

# Вопросы к экзамену по алгоритмам

## SPb HSE, 2-й курс ПМИ, декабрь 2024

### 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 6 любых темы из 8.

### Бор и суффструктуры

- (a) 1. Суффмассив: построение за  $\mathcal{O}(n \log^2 n)$  хешами.
- (a) 2. Суффмассив: поиск подстроки в тексте за  $\mathcal{O}(|s| \cdot \log |text|)$ .
- (a) 3. Суффмассив: построение за  $\mathcal{O}(n^2)$  цифровой сортировкой.
- (b) 4. Суффмассив: **эфффективное** построение за  $\mathcal{O}(n \log n)$  цифровой сортировкой.
- (b) 5. Суффмассив: алгоритм Касаи за  $\mathcal{O}(n)$ ,  $\forall i, j$   $LCP(i, j)$  за  $\mathcal{O}(1)$ .
- (c) 6. Суффмассив: поиск строки в тексте за  $\mathcal{O}(|s| + \log |text|)$ . Сам алгоритм.
- (c) 7. Суффмассив: поиск строки в тексте за  $\mathcal{O}(|s| + \log |text|)$ . Оценка времени.
- (a) 8. *Решение задач суффмассивом: поиск общей подстроки двух строк.*
- (b) 9. *Решение задач суффмассивом: поиск общей подстроки k строк.*
- (b) 10. *Решение задач суффмассивом: LZSS.*
- (a) 11. Бор. Хранение, `map`, `unordered_map`.
- (a) 12. Бор. Сортировка строк бором за  $\mathcal{O}(L \cdot \log |\Sigma|)$ .
- (c) 13. Бор. Сортировка строк бором за  $\mathcal{O}(L + |\Sigma|)$ .
- (a) 14. Ахо-Корасик. Пусть уже известны суффссылки. Поиск словарных слов в тексте.
- (b) 15. Ахо-Корасик. *Для каждого словарного слова определить число вхождений.*
- (a) 16. Ахо-Корасик. Полный автомат, ленивая динамика.
- (b) 17. Ахо-Корасик. Версия с  $\mathcal{O}(\sum |s_i|)$  памяти для произвольного алфавита.
- (a) 18. Suff. Сжатый бор. Построение суффдерева за  $\mathcal{O}(n^2)$ . Оценка на число вершин.
- (a) 19. Suff. Поиск подстроки в тексте, от которого построено суфф.дерево за  $\mathcal{O}(|s|)$ .
- (b) 20. Suff. Преобразование суффдерево  $\rightarrow$  (суффмассив + LCP) за  $\mathcal{O}(n)$ .
- (b) 21. Suff. Преобразование суффдерево  $\leftarrow$  (суффмассив + LCP) за  $\mathcal{O}(n)$ .
- (b) 22. Suff. Алгоритм Укконена. Построение суффдерева за  $\mathcal{O}(n)$ .
- (c) 23. Suff. Алгоритм Укконена. Оценка времени работы.
- (c) 24. Suff. Алгоритм Укконена. Подробности реализации: автонумерация ещё не созданных вершин, фиктивный отец корня, хранение ребра в лист, хранение рёбер, вершин, позиции в дереве.
- (a) 25. *Решение задач суффдеревом: число различных подстрок.*
- (b) 26. *Решение задач суффдеревом: поиск общей подстроки.*
- (b) 27. *Решение задач суффдеревом: LZSS за  $\mathcal{O}(n)$ .*

### Хеширование и сжатие данных

- (a) 28. Универсальное семейство хеш-функций. Пример семейства.
- (b) 29. Универсальное семейство хеш-функций. Время в хеш-таблице на списках.
- (c) 30. 2-независимость,  $k$ -независимость. Пример 2-независимого семейства.
- (b) 31. Фильтр Блюма. Структура данных. Преимущества. Сколько нужно памяти?
- (c) 32. Фильтр Блюма. Оценка вероятностей.
- (a) 33. Совершенное хеширование. Одноуровневая схема.
- (b) 34. Совершенное хеширование. Двухуровневая схема. Только алгоритм.
- (c) 35. Совершенное хеширование. Двухуровневая схема. Строгое обоснование.
- (a) 36. Хеширование множеств.
- (b) 37. Хеширование пар (способ полиномиальным хешированием).
- (a) 38. Сжатие данных. Th «нельзя сжать идеально», Th «можно сжать хорошо». 7-битное.
- (b) 39. Сжатие данных. Хаффман. Хранение словаря.
- (c) 40. Сжатие данных. Арифметическое кодирование.
- (a) 41. Сжатие данных. BWT (только прямое).
- (a) 42. Сжатие данных. RLE, связь с BWT, обратное RLE.
- (b) 43. Сжатие данных. MTF, связь с BWT.
- (b) 44. Сжатие данных. Обратное MTF.
- (c) 45. Сжатие данных. Обратное BWT за  $\mathcal{O}(n)$ .
- (b) 46. Сжатие данных. LZSS на практике: минимизировать количество бит, сжимать 16gb.
- (c) 47. Сжатие данных. Словарное кодирование, простейший пример. LZW.
- (c) 48. Сжатие данных. Связь сжатия и предсказаний. Алгоритм сжатия на основе предсказаний.

