CS289: Pseudorandomness, Winter 2016
Monday/Wednesday 2–4

1 Course Goals

The course will cover the basics as well as some of the state-of-the-art results in pseudoranodmness, explicit constructions in combinatorics, and their applications. The main goal is to introduce the many questions and ideas in pseudorandomness and to cover versatile tools that are useful in other areas such as discrete mathematics (e.g., expanders), algorithms (e.g., hashing, streaming algorithms), and cryptography (extractors, hardness vs randomness).

2 Syllabus

The following is a tentative list of topics to be covered.

- Pseudorandomness: Why, what, and how? (2 lectures)
  - Randomized algorithms.
  - Probabilistic method.
  - What is pseudorandomness?
- Limited independence: The swiss-army knife. (2 lectures)
  - Universal hashing, k-wise independence.
  - Constructions, applications.
- Error correcting codes (2 lectures)
  - Small-bias spaces.
  - Reed-Solomon codes.
- Expander graphs (3 lectures)
  - The many views of expansion.
  - Applications of expanders.
  - Zig-Zag product construction of expanders.
- Extractors (2 lectures)
  - Expanders beating the eigenvalue bound.
  - Applications and connections to codes.
  - Leftover hash lemma.
- Hardness vs randomness (3 lectures)
  - Why should derandomization be possible?
  - Impagliazzo-Wigderson theorem.
- Randomness to hardness (2 lectures)
  - Polynomial identity testing.
  - Kabanets-Impagliazzo result and analogues.

- Pseudorandomness for small-space machines and branding programs (3 lectures)
  - Applications to streaming algorithms.
  - INW PRG.
  - Undirected st-connectivity in log-space

3 Course Grading

The students will have to write lecture notes for the classes; this will account for (20%) of the grade; there will be three assignments (30%), one mid-term (20%), and one final (30%). The grading will also be flexible: students can, if they choose to, exchange an homework for more scribing duties or an approved research project for the final exam.

Writing: The assignments and scribe notes will have to be done using LaTeX. Grades will take into account both the correctness and the quality of the solutions.

Correctness is a prerequisite but clarity is also important: you are responsible for communicating your solution in a simple and understandable way. Sloppy answers will receive fewer or no points even if they are 'correct'. Unless otherwise specified, all answers will need to be throughly justified with complete proofs.

4 Cource Policy

There will be no makeup exams for the course. The mid-term will be held in class.

5 Required Course Text

There is no required course text. Links to appropriate papers or other online material (typically other lecture notes) will be provided for each lecture.