МФТИ, бакалавриат ФИВТ
2009, весенний семестр

Программа курса **Сложность вычислений**

Д.В. Мусатов, А.Е. Ромащенко

1. Многоленточные машины Тьюринга. Диагональная конструкция: существование невычислимых функций.
2. Основные сложностные классы: P, EXPTIME, PSPACE.
3. Теоремы об иерархии по времени и по зоне.
4. Недетерминированные вычисления, класс NP.
5. Сводимость по Карпу и сводимость по Куку. Понятие NP-полной и NP-трудной задачи.
6. Теорема Левина–Кука о NP-полноте задачи SAT.
7. Примеры NP-полных задач: 3КНФ, 3-раскраска, Вершинное покрытие, Клика, Гамильтонов цикл.
8. Схемы из функциональных элементов. Схемная сложность задач Parity и Majority. Вычисление суммы двух n-битовых чисел схемой логарифмической глубины и линейной сложности.
9. Два определение класса P/poly, их эквивалентность.
10. Полиномиальная иерархия.
11. Теорема Сэвича. PSPACE-полнота задачи БФК.
12. Вычисления на логарифмической памяти, классы L и NL. NL-полнота задачи PATH.
13. $\mathrm{NL} = \mathrm{coNL}$.
14. Вероятностные машины Тьюринга, классы BPP, RP, ZPP. Теорема об уменьшении вероятности ошибки.
15. Вероятностный алгоритм Рабина проверки простоты числа.
16. Теорема о вложени BPP в P/poly.
17. Теорема Гача: $\mathrm{BPP} \subset \Sigma_2^p \cap \Pi_2^p$.
18. Детерминированный и вероятностный коммуникационные протоколы вычисления предиката равенства.
19. Построение оракулов A и B таких, что $\mathrm{P}^A = \mathrm{NP}^A$ и $\mathrm{P}^B \neq \mathrm{NP}^B$.
20. Интерактивные доказательства. Задача Неизоморфизм-графов принадлежит классу IP.
21. Интерактивные протоколы с открытым датчиком случайных чисел; эквивалентность определений с секретными и открытыми датчиками случайных чисел: $\mathrm{AM}[\mathrm{poly}] = \mathrm{IP}[\mathrm{poly}]$.
22. $\mathrm{IP} = \mathrm{PSPACE}$.
23. Доказательства с нулевым разглашением. ZKP-протокол для задачи Изоморфизм-графов.

24. Вероятностно проверяемые доказательства, класс PCP(r, q). Формулировка PCP-теоремы.

Список литературы.

1. Ахо А., Хопкрофт Дж., Ульман Дж. Построение и анализ вычислительных алгоритмов. М.: Мир, 1979
2. Гэри М., Джонсон Д. Вычислительные машины и труднорешаемые задачи. М.: Мир, 1982.
3. Sipser. M. Introduction to the Theory of Computation. (Thomson course technology).
4. Arora S., Barak B. Computational Complexity: A Modern Approach. (Cambridge University Press).

Задачи для подготовки к экзамену.

1. Докажите, что следующие задачи распознавания принадлежат классу P: связный граф; граф без треугольников; двудольный граф; $\langle a, b, n, p\rangle$ такие, что $a^n = b \bmod p$ (числа a, b, n, p даны в двоичной записи)
2. Постройте схему сложености $O(n)$ для вычисление функции большинста n булевых значений $majority(x_1, \ldots, x_n)$.
3. $L = \{M$: машина на всяком входе длины n останавливается за $100n^3$ шагов$\}$ Принадлежит ли этот язык P? PSPACE?
4. Обозначим

   $EXPCOM = \{\langle M, x, 1^n\rangle$: машина M на входе x останавливается за 2^n шагов$\}$

   Докажите, что $\mathrm{P}^{EXPCOM} = \mathrm{NP}^{EXPCOM} = \mathrm{EXPTIME}$.
5. Докажите, что проблема остановки NP-трудна, но не NP-полна.
6. Докажите, что задача Гамильтонов-путь NP-полна.
7. $\mathrm{Time}(2^n) \neq \mathrm{Time}(2^{2n})$
8. $\mathrm{NTime}(n) \neq \mathrm{PSPACE}$
9. Обозначим UCYCLE класс всех неориентрованных графов, в которых есть цикл. Докажите, что UCYCLE принадлежит классу L.
10. Докажите, что язык 2SAT лежит в NL.
11. Если $\mathrm{P}^A = \mathrm{NP}^A$ то $\mathrm{PH}^A = \mathrm{NP}^A$.
12. Если NEXPTIME $\neq$ EXPTIME то P $\neq$ NP.
13. Если NP $\subset$ BPP то NP = RP.
14. XO =позиции в игре крестики-нолики на конечных квадратных досках, в которых у крестиков есть выигрышная стратегия (для выигрыша нужно поставить 5 крестиков подряд). Докажите, что $XO \in$ PSPACE
15. Придумайте интерактивное доказательство для свойства *x есть квадратичный невычет по модулю n* (не используя теорему IP = PSPACE).
16. Придумайте протокол с нулевым разглашением (со статистически точным моделированием журнала протокола) для свойства *x есть квадратичный вычет по модулю n.*
17. Если PSPACE $\subset$ P / poly, то PSPACE = AM[1] (AM[1] — игры Артура и Мерлина с 1-раундовым протоколом)