Nexus of Information and Computation Theories

January 25 – 29, 2016

Tutorials

Concentration of Measure
Sudeep Kamath (Princeton)

In classical probability theory, the law of large numbers and the central limit theorem provide sharp guarantees on how the average of a large number of independent and identically distributed random variables concentrates around its mean. In recent years, it has been discovered that this behavior is shared by various families of functions of independent random variables. Quantifying this concentration has become an important research area, and has found applications in numerous fields.
In this tutorial, we will explore fundamental inequalities related to concentration of measure. Specific topics include the Efron-Stein-Steele inequality, hypercontractive inequalities, log-Sobolev inequalities, and the entropy method. The role played by information theory will be stressed when present. We will also discuss applications to concrete problems in combinatorics, information theory, and probability theory.
Background: A basic familiarity with probability theory will be helpful (eg. a graduate-level first course in probability theory will be more than sufficient). A basic familiarity with information theoretic quantities such as entropy, mutual information, and relative entropy (or Kullback-Leibler divergence) will also be very useful in following the tutorial. We will spend some time reviewing this material and no pre-requisites are assumed.

Algorithmic Aspects of Inference
Ankur Moitra (MIT)

Parametric inference is one of the cornerstones of statistics, but much of the classic theory revolves around asymptotic notions of convergence and relies on estimators that are hard to compute (particularly in high-dimensional problems). In this tutorial, we will explore the following questions:
(1) For some of the fundamental problems in statistics, are there surrogates for the maximum likelihood estimator that also converge at an inverse polynomial rate to the true parameters, but in contrast can be computed efficiently?
(2) Can we establish tradeoffs between sample complexity and computational complexity? And what types of hardness assumptions allow us to explore this space?
We will cover topics such as the method of moments, learning mixture models, tensor decomposition, sparse PCA and matrix/tensor completion.

Communication Complexity and Information Complexity
Anup Rao (University of Washington)

The study of efficient communication communication using tools from information theory has led to many interesting results for basic problems in the last few decades. In this mini-course, we shall learn the basic concepts of communication complexity and see some its applications to distributed computing, data structures and complexity theory, stressing the central role played by information theory in this arena.

Privacy and Security via Randomized Methods
Guy Rothblum (Samsung Research America)

Randomness plays a fundamental role in the modern study of cryptography. From the work of Shannon, it was known that randomness is essential to secure communication. Modern cryptography, however, has extended and deepened this understanding. Foundational security notions, such as semantically secure encryption, inherently rely on randomized encryption methods. Computational notions of entropy let us stretch short secret keys to encrypt long messages. Allowing randomization and interaction in proof systems opens new possibilities such proving statements in "zero knowledge", conveying nothing beyond its validity.
More recently, randomness plays a central role in the study of privacy-preserving data analysis. Statistical analysis of sensitive data may yield valuable results, but it also poses serious threats to individuals' privacy. Differential privacy uses randomized methods to address these conflicting concerns, and has emerged as a rigorous and powerful framework for privacy-preserving data analysis.
This tutorial will review some prominent examples of the interplay between randomness and security/privacy, with an emphasis on the emerging study of privacy-preserving data analysis using differential privacy.