CS 744: Pseudorandom Generators

In computer science, randomization is a powerful notion which gives rise to simple and efficient solutions to problems. To some of these problems, efficient deterministic solutions have proved elusive. It is however, our ultimate aim to gain deterministic solutions to our problems. A systematic strategy which we follow is to derive a randomized solution, and then *derandomize* - *i.e.* remove the amount of randomness used - the algorithm to attain a deterministic one. In the field of computational complexity, we hope to derandomize *classes of algorithms* using general techniques, rather than derandomize specific algorithms using special techniques.

We believe, based on our past experience relating *computational hardness* to randomness, that every randomized polynomial-time algorithm making only bounded errors can be fully derandomized – this is the BPP=P conjecture, which is one of the major open problems in theoretical computer science. Crucial to this line of work is the notion of pseudorandom generators — algorithms which use a limited amount of randomness to produce much longer strings which look "sufficiently random" to fool certain statistical tests.

In the course, we will study conditional results about pseudorandomness and derandomization, and explicit constructions of such pseudorandom objects like expanders and extractors.

The course assumes background in linear algebra and discrete probability theory. Grades will be based on assignments, exams and presentation of research papers.

References

1. Goldreich, O. *Foundations of Cryptography*, vol 1, Cambridge University Press, 2001.

2. Vadhan, S. *Pseudorandomness.* Foundations and Trends in Theoretical Computer Science: Vol. 7: No. 13, pp 1-336, now publishers, December 2012.

In addition, we will refer to the original research articles.