IST 597: Foundations of Deep Learning

Assignment 11

Instructor : Dr. C. Lee. Giles
TA : Neisarg Dave
Due Date : Tuesday, September 26, 2023

Course Policy

- Carefully read all the instructions before you start working on the assignment
- Give maximum explanation for each sub-problem. Please avoid single-line answers; submissions without any explanations will receive 0 points.
- Assignments are due before class at 02:29 pm. Please check the due date on Canvas.
- Late exercises will receive 50% credits for the first 24 hours and no credits thereafter.
- All exercise solutions must be turned in, even if late. Failure to do so can result in a deferred grade.
- All source materials must be cited. The University Academic Code of Conduct will be strictly enforced.
- All queries related to Assignment should have a subject line *IST597 : Assignment_11 Queries*

Assignment Instructions:

- The submission for this assignment must be a zipped folder: *{name}_assignment_11.zip*
- The folder must contain two files:
  1. *{name}_assignment_11.pdf*: All results and explanations
  2. *{name}_assignment_11.py*: Python codes

  A template Python file is provided. Feel free to make any suitable changes.

Convolution Neural Network

What is Convolution ?

3Blue1Brown explains it best:

`https://www.youtube.com/watch?v=KuXjwB4LzSA`

In practice, especially for images, instead of performing convolution, we perform cross-correlation operation (and call it Convolution !!)

What is the difference?

Cross-correlation is performing convolution but without inverting the kernel function.

`https://en.wikipedia.org/wiki/Cross-correlation`

Learnable Convolution Kernels
Convolution Neural Networks are composed of multiple layers of cross-correlation operators with learnable kernels.

Max Pooling
Max pooling is a pooling technique where we select the max value from the image masked by the max pooling kernel. We then slide this kernel across our image, resulting in a smaller image.

`https://www.youtube.com/watch?v=ZjM_XQa5s6s`

Conv Layers in PyToch
We will use 2D convolution layers and max pool layers from PyTorch to create our model

- https://pytorch.org/docs/stable/generated/torch.nn.Conv2d.html
- https://pytorch.org/docs/stable/generated/torch.nn.MaxPool2d.html

Task 1

3 marks

Train a decently fit (no underfitting or overfitting) neural network on the CIFAR 10 dataset.

- Keep track of your validation loss to select the best model
- You are free to change network hyperparameters and batch size
- You are free to change optimizer settings and loss function
- Run your model 5 times with different seeds and report the mean and standard deviation of the following metrics on the Test Set:
  1. Accuracy for each class
  2. Precision for each class
  3. Recall for each class
  4. F1 score for each class
  5. Visualize the Confusion Matrix (use only mean values for this)

Task 2

4 marks

Perform the following data augmentation techniques to increase the number of samples in your train set:

1. Rotate Image at an arbitrary angle
2. Crop the Image from the center and resize
3. Flip Image from left to right (Create a mirror image)

Train your network on the augmented dataset 5 times with different seeds and compare results with the network trained in Task 1.

Task 3

5 marks

1. Create an Adversarial Test Set by adding a noise sampled from $\sim \mathcal{N}(\mu = 0, \sigma = 0.1)$ to the given Test Set.
2. Compare models obtained in Task 1 and Task 2 on Adversarial Test Set
3. Augment train set by adding noise to samples from the train set. (You should have both normal samples and noise-added samples in the train set.)
4. Train your model 5 times with different seeds on noise augmented train set and report results on normal Test Set and Adversarial Test Set