Instance Optimality in Differential Privacy

Ke Yi

February 8, 2025

Because of its mathematical rigor and applicability to a broad class of problems, differential privacy (DP) has now become the de facto standard for protecting personal information, widely adopted by both governments and industry. Most classical DP mechanisms are based on the sensitivity of the target function, but many basic functions, such as sum, mean, median, max/min, as well as most SQL queries, do not have a bounded sensitivity. For such functions, existing algorithms often take an ad hoc approach when measuring their utility. In this talk, I will present a unified and principled framework to define the optimality of DP mechanisms for such functions, based on a slightly relaxed notion of instance optimality, and show how this can be achieved for the aforementioned problems.