Randomness Extractors and Pseudorandom Generators

Luca Trevisan, EECS, UC Berkeley

A randomness extractor is a procedure that converts an arbitrary distribution of sufficiently large entropy into an almost uniform distribution; a pseudorandom generator is a procedure that converts a short random input into a long(er) output that is "indistinguishable" from uniform. (Here "indistinguishable" is a technical term, whose definition is non-trivial, but whose interpretation is the one you would expect.)

Both randomness extractors and pseudorandom generators are very useful constructs, and rich theories are devoted to the goal of giving explicit and efficient constructions of them, and to exploit them in several applications. They also look, on the surface, like very different objects: randomness extractors deal with "information-theoretic" randomness, and used to be constructed with tools such as hash functions and expanders graphs; pseudorandom generators deal with a "computational" view of randomness, and are constructed with methods from complexity theory, using hard computational problems.

In this talk we will show that pseudorandom generators of a certain type (in particular, the Nisan-Wigderson generator and variants of it) can be turned into extractors. Our result has been used in some new extractor constructions in the last two years, and it displays a previously unsuspected way of "translating" results from the computational to the information-theoretic view of randomness.