Московский физико-технический институт (ГУ)
Факультет инноваций и высоких технологий
Дерандомизация и псевдослучайность, технический курс по выбору
Программа курса, осень 2016

Аннотация

Некоторые задачи решаются рандомизированными алгоритмами. Некоторые алгоритмы, например, проверка простоты числа или проверка связности графа, были дерандомизированы, т.е. превращены в детерминированные из того же сложностного класса. Для других задач, прежде всего проверки арифметического выражения на тривиальность, дерандомизация пока неизвестна. Общий вопрос состоит в том, можно ли избавиться от случайных битов в общем случае или хотя бы существенно сократить их использованное количество. В курсе будет дан обзор классических результатов и новых продвижений по этой теме.

Список тем

1. Вероятностные алгоритмы и вероятностные сложностные классы. Проверка арифметического выражения на тривиальность. Проверка на достижимость в неориентированном графе.

2. Основные методы дерандомизации: перебор вариантов, неконструктивность, недетерминизм, метод условных математических ожиданий, попарная независимость.

3. Экспандеры (графы-расширители). Два определения, случайные блуждания, явные конструкции, решение задачи о достижимости в графе на логарифмической памяти.

4. Коды, декодируемые списком. Определение, существование, алгоритмы. Построение экспандеров на базе кодов Парвареша-Варди.

5. Экстракторы (графы, извлекающие случайность). Определение, существование, явные конструкции.

6. Генераторы псевдослучайных чисел. Генератор Нисана–Вигдерсона.

7. Экстрактор Тревисана и другие конструкции на базе генератора Нисана–Вигдерсона.

8. Обзор прочих псевдослучайных конструкций: дисперсеры, сэмплеры, суперконцентраторы и т.д.

Требования к слушателям

1. Знакомство с теорией сложности вычислений. Классы **P** и **NP**, полиномиальная сводимость, **NP**-полнота. Вероятностные алгоритмы, класс **BPP**.

2. Свободное владение методами комбинаторики, дискретной математики и линейной алгебры.

3. Знакомство с теорией марковских цепей.

Основная литература

1. S. Vadhan, "Pseudorandomness", Foundations and Trends® in Theoretical Computer Science: Vol. 7: No. 1–3, pp 1-336
`http://people.seas.harvard.edu/~salil/pseudorandomness/`

2. S. Arora, B. Barak, "Computational Complexity: A Modern Approach", Cambridge University Press, 2009 (Главы 19–21; черновики доступны по адресу
`http://www.cs.princeton.edu/theory/index.php/Compbook/Draft`)

Дополнительная литература

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

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

5. O. Goldreich, "Randomized Methods in Computation: Tentative Collection of Reading Material"
`http://www.wisdom.weizmann.ac.il/~oded/PDF/rnd.pdf`

Конспекты, видеолекции и полезные сетевые ресурсы

1. L.Trevisan, "Pseudorandomness",
`https://people.eecs.berkeley.edu/~luca/pacc/`

2. Д. М. Ицыксон, "Вычислительно трудные задачи и дерандомизация", видеолекции,
`http://compsciclub.ru/courses/hardnessvsrandomness/2009-spring/`

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

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

5. Scott Aaronson, “Shtetl-Optimized”,
   http://www.scottaaronson.com/blog/

6. Computational Complexity Blog,
   http://blog.computationalcomplexity.org/

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