

ЛКШ.Зима.2016.А'+.Вопросы к теоретическому зачету.

1. Игры

- (a) Понятие игры, выигрышные/проигрышные состояния. Анализ ациклической игры.
- (b) Циклические игры, ничейные состояния. Ретроанализ циклической игры.
- (c) Сумма игр, эквивалентность игр. Игра «ним». Функция Гранди ациклической игры (тех).
- (d) Правило сложения нимов (хог) с доказательством, поиск выигрышного хода.
- (e) Анализ игры хакенбуш на дереве.

2. Теория чисел

- (a) Решето Эратосфена. Блочное решето Эратосфена.
- (b) Алгоритм Евклида. Расширенный и бинарный алгоритм Евклида.
- (c) Малая теорема Ферма и теорема Эйлера.
- (d) Китайская теорема об остатках.
- (e) Тест Миллера–Рабина.

3. Вычислительная геометрия: структуры данных

- (a) Список с пропусками (Skip List). Добавление, удаление и поиск элементов.
- (b) Дерево интервалов (Interval Tree). Решение задачи о поиске интервалов, содержащих точку.
- (c) Дерево с отрезками (Segment Tree). Решение задачи о поиске отрезков, пересекающих прямоугольник.
- (d) Алгоритм Киркпатрика локализации в триангуляции. Построение и локализация.

4. Распределенные вычисления

- (a) Понятие распределенных вычислений. Поиск максимума в массиве.
- (b) Понятие распределенных вычислений. Проверка правильности скобочной последовательности.
- (c) Понятие распределенных вычислений. Жребий Кржановского (поиск минимального элемента, встречающегося один раз).
- (d) Понятие распределенных вычислений. Нахождение расстояния между двумя точками, равномерно распределенными на окружности (обедающие за столом философы).

5. Потоки

- (a) Определение потока. Операции с потоком. Определение минимального разреза. Теорема Форда–Фалкерсона.
- (b) Определение потока. Алгоритм масштабирования потока. Оценка времени работы.
- (c) Определение потока. Алгоритм Эдмондса–Карпа. Оценка времени работы.
- (d) Определение потока. Алгоритма Диница. Поиск блокирующего потока. Оценка времени работы.

6. Быстрое преобразование Фурье

- (a) Комплексные числа: операции, модуль и аргумент, сопряжение, корни из 1.
- (b) Прямое преобразование Фурье.
- (c) Обратное преобразование Фурье.
- (d) Поиск первообразного корня. FFT по простому модулю специального вида.

7. Центроиды

- (a) Понятие центроида. Поиск центроида. Задача о числе путей длины D в дереве.
- (b) Центроидная декомпозиция. Поиск в дереве вершины минимального веса на расстоянии не более D от заданной. Модификация с учетом стоимости проезда.
- (c) Центроидная декомпозиция. Задача о покраске вершин на расстоянии не более D от заданной.

8. Теория графов

- (a) Понятие k -связного графа. Эквивалентные определения двусвязного графа.
- (b) Теорема Уитни. Формулировка и доказательство в предположении, что верна теорема Менгера.
- (c) Теорема Менгера. Формулировка и доказательство.

9. Криптография

- (a) Алгоритм RSA.
- (b) Алгоритм Diffie-Hellman.
- (c) Слепая криптографическая подпись.
- (d) Доказательство без разглашения не-изоморфизма двух графов.
- (e) Доказательство без разглашения наличия правильной раскраски графа в k -цветов.
- (f) Доказательство без разглашения наличия гамильтонового пути.