Convolutional Neural Network

Rihad Variawa
Samira Variawa

September 18, 2020

Contents

Chapter 1

Summary

WHAT IS CNN?

CNNs (Convolutional Neural Networks) are state-of-the-art Neural Network architectures which are primarily used for computer vision tasks. CNNs can be applied to a number of different applications, such as:

- object classification (also known as image recognition)

- object localization

- image segmentation

- change detection, as well as similar tasks applied in video

This document serves to outline how to implement a **Residual CNN** (often abbreviated Res-CNN, or simply ResNet), as well as how to migrate the network to the cloud (specifically via Databricks)

The files to our ResNet project can be found here:

cars

Note that much of this code came from a previous respository, found here:

previous repo

For technical documentation on the ResCNN architecture, see:

for technical documentation on the ResCNN architecture

Chapter 2

CNN Implementation

2.1   Preliminaries

When we break apart a CNN, they comprise of different 'blocks', with each block simply representing a group of operations to be applied to some input data. These blocks can be broadly categorized into:

- **Identity Blocks**: a series of operations which keep the shape of the data the same

- **Convolution Blocks**: a series of operations which reduce the shape of the input data to a smaller shape

*CNNs are a series of both **Identity & Convolution Blocks** (or Conv Blocks) which reduce an input image to a compact group of numbers. Each of these resulting numbers, if trained correctly, should eventually tell us something useful towards classifying the image*

*ResCNN adds an addition step for each block. The data is saved as a temporary variable before the operations that constitute the block is applied, and then this temporary data is added to the output data. **Generally, this additional step is applied to each block***

To visualize this, imagine a series of n blocks as being represented by functions $f1...fn$, and imagine we begin with some input data X. Then a normal CNN is simply repeated application of $f3(f2(f1(X)))$ and so on (until fn, the final block, is applied). We will finally arrive at some Yn, which is the final output of simplified data

ResCNN, however, would begin with: $f1(X) + X = Y1$ (where $Y1$ is the output of the first block)

We then continue this:

$f2(Y1) + Y1 = Y2$
$f3(Y2) + Y2 = Y3$
...
$fn(Yn1) + Yn1 = Yn$

The reasons for which these residual blocks are more effective is debated, however, whatever the reason, these networks seem to excel at **computer vision** tasks. Also, each function f, representing a block, that being a series of operations, is not necessary an individual convolution block or identity block. They could also be combinations of both. An example image of a ResNet is shown below:

Figure 2.1: An example of a Residual CNN. The arrows jumping over various blocks represent the 'skip' connections characteristic of a ResCNN

2.2 Deep Learning with Keras

There are many different methods of implementing Neural Networks. One of the more intuitive ways is via Keras. **Keras provides a simple front-end library for executing the individual steps which comprise a neural network. Keras can be configured to work with a Tensorflow back-end, or a Theano back-end**
Here, we will be using a Tensorflow back-end. A Keras program is broken up into multiple parts. In general there is a 'main file' in which parameter values are set and functions are called, as well as other files which contain the architecture of the CNN, functions, data reading options, etc.

In the example ResNet provided in cars repo, the files are as follows:

- **CarModel.py** - the main file

- **res-net.py** - contains the primary structure of the ResNet, in terms of Convolution Blocks and Identity Blocks (to be read in by the CarModel.py file)

- **conv-block.py** - contains the structure of a Convolution Block (to be read in by the res-net.py file)

- **identity-block.py** - contains the structure of an Identity Block (to be read in by the res-net.py file)

- **resnets-utils.py** - contains various helper functions, such as those for reading and formatting data

LET'S WALK THROUGH THE CONTENTS OF THE **CarModel.py** FILE

Part 1: At the very beginning, we import all the necessary functions and clear the trash. Then we set the preliminaries:

- img width

- img height

- classes (the number of objects we want to be able to identify)

- epochs (how many times we want the neural network to go through the training data)

- patience (if the accuracy is not improving, how many epochs we want the neural network to try to improve before giving up)

