Machine Learning Engineer Nanodegree

Capstone Project: Dogs vs Cats

Michael Low

February 25th, 2017

Definition

Project Overview

I have chosen to work on the “Dogs vs Cats Redux” Kaggle competition (Kaggle, no date), which is the challenge of automatically distinguishing photos of dogs from photos of cats.

This has been a task that is traditionally very easy for humans, but difficult for computers due to large variety of shapes, breeds, colours, photo composition, lighting and so on in the photos. Ten years ago, it was used as a CAPTCHA challenge (Microsoft, 2007) to distinguish human users of a system from computers. In 2008, techniques in computer vision advanced to sufficiently attack the CAPTCHA with 82.7% accuracy with a SVM classifier (Golle, 2008) making it no longer viable. Modern computer vision techniques using convolutional neural networks should be able to improve on this substantially further still.

I think this is an exciting challenge to work on as, although it may have limited use itself, it encapsulates the fundamental techniques needed to solve a wide range of computer vision problems into a simple problem domain. Consequently, the methods used to achieve high accuracy on the Dogs vs Cats problem can then be applied to a wide range of today's computer vision challenges.

Problem Statement

The problem to be solved is to automatically identify whether a given jpg image is of a cat or a dog, along with a probability reflecting the confidence in that prediction.

The intended way to solve this problem is by using Convolutional Neural Networks (CNNs) and deep learning techniques. The steps necessary are:

* Download an existing neural network model pre-trained on ImageNet data.
* Split the training data into training and validation sets.
* Fine-tune the existing model by training further of our training data.
* Adapt the existing model to return just 'cat' or 'dog' classes, rather than the 1000 ImageNet classes.
* Test and try out different parameters settings to get a high accuracy score on both the training and validation set.

Metrics

The two evaluation metrics proposed to evaluate the classifier performance are accuracy and log loss.

Accuracy is the number of correctly predicted class labels, divided by the total number of predictions made. This is a simple and easy-to-understand metric, and is appropriate due to the dataset being balanced and only binary classification required. In addition, a false positive is not considered either better or worse than a false negative. Therefore, alternative metrics suitable for

imbalanced datasets, such as f1-score, precision and recall, do not offer any real advantage over accuracy in this case.

Log loss is the metric used by Kaggle to judge this competition (Kaggle, no date b). In general, a highly accurate model will also have a low log loss score. Log loss applies a higher penalty for incorrect predictions that had a high probability given to them, making it more appropriate for leaderboard ranking. However, it is less intuitively easy to understand.

As Kaggle uses log loss score, this is the only metric available for the test set. Accuracy can be measured by testing against the validation set.

Analysis

(approx. 2-4 pages)

Data Exploration

In this section, you will be expected to analyse the data you are using for the problem. This data can either be in the form of a dataset (or datasets), input data (or input files), or even an environment. The type of data should be thoroughly described and, if possible, have basic statistics and information presented (such as discussion of input features or defining characteristics about the input or environment). Any abnormalities or interesting qualities about the data that may need to be addressed have been identified (such as features that need to be transformed or the possibility of outliers). Questions to ask yourself when writing this section:

- If a dataset is present for this problem, have you thoroughly discussed certain features about the dataset? Has a data sample been provided to the reader?

- If a dataset is present for this problem, are statistics about the dataset calculated and reported? Have any relevant results from this calculation been discussed?

- If a dataset is \*\*not\*\* present for this problem, has discussion been made about the input space or input data for your problem?

- Are there any abnormalities or characteristics about the input space or dataset that need to be addressed? (categorical variables, missing values, outliers, etc.)

Exploratory Visualization

In this section, you will need to provide some form of visualization that summarizes or extracts a relevant characteristic or feature about the data. The visualization should adequately support the data being used. Discuss why this visualization was chosen and how it is relevant. Questions to ask yourself when writing this section:

- Have you visualized a relevant characteristic or feature about the dataset or input data?

- Is the visualization thoroughly analysed and discussed?

- If a plot is provided, are the axes, title, and datum clearly defined?

Algorithms and Techniques

In this section, you will need to discuss the algorithms and techniques you intend to use for solving the problem. You should justify the use of each one based on the characteristics of the problem and the problem domain. Questions to ask yourself when writing this section:

- Are the algorithms you will use, including any default variables/parameters in the project clearly defined?

- Are the techniques to be used thoroughly discussed and justified?

- Is it made clear how the input data or datasets will be handled by the algorithms and techniques chosen?

Benchmark

In this section, you will need to provide a clearly defined benchmark result or threshold for comparing across performances obtained by your solution. The reasoning behind the benchmark (in the case where it is not an established result) should be discussed. Questions to ask yourself when writing this section:

- Has some result or value been provided that acts as a benchmark for measuring performance?

- Is it clear how this result or value was obtained (whether by data or by hypothesis)?

