On PAC Learning Halfspaces in Non-interactive Local Privacy Model with Public Unlabeled Data

Jinyan Su Jinhui Xu Di Wang

Part of the work was done when Jinyan Su was a research intern at KAUST

ACML
Asian Conference on Machine Learning

Problem setting

- Probably approximately correct (PAC) learning halfspaces.

  $$\underset{(x,y)\sim\mathcal{P}}{Pr}[y \neq \text{sign}(\langle \hat{w}, x \rangle)] \leq \alpha \text{ w.p. } 1-\beta$$

- Locally differentially private (LDP)

  $$Pr[\mathcal{A}(x) \in E] \leq e^{\epsilon} Pr[\mathcal{A}(x^{'}) \in E] + \delta$$

- Non-interactive

  $$T = 1$$

- **Additional public unlabeled data**

  $$q \sim \mathcal{P}_x$$

Via Massart Noise model

Massart Noise

Label are flipped w.p. $\leq \lambda$

1. Private part:
   Construct **Massart Noise example oracle** $\hat{f}$

   - Devide Private data into k **disjoint** groups
   - Using NLDP algorithm in [Wang et al.(2020)] for each groups of data
   - Boost accuracy by majority voting $\Rightarrow \hat{f}$ **with** $\lambda = \frac{3}{16}$

Private data: $\tilde{O}(d\text{Ploy}(\frac{1}{\epsilon}, \frac{1}{\alpha}))$

Public data: $O(\frac{d}{\alpha^4})$

2. Non-private part:
   - Label public data with $\hat{f}$
   - Invoke Non-private algorithm for **learning half spaces with Massart Noise**

Via Self-supervised learning

1. Private part
   - Use **Logistic Loss** NLDP⇒w^{priv}

Pseudo labeler
Sufficiently small but constant error C_{err}

2. Non-private part
   Convert weak learner to strong learner⇒**Self-training**
   - Label unlabeled data with pseudo labeler
   - **Gradient descent** on pseudo labeled data⇒ **Update pseudo labeler**

Private data: $\tilde{O}(d\text{Ploy}(\frac{1}{\epsilon}, \frac{1}{\alpha}))$

Public data: $O(\frac{d}{\alpha^2})$