- verbose (program will output updates as it trains if this is set to 1)

- num train samples (how much of the training data should be used towards actually training the data, as opposed to cross validation)

- num valid samples (how much of the training data should be used towards cross validation, usually around 20% of the total training data)

- mode (what optimizer should be used in trying to minimize the training error)

Part 2: At this point we need to initialize the neural network architecture to be used. This is done by:

1. Reading in the model defined in the res-net.py file

2. Writing the ResNet function (defined in the res-net.py file) to a variable called 'model'

3. Deciding on which optimizer to use (lr = learning rate, decay = how much to reduce the lr each epoch, beta/epsilon are all hyperparameters)

4. Load pre-trained weights if required

5. Finally, compile the model via the command: model.compile(optimizer=optimizer, loss='categorical crossentropy', metrics=['accuracy'])

Part 3: Now we can set-up what are called callbacks. These are handy little pre-built additions that can either help the neural network train better, or track the training process. A few common ones we use include:

- ModelCheckpoint - Probably the most important. This saves the weights at the end of each run, and then you can read them in later to train further without starting from scratch

- CSVLogger - This outputs the accuracy and cross validation (val) accuracy after each epoch. You can also plot this (see section 3.7)

- EarlyStopping - Stops the training if it seems as though accuracy has reached a maximum

- ReduceLROnPlateau - Reduces learning rate when the accuracy reaches a 'plateau'. That is to say, when it becomes a bit harder to learn, the network changes more gradually so as to more carefully find what changes improve performance

There are lots of other callbacks. You can see the full list here: Callbacks API

Part 4: Train the model. The network will now begin the process of forward propagation and back propagation. Depending on the complexity of the network, and size of the Neural Network, this can take minutes to hours (state-of-the-art networks are sometimes trained for days or weeks)

In general, if this is taking more than an hour, it should really be moved to the cloud, see section 3. As the network trains, we will see the training accuracy being printed at each step. At the end of each epoch, the network will use the cross validation data to check the validation error (val acc). This val acc provides a much better estimate of what the final test accuracy will be than the train accuracy, which should always be larger than the val acc

Also note that the weights file, which will be systematically saved if you have the 'ModelCheckpoint' callback, can be quite large, potentially up to a gigabyte

2.2.1 Overfitting

Note that if the difference between the train acc and then val acc are, more or less equivalently, the difference between the train acc and the test acc, becomes too large, this is a case of overfitting

This means that the network has learned the training data too well, and is unable to **generalize to new data**. However, as one tries to push a neural network further and further, it generally happens that at high accuracy train acc, will eventually diverge from the val acc. There is no hard-rule for when this divergence is concerning. It depends hugely on the type of network, the depth, the hyperparameters, the amount of input data, and the nature of the computer vision task

However, as a rule-of-thumb, and speaking entirely from our personal experience, *we can offer the following advice. It seems as though a good neural network should be able to keep train acc and val acc relatively paired until at least 70% accuracy, and when they do eventually diverge, this divergence should not exceed much more than 10%.* As an example, figure 2.2 shows two test/validation accuracy curves. In figure 2(a) we see that the train acc and test acc begin to diverge at extremely low accuracy (around 10 - 20%), and then the gap between the two becomes very large (around 50%). This is a case of fairly serious overfitting. Conversely, in figure 2(b) we see that the two curves stay relatively well paired until (around 60 - 70%), and then the difference between them remains under 20%. Again, the network is still overfitting, yet at such high accuracy it becomes increasingly difficult to do much better (even state-of-the-art implementations on the Standford Cars dataset begin overfitting above (88-93%), as seen in figure 2.2 below
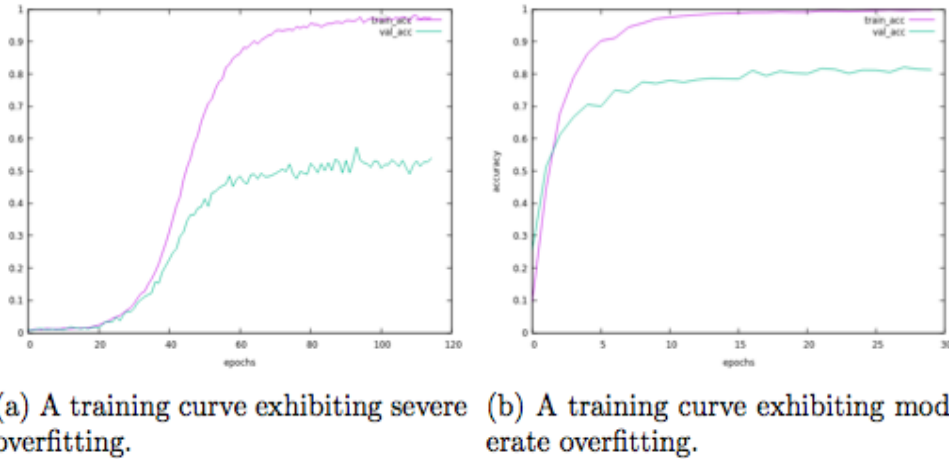