### Теория чисел

- (a) 49. ТЧ. Решето Эратосфена. Алгоритм. Время работы  $\mathcal{O}(n \log \log n)$ . Оптимизация константы.
- (b) 50. ТЧ. Решето Эратосфена. Версия за  $\mathcal{O}(n)$ .
- (c) 51. ТЧ. Решето Эратосфена с памятью  $\mathcal{O}(\sqrt{n})$ .
- (a) 52. ТЧ. Подсчёт мультипликативных функций на  $[1, n]$  за  $\mathcal{O}(n)$ : количество делителей
- (b) 53. ТЧ. Подсчёт мультипликативных функций на  $[1, n]$  за  $\mathcal{O}(n)$ :  $\varphi$ , сумма делителей.
- (a) 54. ТЧ. Расширенный алгоритм Евклида. Рекурсивно.
- (b) 55. ТЧ. Расширенный Евклид. Время работы, не рекурсивная версия, диофантовы уравнения.
- (c) 56. ТЧ. Расширенный Евклид. Свойств коэффициентов. Решение  $ax + by = c, |x| + |y| \rightarrow \min$ .
- (a) 57. ТЧ. Обратное по простому и произвольному модулю. 2 алгоритма.
- (b) 58. ТЧ. Обратное по простому и произвольному модулю. Сравнение способов.
- (c) 59. ТЧ. Поиск обратных к  $1..k$  за  $\mathcal{O}(k)$ .
- (a) 60. ТЧ. RSA: кодирование, декодирование.
- (b) 61. ТЧ. Протокол Диффи-Хеллмана.
- (c) 62. ТЧ. RSA: сложность вычислений.
- (c) 63. ТЧ. RSA. Взлом в частных случаях.
- (a) 64. ТЧ. Первообразный корень. Определение и поиск (без проверки).
- (b) 65. ТЧ. Первообразный корень. Проверка за  $\mathcal{O}(\text{ФАКТ} + \log^3 p)$ .
- (c) 66. ТЧ. Вероятность попадания при поиске первообразного.
- (a) 67. ТЧ. КТО. Формулы. Использование в длинной арифметики.
- (c) 68. ТЧ. КТО. Случай не взаимно простых модулей.
- (b) 69. ТЧ. Дискретный логарифм за  $\mathcal{O}(\sqrt{p})$ .
- (b) 70. ТЧ. Решение  $x^k = y \pmod{p}$ .

## Гаусс и линейная алгебра

- (a) 71. Гаусс для невырожденной матрицы в  $\mathbb{R}, \mathbb{F}_p$  за  $\mathcal{O}(n^3)$ .  
Преобразование к треугольной и диагональной матрицам.
- (a) 72. Нахождение решения СЛАУ для треугольной и диагональной матриц за  $\mathcal{O}(n^2)$ .
- (b) 73. Гаусс для произвольной матрицы в  $\mathbb{R}, \mathbb{F}_p$ , базис пространства за  $\mathcal{O}(nmk)$ .
- (b) 74. Гаусс в  $\mathbb{F}_2$  за  $\mathcal{O}(n^3/w)$ .
- (b) 75. Гаусс для произвольной матрицы. Свободные переменные. Базис решений.
- (c) 76. Метод Гаусса и погрешность. Матрица Гильберта. Способы борьбы с погрешностью.
- (a) 77. Метод простой итерации для системы уравнений  $x = Ax$ .
- (b) 78. Метод простой итерации для системы уравнений  $Ax = b$ .
- (b) 79. Вычисление обратной матрицы за  $\mathcal{O}(n^3)$  и  $\mathcal{O}(n^3/w)$ .
- (a) 80. Разложение вектора в базисе. Гаусс. Offline и online.
- (b) 81. Разложение вектора в базисе. Ортогонализации Грама-Шмидта.
- (a) 82. Вероятности. Задачи, которые умеем решать.
- (b) 83. Вероятности. Вычисление вероятности «выжить на пути  $\langle 1, 1 \rangle \rightarrow \langle n, n \rangle$ ».
- (c) 84. Метод Гаусса в евклидовых кольцах (Евклид).
- (a) 85. Проверка принадлежности точки параллелепипеду.
- (b) 86. Расстояние от точки до подпространства.
- (c) 87. Нахождение решения СЛАУ с минимальной евклидовой нормой.

