способов.
(c) 40. ТЧ. *Поиск обратных к* $1..k$ *за* $\mathcal{O}(k)$.
(a) 41. ТЧ. Асимметричное шифрование. RSA: кодирование, декодирование.
(b) 42. ТЧ. Асимметричное шифрование. RSA: сложность вычислений.
(b) 43. ТЧ. Асимметричное шифрование. Протокол Диффи — Хеллмана.
(c) 44. ТЧ. RSA. Взлом в частных случаях.
(a) 45. ТЧ. Первообразный корень. Определение и поиск (без проверки).
(b) 46. ТЧ. Первообразный корень. Проверка за $\mathcal{O}(\text{FACT} + \log^3 p)$.
(c) 47. ТЧ. Вероятность попадания при поиске.
(a) 48. ТЧ. КТО. Формулы. Использование в длинной арифметики.
(c) 49. ТЧ. КТО. Случай не взаимно простых модулей.
(b) 50. ТЧ. Дискретный логарифм за $\mathcal{O}(\sqrt{p})$.
(b) 51. ТЧ. *Решение* $x^k = y \bmod p$.

Гаусс и линейная алгебра

(a) 52. Гаусс для невырожденной матрицы в $\mathbb{R}$, $\mathbb{F}_p$ за $\mathcal{O}(n^3)$.
Преобразование к треугольной и диагональной матрицам.
(a) 53. Нахождение решения СЛАУ для треугольной и диагональной матриц за $\mathcal{O}(n^2)$.
(b) 54. Гаусс для произвольной матрицы в $\mathbb{R}$, $\mathbb{F}_p$, базис пространства за $\mathcal{O}(nmk)$.
(b) 55. Гаусс в $\mathbb{F}_2$ за $\mathcal{O}(n^3/w)$.
(b) 56. Гаусс для произвольной матрицы. Свободные переменные. Базис решений.
(c) 57. Метод Гаусса и погрешность. Матрица Гильберта. Способы борьбы с погрешностью.
(a) 58. Метод простой итерации для $x = Ax$.
(b) 59. Метод простой итерации для $Ax = b$.
(b) 60. Вычисление обратной матрицы за $\mathcal{O}(n^3)$ и $\mathcal{O}(n^3/w)$.
(a) 61. Разложение вектора в базисе. Гаусс. Offline и online.
(b) 62. Разложение вектора в базисе. Ортогонализации Грама-Шмидта.
(a) 63. Вероятности. Задачи, которые умеем решать.
(b) 64. Вероятности. Вычисление вероятность «выжить на пути $\langle 1, 1\rangle \to \langle n, n\rangle$».
(c) 65. Метод Гаусса в евклидовых кольцах (Евклид).
(a) 66. *Проверка принадлежности точки параллелепипеду.*
(b) 67. *Расстояние от точки до подпространства.*
(c) 68. *Нахождение решения СЛАУ с минимальной евклидовой нормой.*

FFT, длинная арифметика

(a) 69. FFT. Комплексные числа: корни из единицы, группа по умножению, квадраты корней.

(b) 70. FFT. $\sum w^i = 0$, $w^{-1} = w^{n-1}$, $\overline{w}$.

(a) 71. FFT. Схема умножения многочленов за $\mathcal{O}(n \log n)$.

(a) 72. FFT. Рекурсивное вычисление DFT над $\mathbb{C}$ за $\mathcal{O}(n \log n)$.

(b) 73. FFT. Нерекурсивное FFT. Разворот всех битовых записей чисел за $\mathcal{O}(n)$.

(b) 74. FFT. Нерекурсивное FFT. Главные циклы. Кеширование. $\leq n \log_2 n$ умножений.

(c) 75. FFT. Нерекурсивное FFT. Предподсчёт корней, борьба с погрешностью.

(a) 76. FFT. Любой корректный алгоритм обратного без доказательства.

(b) 77. FFT. Связь прямого и обратного DFT. Сведение к DFT(w^{-1}).

(c) 78. FFT. Вычисление обратного DFT через `reverse` и «обращением последовательности действий».

