DS801 Advanced Optimization for Data Science Assignment 4

Spring 2024

Out: 29th May 2024

Due: 9th June 2024 at 11:59pm

Instructions

- Submit a PDF document with your solutions through the assignment portal on KLMS by the due date. Please ensure that your name and student ID are on the front page.
- **Late assignments will not be accepted** except in extenuating circumstances. Special consideration should be applied for in this case.
- It is **required** that you **typeset your solutions in LaTeX**. Handwritten solutions will not be accepted.
- Spend some time ensuring your arguments are **coherent** and your solutions **clearly** communicate your ideas.

Question:	1	2	3	4	Total
Points:	25	25	25	25	100

1. (25 points) Consider a linear model
$$h_\theta(x) = \theta^\top x$$
where θ is the model parameter and x denotes the input data. The goal is to create an adversarial example by perturbing the input data. Perturbation is made by selecting a vector from $\{\delta : \|\delta\|_\infty \leq \epsilon\}$. Then characterize the perturbation vector δ^* that gives rise to an adversarial example and its associated loss $h_\theta(x + \delta^*)$.

2. (25 points) We consider the following loss function.
$$\max_{\delta:\|\delta\|_\infty \leq \epsilon} \ell(f_{\theta+\delta}(x), y).$$
We apply the framework of sharpness-aware minimization by taking the first-order Taylor approximation of the loss function. Characterize the perturbation δ^* that maximizes the the first-order approximation of the loss.

3. (25 points) Recall that the minimax loss function of a generative adversarial network is given by
$$V(\theta, \omega) = \mathbb{E}_{x\sim\mu}\left[\log D_\omega(x)\right] + \mathbb{E}_{z\sim\gamma}\left[\log(1 - D_\omega(G_\theta(z)))\right].$$
Explain that $\nabla_\theta V(\theta, \omega) \to 0$ as $D_\omega(G_\theta(z)) \to 0$.

4. (25 points) Let $f_1, \ldots, f_T$ be an arbitrary sequence of convex loss functions that are L-Lipschitz in a norm $\|\cdot\|$. Assume that the Bregman divergence D_ψ satisfies
$$D_\psi(x, y) \geq \frac{1}{2}\|x - y\|^2$$
for any $x, y \in C$ where C is the domain. Moreover, $R^2 = \sup_{x,y\in C} D_\psi(x, y)$. Prove that online mirror descent with step sizes $\eta_t = R/(L\sqrt{t})$ guarantees that
$$\sum_{t=1}^{T} f_t(x_t) - \min_{x\in C}\sum_{t=1}^{T} f_t(x) = O\left(LR\sqrt{T}\right).$$