## FFT, длинная арифметика

- (a) 88. FFT. Комплексные числа: корни из единицы, группа по умножению, квадраты корней.
- (b) 89. FFT.  $\sum w^i = 0, w^{-1} = w^{n-1}, \bar{w}$ .
- (a) 90. FFT. Схема умножения многочленов за  $\mathcal{O}(n \log n)$ .
- (a) 91. FFT. Рекурсивное вычисление FFT над  $\mathbb{C}$  за  $\mathcal{O}(n \log n)$ .
- (b) 92. FFT. Нерекурсивное FFT + разворот всех битовых записей чисел за  $\mathcal{O}(n)$ .
- (b) 93. FFT. Нерекурсивное FFT. Оптимизации: кэширование,  $\leq \frac{1}{2}n \log_2 n$  умножений.
- (c) 94. FFT. Нерекурсивное FFT. Предподсчёт корней, борьба с погрешностью.
- (a) 95. FFT. Обратное. Вычисление через FFT и `reverse`. Только алгоритм.
- (b) 96. FFT. Обратное. Связь с прямым, сведение к  $\text{FFT}(w^{-1})$ .
- (c) 97. FFT. Обратное. Строгие обоснования.
- (b) 98. FFT. Два вещественных FFT в одном комплексном.
- (b) 99. FFT. Умножение чисел за  $\mathcal{O}(n \log n)$ , выбор системы счисления.
- (c) 100. FFT. FFT по простому модулю.
- (c) 101. FFT. Умножение многочленов над  $\mathbb{Z}/m\mathbb{Z}$ . Достаточно рассказать 1 способ.
- (a) 102. FFT. Возведение в степень за  $\mathcal{O}(n \log n)$ .
- (a) 103. FFT. Вычисление скалярных произведений.
- (b) 104. FFT. Поиск с ошибками. За  $|\Sigma|$  FFT-шек.
- (b) 105. FFT. Поиск с ошибками со знаками «?». За  $|\Sigma|$  FFT-шек.
- (c) 106. FFT. Поиск с ошибками со знаками «?» за  $\mathcal{O}(1)$  FFT-шек.

- (a)107. 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)108. Long. Бинарная арифметика: бинарное умножение.
- (b)109. Long. Бинарная арифметика: бинарный gcd.
- (b)110. Long. Бинарная арифметика: бинарное деление за  $\mathcal{O}(n^2)$ .
- (b)111. Long. Деление чисел за  $\mathcal{O}(n^2/k)$  (в столбик с бинарным поиском по цифре).
- (c)112. Long. Деление чисел за  $\mathcal{O}(n^2/k^2)$  (в столбик без бинарного поиска).
- (c)113. Long. Деление многочленов за  $\mathcal{O}(n \log^2 n)$  («разделяй и властвуй»).
- (c)114. Long. Перевод между системами счисления за  $\mathcal{O}(n \log^2 n)$  («разделяй и властвуй»).

### Четыре русских

- (a)115. Битовое сжатие: умножение матриц над  $\mathbb{F}_2$  за  $\mathcal{O}(n^3/w)$ .
- (a)116. Предподсчёт: умножение матриц над  $\mathbb{F}_2$  за  $\mathcal{O}(n^3/\log n)$ .
- (b)117. Метод четырёх русских. Умножение матриц  $\{0, 1\}^{n \times n} \times \mathbb{Z}^{n \times n}$  над  $\mathbb{Z}$  за  $\mathcal{O}(n^3/\log n)$ .
- (b)118. Умножение матриц над  $\mathbb{F}_2$  и булевым полукольцом за  $\mathcal{O}(n^3/(w \log n))$ .
- (c)119. Метод четырёх русских. НОП над бинарным алфавитом за  $\mathcal{O}(n^2/\log^2 n)$ .
- (c)120. Расстояние Левенштейна за  $\mathcal{O}(n^2/\log^2 n)$ .
- (a)121. Схема по таблице истинности. Решение из  $\mathcal{O}(2^n n)$  гейтов.
- (b)122. Схема по таблице истинности. Решение из  $\mathcal{O}(2^n)$  гейтов.
- (c)123. Схема по таблице истинности. Решение из  $\mathcal{O}(\frac{1}{n} 2^n)$  гейтов.
- (b)124. Оптимизация четырьмя русскими перебора для поиска максимальной подклики.

### Бонус

- (+)125. Алгоритм Каркайнена-Сандерса. Суффмассив за  $\mathcal{O}(n)$ .
- (+)126. Совершенное хеширование. Схема на основе ациклического графа.
- (+)127. Хеширование кукушки. Сравнение с открытой/закрытой адресацией.
- (+)128. Количество простых до  $n$  за  $\mathcal{O}(n^{2/3} \log n)$ .
- (+)129. Изоморфизм корневых деревьев за  $\mathcal{O}(n)$  без хеш-таблиц и хешей.
- (+)130. Решение систем уравнений по разным модулям  $m_i$ .
- (+)131. Алгоритм Шраера-Смита.
- (+)132. Алгоритм Видемана решения системы  $Ax = 0$ .