Assignment 6

CS5370: Deep Learning for Vision/AI5100: Deep Learning/AI2100: Deep Learning
IIT-Hyderabad
Jan-Apr 2021

Max Marks: 40
Due: 26th April 2021 11:59 pm

Instructions

- Please use Google Classroom to upload your submission by the deadline mentioned above. Your submission should comprise of a single ZIP file, named `<Your_Roll_No>_Assign6`, with all your solutions, including code.
- For late submissions, 10% is deducted for each day (including weekend) late after an assignment is due. Note that each student begins the course with 10 grace days for late submission of assignments, of which upto 4 grace days can be used for a single assignment. Late submissions will automatically use your grace days balance, if you have any left. You can see your balance on the Marks and Grace Days document, soon to be shared under the course Google drive.
- You have to use PYTHON for the programming questions.
- Please read the department plagiarism policy. Do not engage in any form of cheating - strict penalties will be imposed for both givers and takers. Please talk to instructor or TA if you have concerns.

1 Theory (15 marks)

You can submit your response as a PDF document, which can be typed out in LaTeX/Word, or handwritten and scanned. If handwritten, please ensure legibility of answers.

1. (*2 marks*) Below is the modified objective function for a Generative Adversarial Network (GAN) where a and b are the class labels for the generated images and real images. Given a fixed generator G, derive the optimum discriminator $D^*(x)$:

$$\min_D [\tfrac{1}{2}\,\mathbb{E}_{x\sim p_{data}(x)}[(D(x)-b)^2] + \tfrac{1}{2}\,\mathbb{E}_{z\sim p_z(z)}[(D(G(z))-a)^2]]$$

2. (*2 marks*) Why does Inception Score (IS) fail in evaluating a GAN? What can be done to overcome that failure?
3. (*2 marks*) Say your class has a facial recognition-based attendance system whose trained model is inaccessible. What subcategory of attacks would you use to make everyone's face to be classified as yours? Substantiate your answer with valid reason(s).
4. (*2 marks*) In CIFAR10, you are given a sample from the automobile class and are asked to make an existing trained model misclassify it as both bird and horse. Write down the appropriate PGD attack equation for it.

5. (*2 marks*) Contrastive loss in Self-Supervised Learning helps in classifying similar samples together and away from dissimilar samples. How should it be modified in order to give us the control of the minimum distance between similar and dissimilar samples?

6. (*2 marks*) Consider the commonly used form of loss function for contrastive learning as below:

$$\mathcal{L} = -\mathbb{E}\left[\log \frac{\exp(score(f(x), f(x^+))/\tau)}{\exp(score(f(x), f(x^+))/\tau) + \sum_{j=1}^{N-1} \exp(score(f(x), f(x_j^-))/\tau)}\right]$$

   where τ is the temperature hyperparameter. How does the temperature parameter in contrastive learning affect the probability distribution? Substantiate your answer.

7. (*1+1=2 marks*) Consider the image colorization problem:

   (a) Why is framing it as a classification problem is preferred over framing it as a regression problem?

   (b) Why LAB color space is preferred over RGB?

8. (*1 mark*) If a newly proposed method claims to be 50-way-6-shot learning strategy, what is the class count in novel classes and base classes? How many samples are there in each?

2 Programming (25 marks)

- The programming questions are shared in "Assignment_6.zip". Please follow the instructions in the notebook. Turn-in the notebook via Google Classroom once you finish your work.
- Marks breakdown is as follows:
  - Question 1: 14 marks
  - Question 2: 11 marks