Methodology

(approx. 3-5 pages)

Data Preprocessing

In this section, all of your preprocessing steps will need to be clearly documented, if any were necessary. From the previous section, any of the abnormalities or characteristics that you identified about the dataset will be addressed and corrected here. Questions to ask yourself when writing this section:

- If the algorithms chosen require preprocessing steps like feature selection or feature transformations, have they been properly documented?

- Based on the \*\*Data Exploration\*\* section, if there were abnormalities or characteristics that needed to be addressed, have they been properly corrected?

- If no preprocessing is needed, has it been made clear why?

Implementation

In this section, the process for which metrics, algorithms, and techniques that you implemented for the given data will need to be clearly documented. It should be abundantly clear how the implementation was carried out, and discussion should be made regarding any complications that occurred during this process. Questions to ask yourself when writing this section:

- Is it made clear how the algorithms and techniques were implemented with the given datasets or input data?

- Were there any complications with the original metrics or techniques that required changing prior to acquiring a solution?

- Was there any part of the coding process (e.g., writing complicated functions) that should be documented?

Refinement

In this section, you will need to discuss the process of improvement you made upon the algorithms and techniques you used in your implementation. For example, adjusting parameters for certain models to acquire improved solutions would fall under the refinement category. Your initial and final solutions should be reported, as well as any significant intermediate results as necessary. Questions to ask yourself when writing this section:

- Has an initial solution been found and clearly reported?

- Is the process of improvement clearly documented, such as what techniques were used?

- Are intermediate and final solutions clearly reported as the process is improved?

Results

(approx. 2-3 pages)

Model Evaluation and Validation

In this section, the final model and any supporting qualities should be evaluated in detail. It should be clear how the final model was derived and why this model was chosen. In addition, some type of analysis should be used to validate the robustness of this model and its solution, such as manipulating the input data or environment to see how the model’s solution is affected (this is called sensitivity analysis). Questions to ask yourself when writing this section:

- Is the final model reasonable and aligning with solution expectations? Are the final parameters of the model appropriate?

- Has the final model been tested with various inputs to evaluate whether the model generalizes well to unseen data?

- Is the model robust enough for the problem? Do small perturbations (changes) in training data or the input space greatly affect the results?

- Can results found from the model be trusted?

Justification

In this section, your model’s final solution and its results should be compared to the benchmark you established earlier in the project using some type of statistical analysis. You should also justify whether these results and the solution are significant enough to have solved the problem posed in the project. Questions to ask yourself when writing this section:

- Are the final results found stronger than the benchmark result reported earlier?

- Have you thoroughly analysed and discussed the final solution?

- Is the final solution significant enough to have solved the problem?

Conclusion

(approx. 1-2 pages)

Free-Form Visualization

In this section, you will need to provide some form of visualization that emphasizes an important quality about the project. It is much more free-form, but should reasonably support a significant result or characteristic about the problem that you want to discuss. Questions to ask yourself when writing this section:

- Have you visualized a relevant or important quality about the problem, dataset, input data, or results?

- Is the visualization thoroughly analysed and discussed?

- If a plot is provided, are the axes, title, and datum clearly defined?

Reflection

In this section, you will summarize the entire end-to-end problem solution and discuss one or two particular aspects of the project you found interesting or difficult. You are expected to reflect on the project as a whole to show that you have a firm understanding of the entire process employed in your work. Questions to ask yourself when writing this section:

- Have you thoroughly summarized the entire process you used for this project?

- Were there any interesting aspects of the project?

- Were there any difficult aspects of the project?

- Does the final model and solution fit your expectations for the problem, and should it be used in a general setting to solve these types of problems?

Improvement

In this section, you will need to provide discussion as to how one aspect of the implementation you designed could be improved. As an example, consider ways your implementation can be made more general, and what would need to be modified. You do not need to make this improvement, but the potential solutions resulting from these changes are considered and compared/contrasted to your current solution. Questions to ask yourself when writing this section:

- Are there further improvements that could be made on the algorithms or techniques you used in this project?

- Were there algorithms or techniques you researched that you did not know how to implement, but would consider using if you knew how?

- If you used your final solution as the new benchmark, do you think an even better solution exists?

References

Golle, P., 2008, October. Machine learning attacks against the Asirra CAPTCHA. In Proceedings of the 15th ACM conference on Computer and communications security (pp. 535-542). ACM.

Kaggle, no date. "Dogs vs. Cats Redux: Kernels Edition" available at <https://www.kaggle.com/c/dogs-vs-cats-redux-kernels-edition>

Keras, no date. "Keras Applications" available at https://keras.io/applications/

Krizhevsky, A., Sutskever, I. and Hinton, G.E., 2012. Imagenet classification with deep convolutional neural networks. In Advances in neural information processing systems (pp. 1097- 1105).

Microsoft, 2007. "Asirra: A CAPTCHA that Exploits Interest-Aligned Manual Image Categorization" available at https://www.microsoft.com/en-us/research/publication/asirra-a-captcha- that-exploits-interest-aligned-manual-image-categorization/