

CMPT 881 - Pseudorandomness
Fall 2004

Instructor: Valentine Kabanets, email: kabanets@cs.sfu.ca

Lectures: Tue 16:30–17:20 and Thu 16:30–18:20, in AQ 5020

Instructor’s office hours: Tue 15:00–16:00 in ASB 9921, or by appointment

Course web page: www.cs.sfu.ca/~kabanets/cmpt881

Please refer to this page regularly for important information related to the course.

Prerequisites: Mathematical maturity. Basic knowledge of discrete math (probability, combinatorics, linear algebra) and basic computational complexity theory (P, NP).

Text: There is no single text for this course. We’ll be using various books, lecture notes, survey and research articles. Please see the course web page for a few pointers.

Course Outline: *Randomness is useful in a variety of areas of computer science: algorithm design, distributed computing, cryptography, complexity, etc. What is the exact power of randomness in such application? Is randomness required for an efficient solution, or can randomness be completely eliminated from the solution without much loss in efficiency? In this course, we will study a number ways of eliminating randomness from efficient computer algorithms without incurring significant slowdown. Almost all such results are conditional: assuming the existence of certain “hard” problems, one can reduce/eliminate randomness in any efficient algorithm. This dependence on “hard” problems turns out to be also necessary: any way of eliminating randomness from randomized algorithm will imply the existence of “hard” problems. On the other hand, proving that some problems are “hard” is a notoriously difficult task in complexity theory. Thus, the theory of pseudorandomness and the computational complexity theory are inextricably intertwined. Finally, while studying various constructions in the area of pseudorandomness, we will see some fascinating connections among such “random-like” objects as pseudorandom generators, error-correcting codes, expander graphs, and randomness extractors.*

Topics to be covered will include some of the following:

- Randomized algorithms (Polynomial Identity Testing, approximate counting, etc.)
- Random walks on graphs, Markov chains
- Expander graphs and their applications
- Randomness extractors
- Pseudorandom generators (cryptography and derandomization)
- Special-purpose derandomization: Pairwise independence, epsilon-biased sets, etc.
- General-purpose derandomization: Hardness-based Pseudorandom Generators (NW generator and its variants)
- List-decodable error correcting codes

- Derandomization of space-bounded randomized algorithms (Nisan’s generator)
- Derandomization and circuit lower bounds, “uniform-setting” derandomization

Marking scheme:

2 homeworks, worth 20% each,
a project, worth 40%,
scribe notes, worth 20%.

Academic honesty: Academic Honesty plays a key role in our efforts to maintain a high standard of academic excellence and integrity. Students are advised that ALL acts of intellectual dishonesty are subject to disciplinary action by the School; serious infractions are dealt with in accordance with the Code of Academic Honesty (T10.02) (<http://www.sfu.ca/policies/teaching/t10-02.htm>). Students are encouraged to read the School’s Statement on Intellectual Honesty (<http://www.cs.sfu.ca/undergrad/Policies/honesty.html>).