(a) A training curve exhibiting severe overfitting.

(b) A training curve exhibiting moderate overfitting.

Figure 2.2: Two example training curves

Part 5: After training, the final step is to test the accuracy on some data that the neural network has not yet seen

It is generally considered standard to use 50% of the total dataset for testing, although this number can vary depending on the quantity of data. The test accuracy (test acc) is considered the true metric for how well the neural network performs

2.3 Data Formatting

A huge part of any computer vision task is **collecting, cleaning, and labelling the data**. We could write an entire book here about the subject, and there is no clear 'best practice' for data preparation

Instead, we will tell you how the data must be formatted so that it can be read in by Keras

2.3.1 HDf5

The Machine Learning world operates on HDf5 (Hierarchical Data Format 5) files see Hierarchical Data Format. These are highly compressed files which are usually annotated by the .hdf5 or .h5 file extensions. Multiple images and labels can be written to HDf5 files, and then later extracted

2.3.2 Reading an HDf5

Once data is saved to an HDf5, it can be later read through the following commands:

$import h5py$

$train dataset = h5py.File('training data.h5', "r")$

$train set x orig = np.array(train dataset["train set x"][:])$

$train set y orig = np.array(train_d dataset["train set y"][:])$

Here, train set x original will be a tensor containing all the images (features). If each image is 224-by-224-by-3, and we have n images, the resulting tensor will have dimensions 224-by-224-by-3-by-n. Conversely, train set y original is a 1D vector containing the corresponding labels

2.3.3 Writing an HDf5

Creating an HDf5 file is somewhat more complicated. Yet in general one needs only a directory containing all the images, as well as a corresponding file containing all the labels. The images should be labelled sequentially (i.e. 00000.jpg, 00001.jpg, 00002.jpg, etc.), and the file containing the labels could be something like: [123, 17, 192, ...], where the first label (123) corresponds to the first image (00000.jpg), and so on. Note that it is also necessary to have a list somewhere which contains the correspondence between numerical labels and

actual labels. For examples, 0 = dog, 2 = cat, 3 = horse, etc. These 'actual' labels are completely unnecessary for training and testing, but the code won't serve much good if, after lots of time spend training and testing, we don't know what real-world objects have actually been identified!

Note: This is certainly not the only way to create HDf5 files, nor to format the data within them. We have, unfortunately, seen different teams using different conventions. For example, some teams prefer to first create one directory for each label, and then sort the images into the directories. When the HDf5 file is created, the label is inferred by the corresponding directory name. Other teams instead append a suffix to the file name, and infer the label from the file name upon reading. And within the HDf5 the images can also be stored as long 1D arrays. All said, be careful when dealing with somebody else's code. Run some sanity checks to make sure the train set x orig and train set y orig numpy arrays contain the data that you think they do

2.4   Keras Blocks

Just in case you're curious about how all of this works, here is a little overview of the 'under-the-hood' components of a Keras Neural Network

Inside the res-net.py file (as well as the conv-block.py and identity-block.py files) are a number of functions that correspond to various steps in a neural network. These steps combine together to make 'layers', and then a few layers will constitute a block. As an example of a single layer, we might have something like this:

$$X = Conv2D(somearguments)(X)$$

$$X = BatchNormalization(somearguments)(X)$$

$$X = Scale(somearguments)(X)$$

$$X = Activation('relu')(X)$$

This layer receives some input data X (likely an image) and consists of four steps.

