Уважаемые студенты!

Контрольная пройдет 19.05 с 9 по 12 в Б. Физической.

К следующему замечанию я попрошу отнестись серьезно.

На контрольную запрещено приносить любые электронные устройства. Разрешено пользоваться книгой Кормена "Алгоритмы", а также разрешено взять один лист А4 с произвольными записями. Наличие любого запрещенного объекта, будь то неучтенный листок бумаги или телефон, приведет к немедленному удалению и нулевой оценке за тест.

Также я настоятельно рекомендую выполнять работу самостоятельно. Согласно протоколу, если заимствование будет идентифицировано, то никакого поиска правых и виноватых производиться 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. С моей точки зрения, самым печальным во всех этих процессах является то, что ошибки копируются буквально.

В ФИНАЛЬНЫЙ ТЕСТ ВКЛЮЧЕНЫ РАЗДЕЛЫ 1–11 ПРОГРАММЫ КУРСА (ВСЕ, КРОМЕ РАЗДЕЛА 12 — ВЕРОЯТНОСТНЫЕ АЛГОРИТМЫ).

В тесте будет 6 основных задач, которые оцениваются примерно по десять баллов, и 10 вспомогательных задач, которые оцениваются по три балла. Примерную разницу в сложности основных и вспомогательных задач можно понять по предыдущему тесту.

Распределение задач теста 19 мая по разделам

Основные задачи.

1. Оценки, основная теорема о рекуррентностях, дерево рекурсий.
2. NP-полнота.

3–5. Алгориты на графах. NP-полнота, выполнимость КНФ, БПФ, ДПФ

6. Потоки в сети
7. Вспомотельные задачи (их 10). Темы: числовые алгоритмы, RSA; классы $\mathcal{P}, \mathcal{NP}, co-\mathcal{NP}$, NP-полнота, полиномиальная сводимость; алгоритмы на графах (пути, деревья, обходы и т.д.); сортировка и порядковые статистики; БПФ; оценки; элементарные сведения о линейном программировании.

Определения, теоремы, алгоритмы, которые могут использоваться в тесте

Определения и понятия.

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

Потоковая сеть, остаточный граф, увеличивающий путь, разрез.

Дерево рекурсии.

Разрешающее дерево для алгоритмов сортировки.

Прямая и двойственная задачи ЛП.

Полиномиальная сводимость. Классы $\mathcal{P}, \mathcal{NP}, co-\mathcal{NP}$. Основные NP-полные задачи, рассмотренные в курсе: выполнимость; протыкающее множество; 3-сочетание; максимальная 2-выполднимость; вершинное покрытие; клика; хроматическое число; гамильтонов цикл; разбиение; максимальный разрез; рюкзак[1].

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).

Теорема двойственности линейного программирования.

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, цифровая сортировка, сортировка подсчетом).

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.

---

[1] Приведем определение, поскольку в некоторых изданиях Кормена эта задача не формулируется явно: РЮКЗАК (на выполнимость)=$\{(a_1, a_2, \ldots, a_n, b) \in \mathbb{N}^{n+1}$ | сумма некоторых a_i равна b, т. е. соответствующее линейное уравнение $\sum a_i x_i = b$ имеет некоторое $\{0,1\}$-решение$\}$.

Определение сильно связных и/или двусвязных 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).

Любой алгоритм решения системы линейных неравенств.

ε-оптимальная процедура решения задачи о рюкзаке.

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). Как мне кажется, до сих пор многие не знают, например, что такое остаточный граф, а увеличивающие пути ищут 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 $2014^{25^{1000}} \pmod{46}$.

В этой задаче нужно обратить внимание на правильную формулировку малой теоремы Ферма.

Оценки

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) $T(n) = T(\lceil \sqrt{n} \rceil - 1) + O(\log n)$.
(v) $T(n) = 2014T(\frac{n}{2013}) + n^{2.011}$.
(v) Запишите рекуррентность, которой удовлетворяет БПФ для массива $[a_0, a_1, \ldots, a_{n-1}]$.
(vi) Оцените трудоемкость перемножения двух полиномов посредством БПФ. Специфицируйте вашу модель вычислений.

Алгоритмы на графах

3. При поиске в глубину в неориентированном 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.

Приближенные алгоритмы

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, корректность которых вы не можете обосновать; можно пользоваться критерием Куратовского).