Introduction to Deep Learning M2177.0043 May 31, 2020
Due on June 9, 2020
Seoul National University

Homework 7

INSTRUCTIONS

- The homework is due at 9:00am on June 9, 2020. Anything that is received after that time will be considered to be late and we do not receive late homeworks. We do however ignore your lowest homework grade.
- Homeworks need to be submitted electronically on ETL. Only PDF generated from LaTex is accepted.
- Make sure you prepare the answers to each question separately. This helps us dispatch the problems to different graders.
- Collaboration on solving the homework is allowed. Discussions are encouraged but you should think about the problems on your own.
- If you do collaborate with someone or use a book or website, you are expected to write up your solution independently. That is, close the book and all of your notes before starting to write up your solution.

1 Setup [0 points]

1. In this homework, we will build and experiment with generative adversarial networks, whitebox attacks, and blackbox attacks. You must use Google Colab, which provides free GPUs.
2. Upload hw7 files to your Google Drive.
3. Ensure you are periodically saving your notebook (File → Save)so that you don't lose your progress if you step away from the assignment and the Colab VM disconnects.
4. Once you have completed all Colab notebooks except collect_submission.ipynb, open collect_submission.ipynb in Colab and execute the notebook cells. This notebook/script will:
   - Generate a zip file of your code (.py and .ipynb) called hw7.zip.
   - Convert all notebooks into a single PDF file.
5. Submit the resulting PDF and the zip file to ETL.

2 Getting familiar with KL Divergence [10 points]

Derive the closed form expression for the KL divergence between two multivariate Gaussian distributions $D_{KL}(p \parallel q)$ where each distribution is parameterized by (μ_1, Σ_1) and (μ_2, Σ_2) respectively.

3 Forward and Reverse KL Divergence [20 points]

In generative modeling, our goal is to produce a model $q_\theta(x)$ of some "true" underlying probability distribution $p(x)$. We would like to use KL divergence as a measure of the different between the true distribution $p(x)$ and our model distribution $q_\theta(x)$. Our goal is to minimize the KL divergence using gradient descent on the parameter θ.

1. (5 points) **Forward KL:** Simplify the objective as much as possible

$$\theta^* = \operatorname*{argmin}_\theta D_{KL}(p(x) \parallel q_\theta(x))$$

2. (5 points) **Reverse KL:** Simplify the objective as much as possible

$$\theta^* = \underset{\theta}{\operatorname{argmin}}\, D_{KL}(q_\theta(x) \parallel p(x))$$

3. (10 points) First, describe the mathematical meanings of each of the terms in the simplified objective. What would happen when $p(x)$ is a unimodal Gaussian? What if $p(x)$ is a bimodal Gaussian (*i.e.* a mixture of two normal distributions)?

4 Minimizing KL divergence with TensorFlow [50 points]

Follow and complete `forward-backward-kl.ipynb`. Note, you need to first solve the previous question for this exercise. Otherwise, you won't be able to implement the algorithm.

5 Mutual information and independence [10 points]

In this problem, we will prove $X \perp\!\!\!\perp Y \iff I(X;Y) = 0$

1. (10 points) Prove $X \perp\!\!\!\perp Y \implies I(X;Y) = 0$
2. (10 points) Prove $I(X;Y) = 0 \implies X \perp\!\!\!\perp Y$

6 Entropy of a multivariate normal distribution [10 points]

Let $X \sim \mathcal{N}(\mu, \Sigma)$. Compute the differential entropy of X.