1. a convolution is applied to the data to make it slightly smaller

2. batch normalization is applied (this is a step which both prevents overfitting, and also avoids a problem known as 'disappearing gradient', which is a bit more technical than we had planned on getting into)

3. the third step relates to the fact that the pixel values of images are generally stored as integers, yet we need floats to allow for sufficient accuracy when performing back-propagation

4. finally, we applies a Rectified Linear (ReLu) function (this is somewhat of a 'cut-off' to avoid negative activation values)

You may also notice that the conv blocks and identity blocks start with:

$$Xshortcut = X$$

and end with:

$$X = Add()([X, Xshortcut])$$

This is a 'skip connection', which is characteristic of Residual CNN (see figure 2.1). In the res-net.py file, there are a few other commands worth noting. For example, near the beginning you will find:

$$X = ZeroPadding2D((3,3))(Xinput)$$

This adds some extra pixels around the sides of the image (in this case 3 on each side), such that applying a convolution step (with a 7-by-7 filter) will leave the image shape unchanged. Near the end we also have:

$$Xfc = AveragePooling2D(somearguments)(X)$$

This reduces the size of the data, similar to a convolution step, however instead of a filter in which pixels are multiplied, here we average across a region. Once we are finished with the convolution layers, we 'flatten' the data into a 1D vector. Finally we can include a 'fully connected', or 'dense' layer (a 1D layer in which all the nodes are fully connected to the next layer of nodes). These steps are accomplished via:

$$Xfc = Flatten(Xfc)$$

$$Xfc = Dense(somearguments)(Xfc)$$

(and in case you're curious, 'Xfc' stands for 'X fully connected')

2.4.1 Transfer Learning

One technique often used to give a huge boost to performance is called **Transfer Learning**. For this we read-in a set of weights that have been pre-trained on other data. These weights may already entail a concept of some basic structures such as: edges, corners, text, circles, etc. This can save a significant amount of time, as a CNN will not have to 're-learn' these basic concepts which is often the most time-consuming step

In the res-net.py file we have applied transfer learning. The weights used are pre-trained on the ImageNet dataset, which contains 1000 object classes. As such, we first include a fully connected layer which maps to 1000 nodes. Then, after uploading the relevant weights, we switch this for a fully connected layer which maps to the number of nodes we need for our specific task 196 in our example, corresponding to the 196 classes of cars. The full code to accomplish this is:

$X = the output of some previous conv and identity blocks$

$Xfc = AveragePooling2D((7,7), name =' avgpool')(X)$

$Xfc = Flatten()(Xfc)$

$Xfc = Dense(1000, activation =' softmax')(Xfc)$

$model = Model(inputs = Xinput, outputs = Xfc, name =' ImageNet1000')$

$model.loadweights('models/resnet152weightstf.h5', byname = True)$

$Xfc2 = AveragePooling2D((7,7), name =' avgpool')(X)$

$Xfc2 = Flatten()(Xfc2)$

$Xfc2 = Dense(196, activation =' softmax')(Xfc2)$

$model = Model(inputs = Xinput, outputs = Xfc2, name =' ResNet150')$

To walk through this explicitly, we first take some output (X) from a number of conv and identity blocks. Then we map this to a layer consisting of a 1D layer of 1000 nodes (consistent with the number of object classes in the ImageNet dataset). We then define this neural network architecture as 'model', and load in weights (named here resnet152 weights tf.h5) for this entire neural network (via the model.load weights command). Lastly, we switch the last few layers (that conclude in a choice of 1000 classes) to the number of classes we need for our purposes (196 here, for the 196 different car models). Note how, in the fourth-to-last line we, input 'X' as opposed to Xfc (hence 'switching' the output layers for the new ones, denoted as Xfc)

