Pseudorandomness and Combinatorial Constructions (CS 395T)

Time/Location/Unique Number. TTh 3:30–5:00, TAY 3.144, #51110.

Instructor. David Zuckerman (`diz@cs`), TAY 3.134, 471–9729.

Office hours. TTh 5:00–6:00 or by appointment.

Course overview. Randomization is very useful in almost all areas of computer science, such as algorithms, cryptography, and distributed computing. These uses of randomness seem wonderful until one realizes that computers do not use truly random bits. Instead, most computers get their random bits by using pseudorandom generators. A pseudo-random generator is a deterministic algorithm that takes as input a short random seed and outputs a long string which is "random" enough for the purpose at hand.

In this course, we will develop provably good pseudorandom generators for a variety of tasks. Along the way, we will frequently require explicit combinatorial constructions. That is, we will want to efficiently and deterministically construct a combinatorial object whose existence is easily ensured by the probabilistic method. In fact, a pseudorandom generator is such an object.

Topics.

1. Introduction – randomized algorithms, probabilistic method
2. Algebraic and combinatorial constructions
   (a) Polynomials and k-wise independence
   (b) ϵ-biased spaces and almost k-wise independence
   (c) Error-correcting codes and list decoding
   (d) Expanders
   (e) Ramsey theory
3. Pseudorandomness
   (a) Leftover Hash Lemma
   (b) Extractors and their applications
   (c) Pseudorandom generators for space-bounded machines
   (d) General pseudorandom generators from hardness assumptions

Grading. Problem sets 65%, project 35%.

Scribing. Each class will have a scribe, who takes good notes and typesets them. I will review each of the scribed notes. Each person will have to scribe two or three times.

Problem set guidelines. I encourage collaboration. However, please write up solutions separately, and list the names of collaborators.

Projects. A typical project will consist of understanding and presenting one or more papers. Original research would be even better. I expect students to work on projects in groups of two or three. I will discuss topics later in the course.

Prerequisite. CS388T or CS388G or equivalent level of mathematical and computational sophistication.

Web page. `http://www.cs.utexas.edu/users/diz/395T/index.html`