Выпуск 1

Контрольная пройдет 13.05 с 9 по 12 в Б. Физической. Для 74 группы контрольная пройдет 13.05 с 12:20 по 15:20 в 414 ГК.

На контрольной запрещено пользоваться любыми электронными устройствами. Разрешено пользоваться книгой Кормена "Алгоритмы", а также разрешено взять один лист А4 с произвольными записями.

К следующему замечанию я попрошу отнестись серьезно. Любые нарушения указанного протокола повлекут нулевую оценку за тест. Также я настоятельно рекомендую выполнять работу самостоятельно. Согласно протоколу, если заимствование будет идентифицировано, то никакого поиска правых и виноватых производится не будет, и результаты всей группы будут обнулены. Пожалуйста, не подводите своих товарищей, которые, возможно, и не подозревают о вашем орлином зрении и выдающихся способностях имитации. Я специально останавливаюсь на этом, поскольку после первого теста участвовал в переписке, в которой выдающийся имитатор, ухитрившийся за сорок минут теста буквально скопировать даже погрешности второго порядка (зачеркивания зачеркиваний) утверждал, что, во-первых, он не знал, что такая деятельность не приветствуется, а во-вторых (дальше идет почти библейская история), что виноват неназванный искуситель, спровоцировавший его тем, что раздал одинаковые варианты соседям. Даже несмотря на выдающееся качество копии все герои этой истории получили 0 баллов (в том числе и тот, ничего не подозревавший студент, у которого списывали). С моей точки зрения, самым печальным во всех этих процессах является то, что ошибки копируются буквально.

РАЗДЕЛЫ ИЗ ПРОГРАММЫ КУРСА, КОТОРЫЕ ВКЛЮЧЕНЫ В ФИНАЛЬНЫЙ ТЕСТ

1. Примеры алгоритмов: проверка простоты, факторизация чисел; Одновременное вычисление максимального и минимального элементов в массиве; быстрое умножение чисел и матриц (алгоритмы Карацубы и Штрассена); аддитивные цепочки.

Модели вычислений. Формальное определение алгоритма. Различные определения трудоемкости алгоритма.

2. Асимптотические оценки. Нотация: $O(\cdot), o(\cdot), \Omega(\cdot), \omega(\cdot), \Theta(\cdot)$. Алгоритмы типа "разделяй-и-властвуй". основная теорема о рекуррентных оценках (нахождение асимптотики рекуррентности вида $T(n) = aT(\frac{n}{b}) + f(n)$). Дерево рекурсии. Линейный алгоритм нахождения медианы массива. Линейные рекуррентные последовательности.

3. Потоки и разрезы в сети. Теорема о максимальном потоке и минимальном разрезе. Понятие остаточного графа и увеличивающего пути. Алгоритм Форда-Фалкерсона для вычисления максимального потока и минимального разреза. Задача о максимальном потоке минимальной стоимости. Обобщения потоковой сети (пропускные способности узлов и пр.). Приложение потоковых алгоритмов: цепное разложение порядков (лемма Дилворта), задача о максимальном паросочетании в двудольном графе, задача о назначениях, расписание с прерываниями на идентичных процессорах.

4. Алгоритмы сортировки: пузырек; быстрая сортировка (quicksort); сортировка с помощью кучи; слияние; цифровая сортировка. Анализ трудоемкости алгоритма quicksort по наихудшему случаю и в среднем. Устойчивость алгоритма сортировки. Нижние оценки сортировки. Разрешающие деревья. Порядковые статистики. Схемы сортировки.

5. Обобщенный алгоритм Евклида. Модульная арифметика. Китайская теорема об остатках. Функция Эйлера. Первообразные корни. Кольца $\mathbb{Z}_n$, в которых существуют первообразные корни. Индексы (дискретные логарифмы). Кодирование с открытым ключом. Квадратичные вычеты. Схема RSA.

6. Дискретное преобразование Фурье, алгоритм быстрого преобразования Фурье (БПФ), перемножение многочленов с помощью БПФ. Использование БПФ для поиска подстрок.

7. Алгоритмы на графах и порядках: поиск в ширину; поиск в глубину; определение двусвязных и/или сильносвязных компонент; кратчайшие пути: алгоритмы Дейкстры, Флойда, Беллмана-Форда; транзитивное замыкание; топологическая сортировка; остовные леса (алгоритмы Прима и Краскала); паросочетания.

8. Детерминированные и недетерминированные МТ. Класс $\mathcal{P}$. Примеры языков из $\mathcal{P}$: полиномиальная реализация алгоритма максимального потока; системы линейных уравнений (полиномиальная реализация метода Гаусса).

Классы $\mathcal{NP}$ и $co-\mathcal{NP}$. Примеры языков из $\mathcal{NP}$: простые числа; непланарные графы (критерий Куратовского).