As a final step, this new model is saved to the 'model' variable (overwriting the previous one), however the values of the weights remain the trained values. Now this model can be called by the main program, for training and testing

Chapter 3

Executing Neural Network On Databricks

3.1   Logging into Databricks

You will need to first login. Assuming your account has already been made, there should be a URL to follow, which looks something like this: Login - Databricks

3.2   Setting up a Cluster

You can view the clusters by clicking 'clusters' on the left sidebar. You will probably not have permission to access other people's clusters, however you should be able to create your own

Name and set-up your cluster. Be sure to choose one with the Runtime Versions that include 'ML' in the name (5.5 ML for example). Enable Autoscaling. The fastest configuration we were able to find was:

Runtime Version Worker Type Driver Type

5.5 ML GPU

p2.xlarge (Min 2, Max 8) p3.16xlarge

This resulted in a speed of about 150s/epoch using a 150 layer ResNet on the Standford Cars dataset with the sgd optimizer. However, keep in mind this is one of the more expensive clusters in terms of DBU (see section 3.6)

3.2.1 Libraries

The Runtime Versions with ML in their names should come with all relevant Machine Learning packages pre-installed (Keras, Tensorflow, openCV, etc.). If, for whatever reason, you need to use another Runtime Version (e.g. sometimes Databricks puts limits on how many clusters you can have running of the same instance type), then you can still install these libraries manually. To do this:

1. click on the 'Databricks' button on the top of the left sidebar

2. under 'Common Tasks', click 'Import Library'

3. for 'Library Source' choose 'PyPl'

4. ignore the Repository option, and simply type in the package name and click 'Create'

5. you can choose to install libraries for all clusters, or only for select clusters

In this instance, for the computer vision code included here, you should be fine with the following three libraries:

1. keras

2. tensorflow

3. opencv-python

3.3 Moving Code to the Cloud

Your code must be adapted to Notebooks, which can then be run on databricks. Here you will find an example notebook, specifically dealing with an ML implementation using Keras: example notebook

If you want to try this notebook yourself, or if you just want to use this Notebook as a blueprint for your own code, scroll down to the 'Example Notebook' section. On the right (in fairly small text) you will see 'Get notebook link'. You can click this and copy the Notebook link. Then switch back to Databricks, choose 'Workspace' on the left sidebar, choose your username, then click the little down-arrow next to your username, and choose 'import'. Here you can paste the Notebook link, or you can upload your own files from your local machine. To edit a cell within a Notebook, simply double-click it

Before we upload the data (h5 files) we can first start re-touching the uploaded files (assuming you uploaded your own), to make sure they work on Databricks. In general, this shouldn't be too much work, but here are a few considerations:

1. a few packages, such as those that deal with plotting, may not work in Databricks. Simply comment anything unnecessary

2. to get a python script to read in another python script, you can generally use:

   from resnets utils import *
   However, this won't work on Databricks. In an otherwise empty cell, you can use:

   Note: It's really important that this is the only command in the cell. Even adding comments will not work. So if you are reading in multiple other notebooks, you need one cell for each. We know it's annoying, but we haven't found another way to get it to work. Also, obviously all notebooks need to be in the same directory as the main notebook

3. for reading in data, you need to add the /dbfs/ prefix in front of the path name. As an example, when running our CNN on our machines, we used:

   train dataset = h5py.File('datasets/train cars.h5', "r")
   However, on Databricks this becomes:
   train dataset = h5py.File('/dbfs/train cars.h5', "r")

   The same is true for any callbacks (for example the path to the weights file or log file). You can also specify sub-directories within the /dbfs/ directory

   Note: If, on Databricks, you want to specifically play with the car identification example we have been working with, you can do so by importing the Cars.ipynb file, found here:
   example repo, to Databricks

