Programming Assignment 4:
Convolutional Neural Networks

CS 4670 Spring 2023

Assigned:	Thursday, April 27
Due:	Tuesday, May 9th
Files to Submit:	`student.py`, `Writeup.pdf`, `model_weights.pth`, Leaderboard submission

This project can be done **individually or in pairs**. You may use up to **10** slip days.

Overview

In this assignment, you will explore convolutional neural networks (CNNs) in the context of image classification. The following are your tasks:

1. Build and train a baseline model
2. Implement data augmentation techniques
3. Build your own model to improve upon the baseline
4. Generate adversarial examples to explore potential shortcomings of CNNs

Initial setup

Download the files for this project from CMS and put them in a single folder. There should be the following project files on CMS:

- `PA4.ipynb`: Jupyter notebook with instructions and visualizations
- `student.py`: Python file for student code
- `data.zip`: Folder of image data
- `models.zip`: Folder holding weights for pretrained baseline model
- `data_augmentation_sample.png` Example output plot for data augmentation portion
- `Leaderboard_Submission.ipynb`: Jupyter notebook with instructions for creating the csv output to submit for Leaderboard on Gradescope.
- `Install skimage`: You may need to install skimage using the following: `conda install scikit-image`

Download PyTorch (Below commands assume you are in Python 3.6)

Mac: `conda install pytorch torchvision -c pytorch`

Windows users: `conda install pytorch-cpu torchvision-cpu -c pytorch`

Additionallly, if you do not have conda, you may checkout https://pytorch.org/ for download instructions. If you have any questions about the initial setup, please check Edstem to see if someone else has run into the same issue. If not, feel free to post a new question!

Opening the assignment

Here is the workflow you should use any time you are working on this project:

1. In a terminal window, activate the `cs4670` environment.
2. Run `jupyter notebook` in the directory containing the project files. This should open up a GUI in your browser.
3. Click on `PA4.ipynb`, which will open up the Jupyter Notebook that we will be using for this project. This file contains detailed explanations about the project and the various TODOs. If you haven't used a Jupyter Notebook before, or if you'd like a refresher, check out this quick video tutorial!
4. All the code that you will write should go into `student.py` – this is the file that will be submitted and graded (in addition to the writeup)! The cells in the notebook simply import your code and run it, and you should not need to change any of the code in the notebook itself (although you are free to do so if you would like to modify the visualizations). Moreover, every cell that imports your code will automatically re-import your latest `student.py` code, so you can just save changes to `student.py` and re-run any cell.
5. Note that the notebook will lose its variables when it's restarted. Whenever you start the Jupyter Notebook server afresh, we recommend re-running all the cells up till the one you are currently working on. This will ensure that all the variables up till that point are re-loaded into the notebook.

Testing and Debugging

In the notebook

We have added cells within `PA4.ipynb` that help you visualize your results so far – these should give you a good idea of whether you're on the right track or not! You can also print variables in the notebook cells in case you'd like to look at them for debugging purposes.

Deliverables

You should submit the following files:

1. `student.py`: contails all of your work filled in for each of the TODOs. This must be submitted on CMSX.
2. `Writeup.pdf`: contains answers to several questions found in the Jupyter notebook. This must be submitted on GradeScope and you must tag the questions with the assigned question label (i.e. Part 2a is labelled as 2a in the writeup)
3. `model_weights.pth`: contains weights to your network submitted to the GradeScope Leaderboard competition. This must be < 5 MB and submitted on CMSX.
   * If you choose not to do the optional competition part, then you do not need to submit this file.

Leaderboard competition (Optional)

There will be a Leaderboard competition on Gradescope for this project. You will train your own models and make predictions on unseen test data (which you will not have labels for). You will get to see your model accuracy on the leaderboard. There will be an instructor model submission, which you will attempt to beat.

A note about grading

You may have noticed that there are no automated tests for this project. That's because it's inherently hard to have test cases with exact numerical comparisons for neural networks. Instead, your grade is based on the following:

- Quality of your images for data augmentation in the writeup
- Quality of adversarial images: must get at least 85 % misclassification rate for full points
- Quality of answers and explanations in writeup
- The optional part will not be graded.

If you have any questions, please ask on Edstem or in office hours. We are here to help!

Optional Resources

The following are optional resources you may use if you would like a refresher on PyTorch or using GPU-accelerated training for your models. These are completely optional and will not be necessary for the assignment.

PyTorch

The examples on this site can give you a quick tutorial on how tensors work with PyTorch and how to use PyTorch in general. There are examples of how to build general models on the website, but note that the content will be different from the model we are asking you to build. The concepts that you will need to know to create the model for the assignment can be found in lecture slides.

CUDA Acceleration

If you have a CUDA-enabled NVIDIA GPU (you can test this by running *torch.cuda.is_available()* in the notebook and have CUDA installed, you can potentially speed up the training of your model. In order to use CUDA acceleration, you need to modify PA4.ipynb. The following list outlines some of the things you may need to change to get CUDA acceleration working.

- Set torch.backends.cudnn.benchmark to True
- set the dataloader pin_memory parameter to True.
- Move the network to the GPU after it is initialized. For example, you can call net.to('cuda').
- Move your loss function to the GPU.
- Move the inputs and labels to the GPU (remember to do this for both the training and validation stage)
- The labels may need to be moved back to the CPU in the validation phase when converting back to NumPy.

Assuming no other issues arise, you should be able to see a speedup in training time. Using a desktop with an I7-6700K and GTX 980TI, we had a training time for the baseline model of $\sim$ 480s using the CPU and $\sim$ 280s using the GPU through cuda acceleration. Depending on your gpu or configuration, you may not experience as dramatic of a speedup or may even slow down due to inefficient memory accesses.

Google Colab

If you don't have a GPU but would still like to use CUDA acceleration to speed up training, you can use Google Colab. Google Colab is rather similar to Jupyter Notebook in format and will allow you to speed up model training since Google has dedicated GPUs that you can use. The free version allows you to use a NVIDIA Tesla K80 GPU for 12 hours at a time.

To get started, head over to colab.research.google.com and upload the PA4.ipynb notebook. From here, you need to upload student.py, data.zip, and models.zip. There are several places where you can load the data.

1. **Google Colab local storage**. Since our dataset is relatively small, you can unzip the model and data folders directly into the Google Colab local storage. The benefit is that you will not deal with delays with memory accesses as you would with google drive. The downside is that it takes a bit to upload the data and everytime you restart your runtime or close your runtime, the files are lost and you will need to re-upload the models, data, and student.py to the local storage.

2. **Google Drive Mounting**. You can mount your google drive to Google Colab and store your models and data on google drive. The benefit is that you won't need to constantly re-upload the models and data. However, you will have quite a large amount of delay between retrieving files from drive to use when training. This will probably increase training time.

3. **Google Cloud Storage** You can also store your data and models in Google Cloud Storage. The access time for GCS is faster than google drive. This is a paid service but you get $300 free credit to use.

Once you've decided how to store the data, if you want to use GPU acceleration, switch to the GPU by going to Edit→ Notebook Settings and select **GPU** from the menu. Finally, follow the steps in the **CUDA Acceleration** to modify the notebook to make use of the GPU.

It took $\sim$ 290s to train the baseline model without hardware acceleration on Google Colab and with CUDA acceleration, it took $\sim$ 180s.