Мехмат МГУ. Программа курса
Алгоритмические методы в теории сложности.
(А.Е. Ромащенко, весна 2013).

1. Формальное определение понятия *алгоритм*. Алгоритмически разрешимые и алгоритмически неразрешимые задачи.
   - Формализация понятия «эффективный алгоритм». Определение сложностных классов P, BPP, RP, PSPACE.
   - Теоремы об иерархии по времени и памяти (для детерминированных вычислений).
   - Понятие переборной задачи.
2. Недетерминированные вычисления.
   - Два эквивалентных определения класса NP.
   - Сводимость по Карпу, понятие NP-полнота.
   - Теорема Кука–Левина: NP-полнота задач выполнимость и 3-КНФ.
3. Леммы об изоляции и их применение.
   - Две леммы об изоляции.
   - Вероятностный алгоритм поиска соврешенного паросочетания в двудольном графе по работе Вазирани–Вазирани–Малмалея (Vazirani–Vazirani–Mulmuley).
   - Вероятностный полиномиальный алгоритм сведения задачи о выполнимости булевой формулы к задаче о булевой формуле с единственным выполняющим набором.
   - Вероятностное сведения задачи о существовании в графе клики данного размера к задаче о существовании единственной клики данного размера.
   - Вероятностное сведение задачи SAT к задаче $\oplus$SAT.
   - Полиномиальная иерархия. Сложностной класс #P. Теорема Тода (Seinosuke Toda).
4. Интерактивные доказательства.
   - Интерактивные доказательства с открытыми и секретными случайными битами. Определение сложностных классов IP и AM.
   - Игра Артура и Мерлина для задачи неизоморфизм графов. Игра Артура и Мерлина для той же задачи с односторонней ошибкой.
   - Доказательство $\mathsf{IP}[\mathsf{poly}] = \mathsf{AM}[\mathsf{poly}]$ методом Килиана (Joe Kilian).
   - Определения доказательства с нулевым разглашением.
   - Доказательство с нулевым разглашением для задачи *изоморфизм графов*.

5. Ветвящиеся программы.

   Теорема Баррингтона (David A. Barrington): если для булевой функции существует булева схема глубины d, то её можно вычислить ветвящейся программой ширины 5 и длины $L \leq 4^d$.

   Следствие: Если функция вычислима булевой схемой логарифмической глубины, то эта функция вычислима ветвящейся программой полиномиальной длины ширины 5.

6. Метод самосводимости.

   - Самосводимость языка SAT. Теорема Махейни (Stephen Mahaney).
   - Эквивалентность существования NP-полного тощего множества и равенства P = NP. Эквивалентность существования NP-полного разреженного множества и равенства P = NP.
   - Вычисление с логарифмической памятью. Самосводимость задачи достижимости на ориентированном графе (достижима ли вершина t из вершины s за $\leq k$ шагов).
   - Теорема Сэвича (Walter Savitch): $\mathsf{Space}(f(n)) \subset \mathsf{Space}(f^2(n))$.
     Следствие: $\mathsf{NPSPACE} \subset \mathsf{NPSPACE}$.
   - Теорема Фортноу (Lance Fortnow): не существует алгоритма, решающего задачу SAT за время $n^{1+o(n)}$ с использованием памяти $O(\log n)$.

Список литературы

[1] Michael Sipser. Introduction to the theory of computation. CENGAGE Learning Custom Publishing, 2012.

[2] Sanjeev Arora and Boaz Barak. Computational Complexity: A Modern Approach. Cambridge, 2009.

[3] Lane A. Hemasphaandra, Mitsunori Ogihara. The Complexity Companion. Springer, 2002.

[4] Ketan Mulmuley, Umesh V. Vazirani. Vijay V. Vazirani. Matching as Easy as Matrix Inversion. Combinatorica, Volume 7, Issue 1, pp. 105–113, 1987.

[5] S. P. Vadhan. A Study of Statistical Zero-Knowledge Proofs. PhD thesis, Massachusetts Institute of Technology, 1999.

[6] O. Goldreich. Foundations of Cryptography, Volumes 1 and 2. Cambridge University Press, 2001, 2004.