3.4   Uploading Data

The UI that comes with Databricks doesn't seem to have an easy way to load in certain non-table files, specifically h5 files. However, you can do it via the Command Line Interface (CLI). Here are the steps:

1. First, in your terminal, install the Databricks CLI with:
   sudo pip install databricks-cli

2. Next, type:
   databricks configure –token

3. For the Databricks Host, enter the URL for your account for example, Login - Databricks

14

4. In the very top right of the Databricks window you will see a small person icon, which you can click to access the 'User Settings'

5. Switch to the 'Access Tokens' tab at the top, and then click 'Generate New Token'

6. Copy this in your terminal when you are prompted for the Token

7. Now you will have access to Databricks directly through the CLI. You can see a list of functionalities with:
   databricks -h
   You can also see more specific commands by including the topic you want to know about, such as:
   databricks clusters -h

8. The command to upload a file is:
   dbfs cp file.h5 dbfs:/file.h5
   You can check what's on the dbfs with:
   dbfs ls
   Uploads can take some time, but when you finish uploading all the necessary files, you're good to get started!

3.5 Running Everything

To run your application, go to the clusters menu and start the one you wish to test on. Then go to the main Notebook, and on the top you will have an option to 'attach' the Notebook to one of the clusters. Note: you don't need to attach other Notebooks that are read/run by the main Notebook, only the main one

It will take some time for your cluster to start running (it can be a bit long for larger ones). Once it is running, you can click 'Run All' at the top of your main Notebook (or run cells one-by-one for testing purposes with shift+enter)

Note: Callbacks in Keras
If your code makes use of callbacks, note they sometimes work a little differently in Keras. For example, the csv logger callback is only printed to the /dbfs/ directory at the very end, not at each epoch (don't worry though, the log file will still contain the accuracy and val accuracy for every epoch). One other important point is that **the weights file can take a long time to save to the /dbfs/ directory**, especially for deeper networks (30+ minutes is not unusual). *Unfortunately, as far as we know, there isn't a way to terminate the cluster while this file saves*

3.6 Costs & Optimization

Databricks measures costs in 'DBU'. When you are configuring a cluster, the cost for given cluster types and sizes are listed (these are the costs in DBU per hour the cluster is active)

Note: When you use multiple worker nodes, the DBU cost is multiplied by the number of nodes, so be careful with this. You will probably want to fiddle around a bit with different settings in terms of both your hyperparameters, as well as with the cluster type

3.7   After Finishing

Once the training is finished, the weights are saved to the /dbfs/ directory, and the test accuracy has been calculated, you can download the weights to your local directory from the cloud using the following command:
dbfs cp dbfs:/weights.best.hdf5 ./weights.best.hdf5

These can then be used to make predictions for new data. You can also execute a similar command to download your log file:

dbfs cp dbfs:/training.log ./training.log

If you wish, you can plot the training and validation curves using gnuplot. Here are the commands (which must obviously be executed in gnuplot, in the same directory as the log file):

gnuplot¿ set datafile separator ","

gnuplot¿ set xlabel 'epochs'

gnuplot¿ set ylabel 'accuracy'

gnuplot¿ plot "training.log" u 1:2 with lines title 'train_acc',

"training.log" u 1:4 with lines title 'val_acc'

Chapter 4

Deploying

Once the weights have been trained, and the test accuracy is satisfactory, it's time to deploy the network on the cloud. **What we ultimately want is a program in which an image can be provided, and the output is the name of the object in the image**. This could be done in two ways: either the image could be directly uploaded, or the image can be linked to via a url

If you look at the 'guess.py' file found here: cars. Then you will find an implementation which takes a url argument and outputs the name of the predicted car model

4.1 Deploying on Databricks

In the same github repository, you'll also find the guess.ipynb file. This is a notebook implementation of the same code. Here you will find a quick overview of the content of the program

Part 0: Firstly, as we did with the main code, we begin by initializing packages, clearing memory, and setting Keras variables. Other notebooks (resnets utils, scale layer, res net) are also read in

