Программа курса "Сложность вычислений" 2002 (дополнительное образование на мехмате).

1. Время и память (зона) как меры сложности вычислений.

2. Полиномиальная эквивалентность по времени одноленточных и многоленточных машин Тьюринга.

3. Класс P функций, вычислимых за полиномиальное время. Принадлежность классу P функций сложения, умножеия и деления целых чисел, и функции возведения в степень по данному модулю.

4. Теорема о иерархии для зонной сложности.

5. Теорема о иерархии для временной сложности.

6. Класс NP. NP-полные проблемы. Принадлежность к NP множества простых чисел

7. Теорема Кука — Левина об NP-полноте проблемы выполнимости булевых формул.

8. NP-полнота задач 3-КНФ, 3-РАСКРАСКА, КЛИКА, ВЕРШИННОЕ ПОКРЫТИЕ, ГАМИЛЬТОНОВ ЦИКЛ, РЮКЗАК, КОММИВОЯЖЕР, ЦЕЛОЧИСЛЕННОЕ ЛИНЕЙНОЕ ПРОГРАММИРОВАНИЕ.

9. Вероятностный алгоритм распознавания простоты чисел.

10. Класс BPP.

11. Класс P/poly, и вложение классов P и BPP в класс P/poly.

12. Полиномиальные игры с конечным числом ходов и полиномиальная иерархия.

13. Полиномиальные игры с полиномиальным числом ходов и класс PSPACE. Вложение классов полиномиальной иерархии в класс PSPACE.

14. PSPACE-полнота задачи об истинности булевых формул с кванторами.

15. Вложение класса BPP в класс Σ_2 полиномиальной иерархии.

16. Интерактивное доказательство неизоморфности данных графов.

17. Класс IP языков, имеющих интерактивную дедуктику. Вложение IP в класс PSPACE

18. Понижение вероятности ошибки в интерактивных доказательствах без увеличения количества раундов.

19. Вложение MA[2] в AM[2]. Здесь AM[2] обозначает класс языков, имеющих интерактивное доказательство с открытыми бросаниями

в один раунд — сначала делает сообщение Артур, затем Мерлин. Через MA[2] обозначается класс языков, имеющих интерактивное доказательство в один раунд — сначала Мерлин, затем Артур.

20. Вложение класса AM[const] в класс AM[2]

21. Вложение PSPACE в класс IP.

22. Вероятностно проверяемые доказательства и PCP-теорема (без доказательства).

23. Невозможность быстрого приблизительного вычисления размера максимальной клики в данном графе (если P не равно NP).

24. Доказательство с нулевым разглашением изоморфности данных графов.

25. Доказательство с нулевым разглашением раскрашиваемости данного графа в три цвета.

26. Надежные и непредсказуемые генераторы псевдослучайных битов. Эквивалентность этих понятий.

27. Построение надежного генератора $n \to p(n)$ на основе надежного генератора $n \to n+1$.

28. Необратимые функции, необратимые перестановки. Построение непредсказуемого генератора $n \to n+1$ на основе необратимой перестановки.

Для сдачи экзамена достаточно решить следующие задачи.

29. Доказать NP-полноту следующей проблемы. Условие: конечное множество A, функция s из A в множество натуральных чисел. Вопрос: можно ли разбить A на два непересекающихся подможества A_1, A_2 так, чтобы $\sum_{a\in A_1} s(a) = \sum_{a\in A_2} s(a)$.

30. Доказать NP-полноту следующей проблемы. Условие: конечное множество A, функция s из A в множество натуральных чисел, и два натуральных числа m, n. Вопрос: можно ли разбить A на m непересекающихся подможеств $A_1, \ldots, A_m$ так, чтобы длина в $\mathbb{R}^m$ вектора $\langle \sum_{a\in A_i} s(a), i = 1, \ldots, m\rangle$ не превосходила n: $\sum_{i=1}^{m} (\sum_{a\in A_i} s(a))^2 \le n^2$.

31. Доказать NP-полноту следующей проблемы. Условие: граф $G = (V, E)$, подмножество $W \subset V$ и натуральное число n. Вопрос: существует ли поддерево в G, содержащее все вершины из W и имеющее не более n ребер.

32. Докажите, что класс AM[2] вложен в класс $\Pi_2 = \text{co-}\Sigma_2$ полиномиальной иерархии.

33. Придумайте интерактивное доказательство того, что данная формула общезначима (то есть истинна при всех значениях переменных).

34. Докажите, что если существует надежный генератор $n \to n+1$, то существует и необратимая функция.

Литература.

1. М. Гэри, Д. Джонсон. Вычислительные машины и труднорешаемые задачи. М.: Мир, 1982.

2. А. Китаев, А. Шень, М. Вялый. Классические и квантовые вычисления. М.: МЦНМО, ЧеРо, 1999.

3. Введение в криптографию. Под общей редакцией В.В.Ященко. — 3-е изд. доп. — М.: МЦНМО: "ЧеРо", 2000. — 288 с.

4. М.И. Анохин, Н.П.Варновский, В.М.Сидельников, В.В. Ященко. Криптография в банковском деле. М.: МИФИ, 1997.

5. L.Babai, "Trading group theory for randomness". Proc. 17th ACM Symp. on Theory of Comp. (1985), pp.421-429.

6. A. Shamir. IP=PSPACE. Journ. of the ACM, 39 (1992) 869–877.

7. O. Goldreich. Foundation of Cryptography. Basic Tools. Cambridge UP. 2001.

8. Т. Кормен, Ч. Лейзерсон, Р. Ривест. Алгоритмы: построение и анализ. М.: МЦНМО, 2001.