Convolutional Networks

TensorFlow

Problem Specification

The objective of this assessment is to build a range of deep learning models using convolutional neural networks.

The data we will be using is the Flowers 17 dataset. You can find the original dataset here. This is a multi-class classification problem with 17 possible classes (17 different classes of flowers). The images have significant variation in pose and lighting and there is also significant variation within certain classes and close similarity between other distinct classes. What makes this dataset even more challenging is that there are only 80 images for each class. Therefore, there are just 1360 images.

Below you can see a selection of images from the dataset.

You will find the data file (**data1.h5.zip**) in the assignment unit on Canvas. The zip file stores the data in a HDF5 file called data1.h5. Instructions for extracting the contents using Google Colab are contained in Appendix A at the end of the assignment specification.

For the purposes of this assignment I have divided the original dataset so that 75% will be used for training and 25% will be used as validation data. As there is such a limited amount of data we will just use training and validation datasets.

Please note that I have performed pre-processing on the dataset, namely all images are now of an equal size (128*128*3) and the data has also been normalized.

The shape of the feature training data is (1020, 128, 128, 3), while the shape of the validation data is (340, 128, 128, 3). Therefore, the data is divided into 1020 training images and 340 validation images.

The assignment consists of the following three sections:

- **Part A**: Explores the application of convolutional networks, data augmentation and ensemble technique.

  [35 Marks]

- **Part B**: Focuses on transfer learning (specifically the using CNNs as feature extractors and fine tuning CNNs).

  [40 Marks]

- **Part C**: Research component explores adversarial machine learning or capsule networks.

  [25 Marks]

Please upload your final submission (as a single zip file) to Canvas before **22:00 on Sunday May 19th**. Please note that normal late penalties will apply if any assignment is submitted after this time.

Your submitted zip file should contain your python files (one notebook or python file for each part) and a report. Please note that all code should be fully commented. **Please do not include the flower dataset in your uploaded zip file**.

Given the reliability issues that have been reported when using DataLab I would recommend that you complete this assignment using Google Colab. I have tested the final code for each of the following sections using Google Colab with a GPU and its performance has been adequate.

PART A: Convolutional Neural Networks: **[35 Marks]**

Part A requires you to build a range of convolutional networks for tackling the Flowers dataset problem. It also requires you to explore the impact of data augmentation and investigate an ensemble technique.

Please use the following optimizer for all models in Part A: tf.keras.optimizers.SGD(lr=0.01). You are free to use whatever learning rate you wish. I have used 0.01 in my code.

For each model you build you should plot the training and validation accuracy as well and the training and validation loss. You should also offer your interpretation of each of plots produced.

(i) Implement a baseline CNN, which contains just a single convolutional layer and a single pooling layer.

Increase the number of layers in your CNN (convolutional and pooling layers) and report the impact on the validation and training accuracy/loss values. You should implement at least three different CNN configurations (inclusive of the baseline case). Compare and contrast the performance of your models. (10 marks)

(ii) What, if any, is the impact, of applying data augmentation on the models that you built in part 1. How do you explain the impact of data augmentation? Does the selection of methods used as part of your data augmentation (such as cropping, flipping etc) have an influence on accuracy?

(10 marks)

(iii) Build a basic CNN ensemble containing a maximum of 10 base learners. Your objective is to take a network with a fixed structure and train it multiple times. Compare the validation accuracy achieved by the ensemble with each of the base learners. As this is a very basic ensemble you may not see a significant improvement in overall performance. One of the reasons for this may be the lack of diversity in the base models. Why might lack of diversity be a problem of ensemble techniques? Can you describe possible steps you could take to introduce additional diversity into the base models?

(15 marks)

PART B: Transfer Learning **[40 Marks]**

Part B focuses on transfer learning. You will be required to investigate and explore the impact of feature extraction and fine-tuning techniques.

