Advanced Topics in Machine Learning (2024)
Assignment 4

October 10, 2024

Question 1

Pure DP is more restrictive than z-CDP

Denote A_{DP} is a DP algorithm, S and S' are neighboring datasets. For pure DP, $\Pr_{Z\sim\text{PrivLoss}(A_{DP}(S)||A_{DP}(S'))}(Z \geq \epsilon) = 0$, while for z-CDP, $\Pr_{Z\sim\text{PrivLoss}(A_{DP}(S)||A_{DP}(S'))}(Z \geq \epsilon) = 0 \leq \exp(-\frac{(\epsilon-\rho)^2}{4\rho})$. So pure DP is more restrctive.

z-CDP is more restrictive than RDP

Denote $D_\alpha(p||q)$ is Renyi Divergence for distribution p and q. According to the definition of these two algorithms, for RDP, it is required that $D_\alpha(A_{DP}(S)||A_{DP}(S') \leq \epsilon(\alpha)$, which means the privacy parameter is related to a specific α. While for z-CDP, it is required for any $\alpha \in (1, +\infty)$, $D_\alpha(A_{DP}(S)||A_{DP}(S') \leq \rho\alpha$. So z-CDP is more restrictive.

RDP is more restrictive than Approx DP

For Approx DP, it is required that $\Pr_{Z\sim\text{PrivLoss}(A_{DP}(S)||A_{DP}(S'))}(Z \geq \epsilon) \leq \epsilon$, where ϵ is a constant. While for RDP, it is required $\Pr_{Z\sim\text{PrivLoss}(A_{DP}(S)||A_{DP}(S'))}(Z \geq \epsilon) \leq \exp((\alpha-1)(\epsilon'-\epsilon))$, which is sub-exponential. So RDP is more restrictive.

Question 2

a

Given that $L = \epsilon_0 \leq \epsilon_0$, according to the definition of pure DP, it is ϵ_0-DP.

b

Given that $L \leq \epsilon_1$, according to the definition of pure DP, it is ϵ_1-DP.

c

Given that

$$\begin{aligned}
\mathbb{E}[e^{\lambda L}] &= \int_{-\infty}^{+\infty} e^{\lambda L} \cdot \frac{1}{\sqrt{2\pi\sigma^2}} e^{\frac{L^2}{2\sigma^2}} \, dL \\
&= \frac{1}{\sqrt{2\pi\sigma^2}} \int_{-\infty}^{+\infty} e^{\lambda L + \frac{L^2}{2\sigma^2}} \\
&= e^{\frac{\lambda^2\sigma^2}{2}} \text{(Gaussian integral)}
\end{aligned} \tag{1}$$

. According to the definition, it is $\rho - z$CDP.

d

Given that

$$\begin{aligned}\int_{\epsilon}^{+\infty} f(L) &= \frac{1}{2b}\int_{\epsilon}^{+\infty} e^{-\frac{|L|}{b}} \\ &= \frac{1}{2}e^{-\frac{\epsilon}{b}}\end{aligned} \tag{2}$$

And it is easy to find a pair of α' and ϵ' to satisfy that $\frac{1}{2}e^{-\frac{\epsilon}{b}\leq \exp((\alpha-1)(\epsilon'-\epsilon))}$. When $\epsilon' > blog2$ and $\alpha < \frac{1}{b}+1$

$$\begin{aligned}(\alpha-1)(\epsilon-\epsilon') &\leq \frac{\epsilon}{b} + log2 \\ -\frac{\epsilon}{b} &\leq (\alpha-1)(\epsilon'-\epsilon) - log2 \\ \frac{1}{2}e^{-\frac{\epsilon}{b}} &\leq \exp((\alpha-1)(\epsilon'-\epsilon))\end{aligned} \tag{3}$$

According to the definition, it is RDP.

e

Given that $L \leq \epsilon_2$, according to the definition of pure DP, it is ϵ_2-DP.

Question 3

There is a point set with size n, $\{x_1, x_2, ..., x_n\}$, and each element of this set is a vertex of the convex n-sided polygon C_1. For any label distribution, where there is k positive labels, we can produce a convex k-sided polygon C_2 by connecting all k points with positive labels. Then c_{C_2} can separate all points. Hence, $\mathcal{C}$ can shattered the point set with any size. So the VC dimension of $\mathcal{C}$ is ∞.

Question 4

According to the theorem, the hypothesis class is learnable if and only if its VC dimension is finite[1], **C** is not learnable.

References

[1] Anselm Blumer, Andrzej Ehrenfeucht, David Haussler, and Manfred K Warmuth. Learnability and the vapnik-chervonenkis dimension. *Journal of the ACM (JACM)*, 36(4):929–965, 1989.