CS 101

OM schedule for: OM on 1/4/16 room 106 at 5:00 pm
Units: 2-0-8
Instructor: Gil Cohen's

Title: Randomness-Extractors Theory

Short description:

Generally speaking, a randomness extractor is an algorithm that produces truly random bits given a sample from one or more "weak" sources of randomness. Extractors are central objects in theoretical computer science that have found many applications to complexity theory, cryptography, data structures, and combinatorics, to name a few.
Randomness-extractors theory is a vibrant research field that makes frequent use of coding theory, additive combinatorics, Fourier analysis, and more.

In this course we will cover constructions of the main two types of extractors -- seeded extractors and multi-source extractors. More intrinsic primitives such as mergers, condensers, non-malleable extractors, and correlation breakers will be presented as well. We will discuss some applications to privacy, data structures, and Ramsey theory, among others.