Advanced Topics in Machine Learning (2024)
Assignment 5

October 24, 2024

Question 1

Pseudocode of the algorithm

Algorithm 1

Require: Dataset $D \in (\mathcal{X} \times \mathcal{Y})^n$, finite hypothesis class $\mathcal{H}_d$, privacy parameter ϵ

1: Compute $\mathcal{R}(h; D)$ for each $h \in \mathcal{H}_d$
2: Select $\hat{h}$ with probability $Pr[\hat{h} = h] \propto \exp(-\frac{\epsilon n}{2} R(h; D))$
3: **return** $\hat{h}$

Proof of the privacy

Denote D' as the neighboring dataset of D. Given that

$$\mathcal{R}(h; D) = \frac{1}{n} \sum_{i}^{n} \mathbf{1}\{h(x_i) \neq y_i\} \tag{1}$$

then denote $\mathcal{K} : D \to \mathcal{H}_d$ as $\arg\min_{h \in \mathcal{H}} \mathcal{R}(h; D)$

$$\max_{D, D'} |\mathcal{K}(D) - \mathcal{K}(D')| = \frac{1}{n} \tag{2}$$

According to the exponential mechanism where the score function is $-R(h; D)$, it satisfies ϵ-DP.

Proof of utility

According to the Hoeffding's inequality,

$$\begin{aligned} Pr_{S \sim D, \hat{h} \sim \mathcal{A}_{DP}(S)}[|R(\hat{h}; S) - \mathbb{E}[R(\hat{h}; S)] > \delta] \leq 2 \exp(-2n\delta^2) \\ Pr_{S \sim D, \hat{h} \sim \mathcal{A}_{DP}(S)}[|R(\hat{h}; S) - R(\hat{h}; D)| > \delta] \leq 2 \exp(-2n\delta^2) \end{aligned} \tag{3}$$

According to the union bound,

$$Pr_{S \sim D}[\exists \hat{h} \in \mathcal{H}_d, |R(\hat{h}; S) - R(\hat{h}; D)| > \delta] \leq 2|\mathcal{H}_d| \exp(-2n\delta^2) \tag{4}$$

Let $2|\mathcal{H}_d| \exp(-2n\delta^2) = \frac{\beta}{2}$, then $\delta = \sqrt{-\frac{\log(\beta/4|\mathcal{H}_d|)}{2n}}$, and

$$Pr_{S \sim D}[\forall \hat{h} \in \mathcal{H}_d, |R(\hat{h}; S) - R(\hat{h}; D)| \leq \delta] \geq 1 - \frac{\beta}{2} \tag{5}$$

According to the theorem of utility in exponential mechanism:

$$\mathbb{P}\left[\sigma\left(\mathcal{M}_E\left(S,\mathcal{O},\sigma\right),S\right)\leq \mathrm{OPT}_\sigma\left(S\right)-\frac{2\Delta_\sigma}{\epsilon}\left(\log\left(\frac{|\mathcal{O}|}{|\mathcal{O}_{\mathrm{OPT}}\left(S\right)|}\right)+t\right)\right]\leq \exp\left(-t\right) \quad (6)$$

where the score function is $-R(h,D)$. Let $t=\log(\frac{2}{\beta})$, we have

$$\Pr\left[R(\hat{h};D)\leq \min_{h\in\mathcal{H}_d} R(h;S)+\frac{2}{\epsilon n}\left(\log\left(\frac{|\mathcal{H}_d|}{|\mathcal{O}_{\mathrm{OPT}_\sigma(S)}|}\right)+\log(2/\beta)\right)\right]\geq 1-\frac{\beta}{2} \quad (7)$$

Denote event (5) and (7) as A and B(the opposite of event B), $P(A\cap B)=1-P(A'\cup B')$. According to the union bound $P(A\cap B)\geq 1-(\frac{\beta}{2}+\frac{\beta}{2})=1-\beta$. When A and B happens at the same time, we have $R(\hat{h};D)\leq R(\hat{h};S)+\delta$

$$Pr_{S,\hat{h}\sim\mathcal{A}_{DP}}[R(\hat{h};D)\leq\alpha)]\geq 1-\beta \quad (8)$$

where

$$\alpha\geq R(h^*;D)+\frac{2}{\epsilon n}\left(\log\left(\frac{|\mathcal{H}_d|}{|\mathcal{O}_{\mathrm{OPT}_\sigma(S)}|}\right)+\log(2/\beta)\right)+\sqrt{-\frac{\log(\beta/4|\mathcal{H}_d|)}{2n}} \quad (9)$$

Calculate the expectation of both sides. Given that the right side is independent of different $\hat{h}$, it remains unchanged. Hence,

$$Pr_S[\mathbb{E}[R(\hat{h};D)]\leq\alpha)]\geq 1-\beta \quad (10)$$

Question 2

Pseudocode of the algorithm

Algorithm 2

Require: Data set $D=(\mathcal{X}\times\mathcal{Y})^n$, VC dimension d, hypothesis class $\mathcal{H}_d$, parameters ϵ.

1: Apply Sauer-Shelah lemma to $\mathcal{H}_d$ to find a finite set of hypothesis $\mathcal{H}'_d\subseteq\mathcal{H}_d$, such that $\mathcal{H}'_d$ sufficiently approximates $\mathcal{H}_d$.
2: Compute $\mathcal{R}(h;D)$ for each $h\in\mathcal{H}'_d$
3: Select $\hat{h}$ with probability $Pr[\hat{h}=h]\propto\exp(-\frac{\epsilon n}{2}R(h;D))$
4: **return** $\hat{h}$

Proof of privacy

Given that sensitivity of the function remains unchanged, it is as same as Question 1. According to the exponential mechanism, it satisfies ϵ-DP.

Proof of utility

Given that $|\mathcal{X}_p|\leq\exp(p)$, according to Sauer-Shelah lemma, $|\mathcal{H}'_d|\leq\exp(O(dlog(\frac{p}{d})))$.

Substitute it into the previous theorem,

$$\alpha\geq 2\sqrt{\frac{O(d\cdot\log(p/d)+\log(2/\beta))}{2n}}+\frac{2}{\varepsilon n}O(d\cdot\log(p/d)+\log(2/\beta)) \quad (11)$$

then, we have

$$n=O\left(\frac{d\cdot\log(p/d)+\log(1/\beta)}{\alpha^2\varepsilon}\right) \quad (12)$$

This is a polynomial in terms of d, p, $1/\alpha$, $1/\varepsilon$, and $\log(1/\beta)$, which corresponds the setting of the problem.

Question 3

From the perspective of statistics, more data is required by private PAC learning to achieve the same error bound compared to non-private PAC learning due to the need to protect privacy.

From the perspective of computation, private algorithms often involve additional steps, like noise addition or sampling, which increase runtime complexity. In contrast, non-private learning can directly minimize empirical risk without these privacy constraints, requiring fewer computations and less data for comparable error rates.