The Hong Kong University of Science and Technology

Department of Mathematics

PhD THESIS EXAMINATION

Differentially Private Learning with Streaming and Distributed Data

By

Mr. Zhicong LIANG

ABSTRACT

Differential privacy (DP) has become a popular topic in recent machine learning algorithm designs in demand for protecting sensitive personal data. In the first part of this paper, we study differentially private stochastic convex optimization (DP-SCO) with streaming data and continual release requirement, which is known as the online setting. Despite that numerous algorithms have been developed to achieve the optimal excess risks in different ℓ_p norm geometries, yet none of the existing ones can be adapted to the streaming and continual release setting. To address such a challenge, we propose a private variant of online Frank-Wolfe algorithm with recursive gradients. Combined with the adaptive differential privacy analysis, our online algorithm achieves in linear time the optimal excess risk when $1 < p \leq 2$ and the state-of-the-art excess risk meeting the non-private lower ones when $2 < p \leq \infty$. Our algorithm can also be extended to the case $p = 1$ to achieve nearly dimension-independent excess risk. In the second part, we consider differentially private federated learning (DP-Fed) where multiple data owners, referred to as clients, can cooperatively learn a useful model without disclosing their sensitive data. A key observation is that the federated average of gradients are often smooth or sparse in Fourier basis with polynomial decays, based on which we apply Laplacian Smoothing (DP-Fed-LS) to reduce variance with improved estimates of such gradients. Under heterogeneous data distributions, the rates on convergence bounds and communication complexity of our proposed algorithm match those on federated learning without differential privacy, or the ones of empirical risk minimization (ERM) via SGD with differential privacy in a centralized setting. We demonstrate the utility of our algorithm with comprehensive numerical experiments.

Date : **11 November 2022, Friday**

Time : **10:30 a.m.**

Venue : **Room 4472 (Lifts 25-26)**

Zoom ID: **403 313 6156 (passcode: 202211)**
https://hkust.zoom.us/j/4033136156

***Thesis Examination Committee*:**

Chairman	**:**	**Prof. Yingying LI, ISOM/HKUST**
Thesis Supervisor	**:**	**Prof. Yuan YAO, MATH/HKUST**
Member	**:**	**Prof. Tong ZHANG, MATH/HKUST**
Member	**:**	**Prof. Can YANG, MATH/HKUST**
Member	**:**	**Prof. Wei YOU, IEDA /HKUST**
External Examiner	**:**	**Prof. Yongxin TONG,** **Department of Computer Science and Engineering/ Beihang University**

(Open to all faculty and students)

The student's thesis is now being displayed on the reception counter in the General Administration Office (Room 3461).