On robustness and local differential privacy

A seminar by Thomas Berrett

Department of Statistics - University of Warwick (UK)

Thursday 11 Apr 2024 | 2.30 p.m.
Room Benvenuti
Department of Statistical Sciences

It is of soaring demand to develop statistical analysis tools that are robust against contamination as well as preserving individual data owners' privacy. In spite of the fact that both topics host a rich body of literature, to the best of our knowledge, we are the first to systematically study the connections between the optimality under Huber's contamination model and the local differential privacy (LDP) constraints. We start with a general minimax lower bound result, which disentangles the costs of being robust against Huber's contamination and preserving LDP. We further study four concrete examples: a two-point testing problem, a heavy-tailed mean estimation problem, a nonparametric density estimation problem and a univariate median estimation problem. For each problem, we demonstrate procedures that are optimal in the presence of both contamination and LDP constraints, comment on the connections with the state-of-the-art methods that are only studied under either contamination or privacy constraints, and unveil the connections between robustness and LDP via partially answering whether LDP procedures are robust and whether robust procedures can be efficiently privatised. Overall, our work showcases a promising prospect of joint study for robustness and local differential privacy.
This is joint work with Mengchu Li and Yi Yu

Università degli Studi di Padova

Dipartimento di Scienze Statistiche