9. Полиномиальная сводимость. Сводимость по Карпу и по Куку (по Тьюрингу). Теорема Кука-Левина. Примеры полиномиально полных языков: выполнимость; протыкающее множество; 3-сочетание; максимальное 2-сочетание; вершинное покрытие; клика; хроматическое число; гамильтонов цикл; рюкзак; разбиение; максимальный разрез.

10. Методы решения переборных задач: динамическое программирование, шкалирование, ветви и границы, приближенные алгоритмы. ε-оптимальная процедура решения задачи о рюкзаке.

11. Вероятностные алгоритмы. Классы $\mathcal{RP}$, $\mathcal{BPP}$, $\mathcal{ZPP}$. Вероятностные алгоритмы: проверка простоты; вычисление медианы массива; проверка полиномиальных тождеств; поиск паросочетаний в графах; алгоритм Каргера поиска минимального разреза.

Распределение задач теста 13 мая по разделам

1. Оценки, вероятностные алгоритмы, основная теорема о рекуррентностях.
2. Сортировка и числа.
3. NP-полнота.
4. Алгоритмы на графах

5. ДПФ и БПФ.
6. Потоки в сети
7. Повторительные задачи (их 10).

Определения, теоремы, алгоритмы, которые могут использоваться в тесте

Определения и понятия.

Первообразный корень, обратный остаток, порядок элемента в группе вычетов, φ-функция Эйлера, индекс.

Потоковая сеть, остаточный граф, увеличивающий путь, разрез.

Дерево рекурсии.
Разрешающее дерево для алгоритмов сортировки.

Теоремы.

Основная теорема о рекуррентных оценках.
Теорема о максимальном потоке и минимальном разрезе.
Малая теорема Ферма.
Нижние оценки для сортировки.
Китайская теорема об остатках.
Критерий планарности Куратовского (без доказательства).
Теорема о скобочной структуре отметок поиска в глубину на графах.
Теорема Кука- Левина.
Теоремы об NP-полноте основных рассмотренных в курсе языков (выполнимость; протыкающее множество; 3-сочетание; максимальное 2-сочетание; вершинное покрытие; клика; хроматическое число; гамильтонов цикл; рюкзак; разбиение; максимальный разрез).

Алгоритмы.

Числа

Решето Эратосфена.
Алгоритм Эвклида.
Метод Гаусса решения ситем линейных уравнений.
Быстрое умножение и возведение в степень чисел и матриц.
Построение общего множества решений ЛРП.
Система RSA (кодирование, декодирование, электронная подпись).
Решение линейных диофантовых уравнений.
Хеш-функции.

Потоки

Алгоритм Форда-Фалкерсона нахождения максимального потока и минимального разреза (тут 2 алгоритма, сколь бы ни прост был второй).
Приложение потоковых алгоритмов: задача о максимальном паросочетании в двудольном графе, задача о назначениях.

Сортировка.

Алгоритмы сортировки (пузырек, слияние, куча, quicksort).
Линейные алгоритмы поиска медианы (детерминированный и вероятностный); порядковые статистики (поиск k-о элемента).

ДПФ и БПФ.
Алгоритм БПФ. Трудоемкость алгоритма БПФ. Алгоритм поиска подстрок посредством БПФ.

Алгоритмы на графах.

Поиск в ширину; поиск в глубину.
Определение двусвязных и/или сильносвязных компонент.
Кратчайшие пути: алгоритмы Дейкстры, Флойда, Беллмана-Форда; транзитивное замыкание.
топологическая сортировка.
остовные леса (алгоритмы Прима и Краскала).
Паросочетания и взвешенные паросочетания в двудольных графах (венгерский алгоритм).

ε-оптимальная процедура решения задачи о рюкзаке.

Вероятностные алгоритмы.

Проверка простоты.
Вычисление медианы массива.
Проверка полиномиальных тождеств.
Поиск паросочетаний в графах.
Алгоритм Каргера поиска минимального разреза.

ЛИТЕРАТУРА

Основная

1. Ахо А., Хопкрофт Д., Ульман Д.*Построение и Анализ Вычислительных Алгоритмов.* М.: Мир, 1979.
1. Гери М., Джонсон Д. *Вычислительные машины и труднорешаемые задачи.* М.: Мир, 1982.
3. **[Кормен 1]** Кормен Т., Лейзерсон Ч., Ривест Р. *Алгоритмы: Построение и Анализ.* М.: МЦНМО, 2002.
4. **[Кормен 2]** Кормен Т., Лейзерсон Ч., Ривест Р., Штайн К. *Алгоритмы: Построение и Анализ. (2-е изд.)* М.: Вильямс, 2005.
5. Кузюринн Н., Фомин С. *Эффективные алгоритмы и сложность вычислений.* М.: МФТИ, 2007.

