Программа курса “Сложность вычислений” 2008/2009.

1. Полиномиальная эквивалентность по времени одноленточных и многоленточных машин Тьюринга. Класс P функций, вычислимых за полиномиальное время. Принадлежность классу P функций сложения, умножения и деления целых чисел, и функции возведения в степень по данному модулю. Вычисление за полиномиальное время наибольшего общего делителя целых чисел.

2. Равнодоступные адресные машины (РАМ). Моделирование РАМ на двуленточных машинах Тьюринга.

3. Теорема о иерархии для временной сложности.

4. Теорема Фишера–Рабина об экспоненциальной нижней оценки времени разрешения элементарной теории аддитивной группы действительных чисел.

5. Классы P/poly, n.u.P, их равнообъемность и вложение класса P в класс n.u.P.

6. Вероятностные алгоритмы. Уменьшение вероятности ошибки. Классы BPP и FBPP. Включение класса BPP в класс P/poly.

7. Алгоритм Миллера–Рабина проверки простоты натуральных чисел.

8. Класс NP. Сводимость Карпа и ее свойства. Теорема Кука — Левина об NP-полноте проблемы выполнимости схем из функциональных элементов.

9. NP-полнота задач 3-КНФ, 3-РАСКРАСКА, КЛИКА, ВЕРШИННОЕ ПОКРЫТИЕ, ГАМИЛЬТОНОВ ЦИКЛ, КОММИВОЯЖЕР, СУММА ПОДМНОЖЕСТВ

10. Полиномиальные игры с конечным числом ходов и полиномиальная иерархия PH.

11. Вложение класса BPP в класс Σ_2 полиномиальной иерархии.

12. Задачи подсчета. Класс $\#P$. Полнота в классе $\#P$ задач подсчета количества выполняющих наборов 3-КНФ, количества клик данного размера, количества 3-раскрасок данного графа. $\#P$-полнота задачи о вычислении перманента булевой матрицы.

13. Теорема Вэльянта—Вазирани о сведении NP-задач к NP-задачам с единственным свидетелем.

14. Распределенные задачи. Простые распределенные задачи. Класс DistNP. Частичный порядок на распределениях. Сводимость Карпа для распределенных задач. Полная в классе DistNP распределенная задача.

15. Вычислительно простые генерируемые распределния. Dist'NP. Существование Dist'NP-полных задач.

16. Существование Dist'NP-полных задач с равномерным распределением на входах относительно вероятностных сведений.

17. Dist'NP-полнота задачи о замощении.

18. Сведение задач поиска к задачам распознавания.

19. Сведение задач поиска к задачам поиска с вычислительно простым распределением на входах.

20. Полиномиальная иерархия. Классы PSPACE и EXP. Вложение PSPACE в EXP и вложение классов полиномиальной иерархии в PSPACE.

21. Полиномиальные игры с полиномиальным числом ходов и класс PSPACE (теорема Сэвича).

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

23. PSPACE-полнота задачи об эквивалентности регулярных выражений.

24. Класс LOGSPACE. Принадлежность классу LOGSPACE задачи о достижимости в неориентированных графах. Принадлежность классу SPACE($\log^2 n$) задачи о достижимости в ориентированных графах.

25. Теорема Иммермана: NLOGSPACE=co-NLOGSPACE.

26. Интерактивные доказательства. Класс IP. Интерактивное доказательство неизоморфности данных графов.

27. Последовательное и параллельное повторение интерактивного доказательства уменьшает вероятность ошибки.

28. Вложение IP в класс PSPACE

29. Обратное вложение: PSPACE $\subset$ IP.

30. Интерактивные доказательства с открытыми бросаниями в конечное число раундов. Классы AM и MA. Включение MA в AM.

31. Интерактивные доказательства с нулевым разглашением.

32. Включение MA в Π_2 и MA в Σ_2.

33. Интерактивный протокол с открытыми бросаниями для задачи неизоморфности графов. Если задача изоморфизма графов является NP-полной, то $PH = \Sigma_2$.

34. Применение PCP-теоремы для доказательства неапроксимируемости кликового числа.

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

4. http://lpcs.math.msu.su/ ˜ ver/teaching/ComputationalComplexity/index.html