Differential Privacy and Bayesian Computation: Two Vignettes

A seminar by Vinayak Rao

Purdue University - USA

Friday 2 Dec 2022 | 12:30 p.m.
Room Benvenuti and live Zoom
Department of Statistical Sciences

Differential privacy (DP) protects privacy by introducing additional randomness into a recorded dataset. It comes with strong theoretical guarantees, and has become a state-of-the-art framework for privacy protection. In this talk, we consider two complementary challenges raised by DP. In the first part, we recognize that implementing DP mechanisms require sampling algorithms like MCMC or rejection sampling. In these instances, the algorithm runtime itself can leak privacy, so that practical implementations fail to maintain the original theoretical guarantees. To address this, we propose modifications to rejection and adaptive rejection sampling algorithms, with varying assumptions, to protect against timing attacks. In the second part, we focus on a more traditional statistics problem related to differential privacy: given access to only the privatized data, how to perform valid statistical inference on parameters underlying the confidential data. Here, the likelihood function of the privatized data requires integrating over the large space of confidential databases and is typically intractable, resulting, in Bayesian settings, in a posterior distribution that is doubly intractable. We propose a generic MCMC framework which is applicable to a wide range of statistical models and privacy mechanisms. Our MCMC algorithm is a simple wrapper that extends MCMC algorithms for the unobserved confidential data to settings where the data is privatized. Our approach translates privacy guarantees of the DP mechanism into mixing properties of the MCMC algorithm, while maintaining the same order of computational cost as the algorithm for non-privatized data. We illustrate the efficacy and applicability of both our ideas on several examples.

800 ANNI 1222·2022 UNIVERSITÀ DEGLI STUDI DI PADOVA
DIPARTIMENTO DI SCIENZE STATISTICHE