Дополнительная

1. Верещагин Н., Шень А. *Вычислимые Функции.* М.: МЦНМО, 1999. (Электронный вариант: www.mccme.ru/free-books)
2. Виноградов И. *Основы теории чисел.* М.-Л.: Гостехиздат, 1952
3. Вялый М., Журавлев Ю., Флеров Ю. *Дискретный анализ. Основы высшей алгебры.* М.: МЗ Пресс, 2007.
4. **К-Ш-В** Китаев А., Шень А., Вялый М. *Классические и квантовые вычисления.* М.: МНЦМО-ЧеРо, 1999.
4. **Хинчин** Хинчин А. Цепные дроби. М.: Наука, 1979.
6. Шень А. *Программирование. Теоремы и задачи.* М.: МЦНМО, 2007. (Электронный вариант: www.mccme.ru/free-books)
7. Lovasz L. *Computational complexity.* www.cs.elte.hu/ lovasz/complexity.pdf

Вариант для подготовки
Он может сильно отличаться от теста.

1) Прежде всего я рекомендую найти, используя алгоритм Форда-Фалкерсона, максимальный поток и минимальный разрез в сети (можете взять пример из задания). Дело в том, 90% писавших тест 1 вообще этот алгоритм не понимали Например, на знали что такое остаточный граф; увеличивающие пути искали прямо по сети, используя запрещенную подпрограмму "палец" и т.д. Хорошим мысленным экспериментом является следующий: как вы будете действовать, если в сети 10000 ребер?

Числа

1. Вычислите $2013^{25^{1000}} \pmod{46}$.

Это буквально пример из последнего теста. С ним не справилось, несмотря на его простоту, процентов 80.

Оценки

И с этой темой были трудности в предыдущем тесте. Их, конечно, будет меньше, поскольку будет возможность заглянуть в Кормена. Теме не менее, небольшая практика не помешает. При вычислении асимптотик обязательно исследуйте эффекты, связанные с использованием функций типа $\lfloor\cdot\rfloor$ и сдвига аргумента.

2. (i) $T(n) = 3T(\lfloor\frac{n}{2}\rfloor + 2) + O(n^2)$.
(ii) $T(n) = T(\lceil\frac{n}{3}\rceil - 1) + O(n)$.
(iii) $T(n) = T(\lceil\sqrt{n}\rceil - 1) + O(\log n)$.
(iv) Запишите рекуррентность, которой удовлетворяет БПФ для массива $[a_0, a_1, \ldots, a_{n-1}]$.
(v) Оцените трудоемкость перемножения двух полиномов посредством БПФ. Специфицируйте вашу модель вычислений.

Алгоритмы на графах

3. При поиске в глубину в неорентированном графе G вершина u получила метки $d[u] = 3$ и $f[u] = 13$. В G есть ребро (u, v). Какие из вариантов отметок $[d, f]$, которые может получить v, корректны? 1) $[5, 8]$; 2) $[6, 17]$; 1) $1, 6]$; 2) $[18, 27]$.

4. Дан взвешенный граф с положительными весами. Постройте алгоритм, который вычисляет кратчайший мультипликативный путь между заданной парой вершин s и t (произведение соответствующих весов ребер) и укажите класс сетей, для которых процедура будет корректной.

5. Дан граф с положительными весами ребер. Сохранится ли путь между вершинами s и t, имеющий минимальный вес, если увеличить вес каждого ребра на 5 единиц? Тот же вопрос, если речь идет о пути максимального веса. Тот же вопрос, если речь идет о кратчайшем остовном дереве.

Алгоритмы на графах

6. (Возможно, полезно почитать об эффективности жадного алгоритма покрытия.) Мы использовали жадный алгоритм в задаче покрытии (SET COVER) множества из 93 элементов и на некотором шаге покрыли 15 элементов. Оцените снизу мощность оптимального покрытия.

7. (i) Постройте 2-приближенный алгоритм для задачи коммивояжера, если матрица расстояний удовлетворяет неравенству треугольника.
(ii) Постройте 2-приближенный алгоритм для двух коммивояжеров. По-прежнему матрица расстояний удовлетворяет неравенству треугольника, и также заданы (различные) точки a, b старта. Каждый коммивояжер должен закончить обход в точке своего старта и не должен заходить в один и тот же город дважды. И в каждый город должен зайти хотя бы один коммивояжер.

$\mathcal{P}$, $\mathcal{NP}$, $co-\mathcal{NP}$, полиномиальная сводимость

8. Пусть A — это язык из $\mathcal{P}$, не совпадающий с $\emptyset$ или с Σ^*. Верно ли, что оба семейства языков $\{B \mid B \leq_P A\}$ и $\{B \mid A \leq_P B\}$ (“$\leq_P$” означает полиномиальную сводимость) не более, чем счетные?

Тот же вопрос, если $A \in \mathcal{NP}$. Тот же вопрос, если $A \in co-\mathcal{NP}$.

9. Является ли полиномиально полным язык L, состоящий из кодировок всех графов, в которых есть простой цикл, имеющий не менее $|V|/2$ вершин?

10. Приведите доказательство, что язык ПЛАНАРНЫЕ ГРАФЫ принадлежит $co-\mathcal{NP}$ (нельзя ссылаться на алгоритмы, корректнсть которых вы не можете обосновать; можно пользоваться критерием Куратовского).