

# Вопросы на 5 к экзамену по алгоритмам SPb HSE, 2-й курс ПМИ, декабрь 2024

## Бор и суффструктуры

- (c) 1. Суффмассив: поиск строки в тексте за  $\mathcal{O}(|s| + \log |text|)$ . Сам алгоритм.
- (c) 2. Суффмассив: поиск строки в тексте за  $\mathcal{O}(|s| + \log |text|)$ . Оценка времени.
- (c) 3. Бор. Сортировка строк бором за  $\mathcal{O}(L + |\Sigma|)$ .
- (c) 4. Suff. Алгоритм Укконена. Оценка времени работы.
- (c) 5. Suff. Алгоритм Укконена. Подробности реализации: автонумерация ещё не созданных вершин, фиктивный отец корня, хранение ребра в лист, хранение рёбер, вершин, позиции в дереве.

## Хеширование и сжатие данных

- (c) 6. 2-независимость,  $k$ -независимость. Пример 2-независимого семейства.
- (c) 7. Фильтр Блюма. Оценка вероятностей.
- (c) 8. Совершенное хеширование. Двухуровневая схема. Строгое обоснование.
- (c) 9. Сжатие данных. Арифметическое кодирование.
- (c) 10. Сжатие данных. Обратное BWT за  $\mathcal{O}(n)$ .
- (c) 11. Сжатие данных. Словарное кодирование, простейший пример. LZW.
- (c) 12. Сжатие данных. Связь сжатия и предсказаний. Алгоритм сжатия на основе предсказаний.

## Теория чисел

- (c) 13. ТЧ. Решето Эратосфена с памятью  $\mathcal{O}(\sqrt{n})$ .
- (c) 14. ТЧ. Расширенный Евклид. Свойств коэффициентов. Решение  $ax + by = c, |x| + |y| \rightarrow \min$ .
- (c) 15. ТЧ. Поиск обратных к  $1..k$  за  $\mathcal{O}(k)$ .
- (c) 16. ТЧ. RSA: сложность вычислений.
- (c) 17. ТЧ. RSA. Взлом в частных случаях.
- (c) 18. ТЧ. Вероятность попадания при поиске первообразного.
- (c) 19. ТЧ. КТО. Случай не взаимно простых модулей.

## Гаусс и линейная алгебра

- (c) 20. Метод Гаусса и погрешность. Матрица Гильберта. Способы борьбы с погрешностью.
- (c) 21. Метод Гаусса в евклидовых кольцах (Евклид).
- (c) 22. Нахождение решения СЛАУ с минимальной евклидовой нормой.

## FFT, длинная арифметика

- (c) 23. FFT. Нерекурсивное FFT. Предподсчёт корней, борьба с погрешностью.
- (c) 24. FFT. Обратное. Строгие обоснования.
- (c) 25. FFT. FFT по простому модулю.
- (c) 26. FFT. Умножение многочленов над  $\mathbb{Z}/m\mathbb{Z}$ . Достаточно рассказать 1 способ.
- (c) 27. FFT. Поиск с ошибками со знаками «?» за  $\mathcal{O}(1)$  FFT-шек.
- (c) 28. Long. Деление чисел за  $\mathcal{O}(n^2/k^2)$  (в столбик без бинпоиска).
- (c) 29. Long. Деление многочленов за  $\mathcal{O}(n \log^2 n)$  («разделяй и властвуй»).

(c) 30. Long. Перевод между система счисления за  $\mathcal{O}(n \log^2 n)$  («разделяй и властвуй»).

### Четыре русских

(c) 31. Метод четырёх русских. НОП над бинарным алфавитом за  $\mathcal{O}(n^2 / \log^2 n)$ .

(c) 32. Расстояние Левенштейна за  $\mathcal{O}(n^2 / \log^2 n)$ .

(c) 33. Схема по таблице истинности. Решение из  $\mathcal{O}(\frac{1}{n} 2^n)$  гейтов.