

1116-68-96

**Boaz Barak\*** ([info@boazbarak.org](mailto:info@boazbarak.org)). *A different kind of pseudo.*

In this talk I will describe a different type of “pseudo-randomness” that is the computational analog of Bayesian statistics in the same way that standard pseudorandomness can be considered as the computational analog of frequentist statistics. It can also be thought of as relating to standard pseudorandomness in the same way that proof complexity relates to algorithmic complexity.

A pseudo-distribution  $X$  reflects the uncertainty that a computationally bounded observer has about a certain quantity. It can be thought of as the “distribution” that respects all the facts that can be derived about this quantity using a computationally bounded proof system. It is not necessarily an actual distribution and can in fact assign negative probabilities to elements in the domain, as long as this cannot be detected by a bounded observer.

I will formally define pseudo-distributions (w.r.t a particular proof system) and explain how they can be used in the context of analyzing the performance of the Sum-of-Squares algorithm on various computational problems. (Received July 22, 2015)