

Вопросы на 4 к экзамену по алгоритмам SPb HSE, 2-й курс, декабрь 2021

Строки, хеширование, сжатие данных

- (b) 1. Универсальное семейство хеш-функций. Время в хеш-таблице на списках.
- (b) 2. Фильтр Блюма.
- (b) 3. Совершенное хеширование. Двухуровневая схема.
- (b) 4. Хеширование пар (способ полиномиальным хешированием).
- (b) 5. Сжатие данных. Хаффман. Хранение словаря.
- (b) 6. Сжатие данных. MTF, связь с BWT.
- (b) 7. Сжатие данных. Обратное MTF.
- (b) 8. Сжатие данных. LZSS на практике (как сжимать 16gb? минимизировать количество бит?)
- (b) 9. Ахо-Корасик. Для каждого словарного слова определить число вхождений.
- (b) 10. Ахо-Корасик. Версия с $\mathcal{O}(\sum |s_i|)$ памяти для произвольного алфавита.
- (b) 11. Суффдерево. Алгоритм Укконена. Построение за $\mathcal{O}(n)$.
- (b) 12. Решение задач суффдеревом: поиск общей подстроки.
- (b) 13. Решение задач суффдеревом: LZSS за $\mathcal{O}(n)$.

Теория чисел

- (b) 14. ТЧ. Решето Эратосфена. Версия за $\mathcal{O}(n)$.
- (b) 15. ТЧ. Подсчёт мультипликативных функций на $[1, n]$ за $\mathcal{O}(n)$: φ , сумма делителей.
- (b) 16. ТЧ. Расширенный Евклид. Время работы, нерекурсивная версия, диофантовы уравнения.
- (b) 17. ТЧ. Обратное по простому и произвольному модулю. Сравнение способов.
- (b) 18. ТЧ. Асимметричное шифрование. RSA: сложность вычислений.
- (b) 19. ТЧ. Асимметричное шифрование. Протокол Диффи — Хеллмана.
- (b) 20. ТЧ. Первообразный корень. Проверка за $\mathcal{O}(\text{ФАСТ} + \log^3 p)$.
- (b) 21. ТЧ. Дискретный логарифм за $\mathcal{O}(\sqrt{p})$.
- (b) 22. ТЧ. Решение $x^k = y \pmod p$.

Гаусс и линейная алгебра

- (b) 23. Гаусс для произвольной матрицы в \mathbb{R}, \mathbb{F}_p , базис пространства за $\mathcal{O}(ntk)$.
- (b) 24. Гаусс в \mathbb{F}_2 за $\mathcal{O}(n^3/w)$.
- (b) 25. Гаусс для произвольной матрицы. Свободные переменные. Базис решений.
- (b) 26. Метод простой итерации для $Ax = b$.
- (b) 27. Вычисление обратной матрицы за $\mathcal{O}(n^3)$ и $\mathcal{O}(n^3/w)$.
- (b) 28. Разложение вектора в базисе. Ортогонализации Грама-Шмидта.
- (b) 29. Вероятности. Вычисление вероятности «выжить на пути $\langle 1, 1 \rangle \rightarrow \langle n, n \rangle$ ».
- (b) 30. Расстояние от точки до подпространства.

FFT, длинная арифметика

- (b) 31. FFT. $\sum w^i = 0, w^{-1} = w^{n-1}, \bar{w}$.
- (b) 32. FFT. Нерекурсивное FFT. Разворот всех битовых записей чисел за $\mathcal{O}(n)$.

- (b) 33. FFT. Нерекурсивное FFT. Главные циклы. Кеширование. $\leq n \log_2 n$ умножений.
- (b) 34. FFT. Связь прямого и обратного DFT. Сведение к $\text{DFT}(w^{-1})$.
- (b) 35. FFT. Два вещественных DFT в одном комплексном.
- (b) 36. FFT. Умножение **чисел** за $\mathcal{O}(n \log n)$, выбор системы счисления.
- (b) 37. FFT. *Поиск с ошибками*.
- (b) 38. Long. Бинарная арифметика: бинарный gcd.
- (b) 39. Long. Деление чисел, за $\mathcal{O}(n^2/k)$ (в столбик с бинарным поиском внутри).
- (b) 40. Long. Перевод между системами счисления за $\mathcal{O}(n \log^2 n)$ («разделяй и властвуй»).

Четыре русских

- (b) 41. 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) 42. Умножение матриц над \mathbb{F}_2 и булевым полукольцом за $\mathcal{O}(n^3 / (w \log n))$.
- (b) 43. Схема по таблице истинности. Решение из $\mathcal{O}(2^n)$ гейтов.
- (b) 44. *Транзитивное замыкание* за $\mathcal{O}(n^3 / (w \log n))$.