Part 1: Next, we read in the model we previously defined in the resnet file, as well as the weights we have now trained up to high accuracy (which should be stored in the dbfs directory). We also read in a file named cars meta.mat (which comes pre-packaged with the Stanford Cars dataset). This file contains the correspondence between the label numbers and the label names (e.g. 0 = 2012 Tesla Model S, 1 = 2012 BMW M3 coupe, etc.). The code to accomplish this looks as follows:

img-width, img-height = 224, 224

model = load-model-weights()

model.load-weights('/dbfs/2series/weights.best.hdf5')

cars-meta = scipy.io.loadmat('/dbfs/2series/cars-meta')

class-names = cars-meta['class-names'] shape=(1, 196)

class-names = np.transpose(class-names)

Note that the 'load model weights' function is defined in the resnets-utils file

Part 2: Now, we can define a 'guess' function, which reads in a URL to an image, and then outputs a prediction for the car model. At the core of this function are these 3 lines:

preds = model.predict(rgb-img)

prob = np.max(preds)

class-id = np.argmax(preds)

What we are doing here is inserting an RGB image into our model, and returning a 1D array (with 196 elements). The index which contains the highest value (defined as class id here) is the 'best guess' for the object's class, and the value itself is a measure of how 'confident' the model feels about this guess

Part 3: Now, we're free to play around with actual URL links. The code should look something like this:

url-list = ["url-1", "url-2", "url-3", ...]

for url in url-list:

print(guess(url))

Figure 4.1: An example of Car Classification on a single picture (The state car of Vladimir Putin)

This code will return both a car model, and a corresponding confidence measure. You can see a real example (showing only this last cell in the notebook) in figure 4. Note that the output is shown at the very bottom, and correctly guesses the car as a Rolls-Royce Ghost Sedan 2012, with probability roughly 80%

Note that if you're making a large amount of predictions at once, and want to save all your predictions in one place, you can write the output of the guess function to a 'results' variable, and then add this code:

with open('results.json', 'w') as file: json.dump(results, file, indent=4)
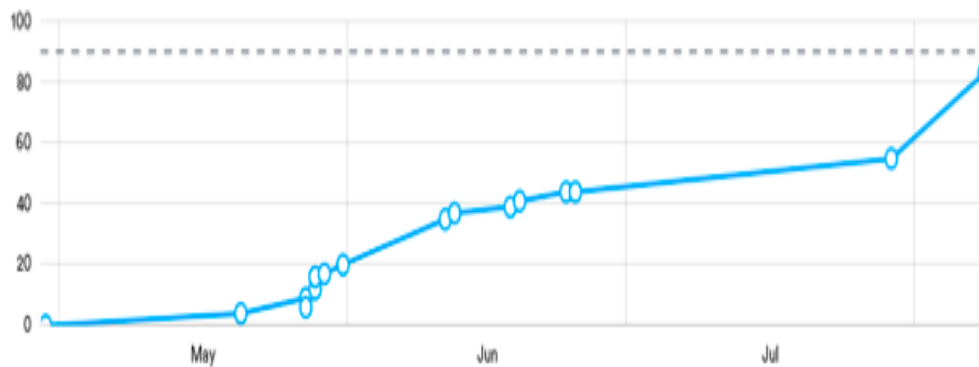This will save predictions to a json file

Figure 4.2: CNN Accuracy over time. I had set myself the personal goal of 90%, which I wasn't actually able to reach. I figured 84% was good enough to call it quits

Chapter 5

Conclusion

We think this should be everything needed to implement an equally robust Deep Learning application. It took us a lot of toiling and fiddling to get it up to competitive (80%+ accuracy) levels. You can actually track our progress in figure 4

Hopefully, if you use what we have presented here as a foundation from which to get started, the only tasks you will have to do are, firstly, data collection and organization, and, secondly, hyperparameter tuning. That should save you a huge amount of time

So have fun exploring this exciting new world of Deep Learning! **No making killer robots please...**

Rockwall Analytics

DATA & ANALYTICS ADVISORY