(i) Use a pre-trained CNN model (such as VGG or Inception models) as a feature extractor and pair its output with a secondary (standard) machine learning algorithm. For example, you could use a pretrained VGG16 network as a feature extractor and feed the extracted feature data into a logistic regression model. What is the impact on the validation and training accuracy values?

To grade well in this question, you should explore and examine appropriate variants of the above structure. For example, one appropriate variant would be to examine a selection of different secondary machine learning algorithms in order to improve the overall level of validation accuracy (for example would a Random Forest provide any performance advantage over a logistic regression unit). You should include a description of the different variants you examined, a rationale for examining each variant and it's impact on accuracy values. (20 marks)

(ii) Explore the application of fine tuning as a method of transfer learning for the Flowers dataset.

Again, to grade well in this question you should include appropriate exploratory work. Your objective is to identify the best validation accuracy that you can achieve for the Flower dataset. Therefore, you should consider the variables involved when performing fine tuning as well as additional techniques you could use to improve performance. (20 marks)

PART C: Research **[25 Marks]**

Deep convolutional networks have achieved exceptional levels of accuracy when applied to image related machine learning problems.

However, convolutional networks do have some significant limitations and vulnerabilities, some of which may undermine their long-term success and viability. Geoffrey Hinton, one of the leading figures in deep learning research, has argued that despite the success of CNNs they have some have significant disadvantages that may be difficult to solve.

The objective of this section is to write a short research report. Please select one of the following topics for your research report.

- Adversarial Machine Learning: The goal of adversarial techniques is to fool a machine learning model through the provision of malicious input. (Please note this is not the same thing as generative adversarial models).

- Capsule Networks. A relatively recent technique that attempts to model hierarchical relationships in a CNN and overcome one of the core limitations of CNNs.

Your research report should not exceed 3 pages (guideline for max word count 1500 words). Please include any references. To grade well for this question you should demonstrate that you have researched the topic from a range of sources, your explanation should convey a clear understanding of your selected topic, expressed in your own words, along with a good grasp of the underpinning technical knowledge.

Appendix A: Accessing Training and Validation for the Flower Dataset (Using Google Colab).

The following instructions describe an efficient way of accessing the flower data using Colab.

1. The flowers dataset is stored in a zip file called data1.h5.zip, which you can find on Canvas in the assignment unit.

2. Copy the compressed data file (data1.h5.zip) to a folder in your Google Drive (wait for the upload to complete). For the purposes of this example I have placed the zip in a Google Drive folder called Flowers.

3. Once the compressed data file has been transferred to the Flowers folder in your Google Drive open a new Google Colab notebook. All of the code for the steps below is contained in this Colab Notebook. Once open execute the following steps:

    a. Step 1 requires you to mount your Google Drive. In your Colab notebook execute the following code. This will ask you to enter follow a link and enter an authorisation code. Once complete you should see the message "Mounted at /content/gdrive"

```
from google.colab import drive

drive.mount('/content/gdrive')
```

    b. Next extract the contents from the file data1.h5.zip by entering the following in a Colab notebook. Remember my zip file in stored in the folder Flowers.

```
!unzip "/content/gdrive/My Drive/Flowers/data1.h5.zip"
```

    c. This should extract the file **data1.h5** into your current working directory. To confirm run the following in a Colab cell and you should see the file data1.h5.

```
!ls
```

4. You can now use the code below to open the HDf5 file and extract the contents and store in a NumPy array. Upon executing this code you should see the size of each NumPy array printed as follows:

   (1020, 128, 128, 3) (1020,)
   (340, 128, 128, 3) (340,)

```
import numpy as np

import h5py


def loadDataH5():

    with h5py.File('data1.h5','r') as hf:

        trainX = np.array(hf.get('trainX'))

        trainY = np.array(hf.get('trainY'))

        valX = np.array(hf.get('valX'))

        valY = np.array(hf.get('valY'))

        print (trainX.shape,trainY.shape)

        print (valX.shape,valY.shape)

    return trainX, trainY, valX, valY


trainX, trainY, testX, testY = loadDataH5()
```