CS286C-02: Pseudorandomness and combinatorial constructions

Course description: The use of randomness is pervasive in modern algorithm design and other settings. Allowing an algorithm to flip coins can greatly simplify its description and implementation, and in some cases randomized solutions are the only efficient ones known. In this course we study randomness as a computational *resource*, to be conserved just as the more traditional resources of running time or storage space. One motivation for this study is that it is difficult for computers to access truly random bits, so it is desirable to make do with as few as possible. Another motivation is that several of the most important open problems in Computational Complexity turn on the question of whether the use of randomness can be removed in certain settings.

The theory of *pseudorandomness* provides a uniform way to approach these questions. Here the goal is to explicitly construct combinatorial objects that *appear* random to a limited class of tests. We will examine a variety of objects (expander graphs, randomness extractors, pseudorandom generators, others) from this perspective. In some cases we will be able to unconditionally construct explicit objects with certain well-defined "random-like" properties; in other cases our constructions will rely on a complexity assumption. Along the way we will encounter many open problems.

This course is intended to be a largely self-contained, graduate-level introduction to this very active research area.

Course information:

- Instructor: Chris Umans (`umans@cs.caltech.edu`)
- Lectures: Tuesdays and Thursdays 1:00 – 2:25 in Jorgensen 287
- Office hours: TBD
- Text: there is no text; the webpage will contain links to relevant papers and lecture notes.
- Webpage: `http://www.cs.caltech.edu/~umans/cs286/`

Course requirements: Attend lectures, read and present a paper, or produce scribed lecture notes for 1-2 lectures.

(Very) tentative lecture schedule:

#	Date	Subject
1	Mar. 28	Introduction; error-correcting codes
2	Mar. 30	k-wise and ϵ-biased spaces and hash functions
3	Apr. 4	expanders and their applications, Zig-Zag construction
4	Apr. 6	Zig-Zag expander construction continued
5	Apr. 11	randomness extractors and their applications, construction based on hashing
6	Apr. 13	Trevisan extractor construction
7	Apr. 18	an algebraic extractor construction
8	Apr. 20	randomness condensers and a construction
9	Apr. 25	pseudorandom generators (PRGs), Nisan-Wigderson construction
10	Apr. 27	constructing average-case hard functions from worst-case hard ones
11	May 2	an algebraic pseudorandom generator construction
12	May 4	PRGS against higher and lower classes
13	May 9	PRGs for logspace
14	May 11	PRGs for logspace
15	May 16	Guest lecture?
16	May 18	Guest lecture?
17	May 23	Reingold's unconditional derandomization of symmetric logspace
18	May 25	Reingold's unconditional derandomization of symmetric logspace
-	May 27 – June 2	paper presentations