Московский физико-технический институт (ГУ)
Факультет инноваций и высоких технологий
Бакалавриат кафедр анализа данных и дискретной математики
Сложность вычислений: дополнительные главы, 6-ой семестр
Программа курса

1. Общее понятие интерактивного протокола между доказывающим (прувером) и проверяющим (верификатором). Распознавание языков при помощи интерактивных протоколов. Точность и полнота распознавания.

2. Класс **dIP** языков, распознаваемых интерактивными протоколами с детерминированными полиномиальными верификаторами. Теорема: $\mathbf{dIP} = \mathbf{NP}$.

3. Класс **IP** языков, распознаваемых интерактивными протоколами с вероятностными полиномиальными верификаторами и полиномиальным числом раундов. Примеры: изоморфизм графов, квадратичные невычеты. Вариации определения: полнота может быть сделана единичной, а точность — отличной от единицы на экспоненциально малую величину. Существование оптимального прувера, работающего на полиномиальной памяти. Теорема: $\mathbf{IP} \subset \mathbf{PSPACE}$.

4. Интерактивные протоколы с общими случайными битами. Игры Артура–Мерлина, классы **AM** и **MA**. Семейства попарно независимых хеш-функций: определение, построение через конечные поля. Протокол Голдвассера–Сипсера для доказательства нижней оценки на размер множества. Построение **AM**-протокола для задачи неизоморфизма графов.

5. Идея арифметизации. Интерактивный протокол для задачи $\#\mathsf{SAT}_D$. Построение интерактивного протокола для задачи TQBF при помощи техники линеаризации. Следствие: $\mathbf{IP} = \mathbf{PSPACE}$.

6. Интерактивные протоколы с несколькими пруверами и класс **MIP**. Теорема: $\mathbf{MIP} \subset \mathbf{NEXP}$.

7. Совершенно, статистически и вычислительно нулевое разглашение в интерактивном протоколе: различные вариации определений. Классы **PZK**, **SZK** и **CZK**. Интерактивный протокол с совершенно нулевым разглашением для задачи об изоморфизме графов.

8. Криптография: односторонние функции, протокол привязки к сообщению. Интерактивный протокол с вычислительно нулевым разглашением для задачи о 3-раскраске. Теоремы $\mathbf{NP} \subset \mathbf{CZK}$ и $\mathbf{IP} \subset \mathbf{CZK}$: идеи доказательства.

9. Вероятностно проверяемые доказательства. Класс **PCP**. Приближённое решение **NP**-полных задач. Две формулировки **PCP**-теоремы: через класс **PCP** и через приближённое решение задачи SAT, их эквивалентность. Экспоненциальная **PCP**-теорема: $\mathbf{NP} \subset \mathbf{PCP}(\mathrm{poly}, 1)$. Теорема: $\mathbf{MIP} = \mathbf{PCP}(\mathrm{poly}, \mathrm{poly}) = \mathbf{NEXP}$. Идея доказательства основной **PCP**-теоремы: $\mathbf{NP} = \mathbf{PCP}(\log, 1)$.

Литература:

1. S. Arora, B. Barak, "Computational Complexity: A Modern Approach", Cambridge University Press, 2009 (Черновики доступны по адресу `http://www.cs.princeton.edu/theory/index.php/Compbook/Draft`)

2. O. Goldreich, "Foundations of Cryptography. Volume I: Basic Tools", Camridge University Press, 2001

Дополнительная литература:

3. J. Katz, "Notes on Complexity Theory", 2011
`http://www.cs.umd.edu/~jkatz/complexity/f11/all.pdf`

4. C. Papadimitriou, "Computational complexity", Addison Wesley, 1994

5. M. Sipser, "Introduction to the theory of computation", Course Technology, 2005

6. O. Goldreich, "Computational Complexity: a Conceptual Perspective", Cambridge University Press, 2008

Полезные сетевые ресурсы:

1. Андрей Станкевич, "Теория сложности", Викиконспекты НИУ ИТМО,
`http://neerc.ifmo.ru/wiki/index.php?title=Теория_Сложности`

2. Scott Aaronson, Charles Fu, Greg Kuperberg, Christopher Granade, "Complexity Zoo".
`https://complexityzoo.uwaterloo.ca/Complexity_Zoo`

3. Dick Lipton, "Gödel's Lost Letter and P=NP",
`http://rjlipton.wordpress.com/`

4. Scott Aaronson, "Shtetl-Optimized",
`http://www.scottaaronson.com/blog/`

5. Computational Complexity Blog,
`http://blog.computationalcomplexity.org/`

6. Вопросы и ответы по теоретической информатике
`http://cstheory.stackexchange.com/`