(b) 79. FFT. Два вещественных DFT в одном комплексном.

(b) 80. FFT. Умножение **чисел** за $\mathcal{O}(n \log n)$, выбор системы счисления.

(c) 81. FFT. *FFT по простому модулю.*

(c) 82. FFT. *Умножение многочленов над $\mathbb{Z}/m\mathbb{Z}$. Достаточно рассказать 1 способ.*

(a) 83. FFT. *Возведение в степень за $\mathcal{O}(n \log n)$.*

(a) 84. FFT. Вычисление скалярных произведений.

(b) 85. FFT. *Поиск с ошибками.*

(c) 86. FFT. *Поиск с ошибками со знаками «?».*

(a) 87. Long. Длинная арифметика: хранение; сложение, вычитание и деление на короткое за $\mathcal{O}(n/k)$, умножение за $\mathcal{O}((n/k)^2)$. Выбор k.

(a) 88. Long. Бинарная арифметика: бинарное умножение.

(b) 89. Long. Бинарная арифметика: бинарный gcd.

(c) 90. Long. Бинарная арифметика: бинарное деление.

(a) 91. Long. Деление чисел, базовые алгоритмы: за $\mathcal{O}(n^3/k^2)$ (бинпоиск), за $\mathcal{O}(n^2 \log n)$ (бинпоиск + FFT).

(b) 92. Long. Деление чисел, за $\mathcal{O}(n^2/k)$ (в столбик с бинпоиском внутри).

(c) 93. Long. Деление чисел за $\mathcal{O}(n^2/k^2)$ (в столбик без бинпоиска).

(c) 94. Long. Деление многочленов за $\mathcal{O}(n \log^2 n)$ («разделяй и властвуй»).

(b) 95. Long. Перевод между система счисления за $\mathcal{O}(n \log^2 n)$ («разделяй и властвуй»).

Четыре русских

(a) 96. Умножение матриц над $\mathbb{F}_2$ за $\mathcal{O}(n^3/w)$.

(b) 97. Метод четырёх русских. Умножение матриц $\mathbb{F}_2^{n \times n} \times \mathbb{Z}^{n \times n}$ над $\mathbb{Z}$ за $\mathcal{O}(n^3/\log n)$.

(b) 98. Умножение матриц над $\mathbb{F}_2$ и булевым полукольцом за $\mathcal{O}(n^3/(w \log n))$.

(c) 99. *Метод четырёх русских. Наибольшая общая подпоследовательность над бинарным алфавитом за $\mathcal{O}(n^2/\log^2 n)$.*

(c)100. *Расстояние Левенштейна за $\mathcal{O}(n^2/\log^2 n)$.*

(a)101. Схема по таблице истинности. Решение из $\mathcal{O}(2^n n)$ гейтов.

(b)102. Схема по таблице истинности. Решение из $\mathcal{O}(2^n)$ гейтов.

(c)103. Схема по таблице истинности. Решение из $\mathcal{O}(\frac{1}{n}2^n)$ гейтов.

(a)104. *Транзитивное замыкание через $\mathcal{O}(\log n)$ умножений. Время работы.*

(b)105. *Транзитивное замыкание за $\mathcal{O}(n^3/(w \log n))$.*

(c)106. *Инкрементальное транзитивное замыкание за* $\mathcal{O}(q\frac{n}{w} + \frac{n^3}{w})$.

Бонус

(+)107. Совершенное хеширование. Схема на основе ацикличного графа.

(+)108. Хеширование кукушки.

(+)109. Количество простых до n за $\mathcal{O}(n^{2/3} \log n)$.

(+)110. Изоморфизм корневых деревьев за $\mathcal{O}(n)$ без хеш-таблиц и хешей.

(+)111. Решение систем уравнений над $\mathbb{Z}$ и над $\mathbb{Z}/m\mathbb{Z}$.

(+)112. Решение k-subsetsum (выбрать ровно k предметов с суммой ровно S) за $\mathcal{O}(\sqrt{k}nS)$.