

Convolutional Neural Networks for Classifying Handwritten Digits

Favyen Bastani
fbastani@perennate.com

Zhengli Wang
wzl@mit.edu

December 5, 2014

Abstract

In this project, we implement a CPU-based convolutional neural network (CNN) library in Python, using the `numpy` library for fast array operations. We evaluate CNN performance in terms of classification accuracy and training time on the MNIST database under a wide range of network parameters, and compare CNN to feature extraction approaches such as HOG. We find that CNN is able to achieve much lower misclassification rate, but also requires significantly more time for training of features.

1 Introduction

Image recognition algorithms have become pervasive: on Google Maps Street View, image recognition protects privacy by automatically blurring faces and license plate numbers [2]; robots use object recognition to autonomously move or assemble structures; meanwhile, individuals routinely employ optical character recognition for scanning documents and facial recognition for labeling photographs. Over the last decade, image recognition approaches have developed dramatically. Initially, feature extraction techniques such as HOG and FAST were typically combined with support vector machine (SVM) classifiers, with research often focusing on selection of SVM kernels and defining features for specific image types. Recently, though, neural networks have received renewed attention and achieved high classification performance.

Cells in the mammalian visual cortex are able to identify local patterns in the visual field [3]. Convolutional neural networks (CNNs) aim to do the same through *convolutional and pooling layers*. While traditional neural networks are composed of densely connected layers, where each neuron in the previous layer connects to each neuron in the next layer, convolutional layers restrict filters to be applied on local sub-regions of an in-

put image. By training these layers through back-propagation, these filters eventually detect specific features in the image that help with classification. CNNs have achieved high image recognition accuracy on a large number of datasets [ref].

In this project, we implement a fast CPU-based CNN toolkit [1] in Python using the `numpy` scientific computing library, and apply it to the MNIST handwritten digits database [4]. We evaluate the performance of various neural network parameters (including layer configuration, output layer activation function, and training algorithm) in terms of classification accuracy and training speed, and compare CNN to feature extraction approaches. We find that while CNNs require significantly more training time, they outperform other algorithms with minimal tuning of the network.

In Sections 2 and 3, we detail convolution and pooling functions, the convolutional neural network structure and training algorithm, and our implementation. In Section 4, we experiment with various neural network parameters, and in Section 5, we compare with SVM-based algorithms. Finally, we conclude in Section 6.

2 Neural networks

An artificial neural network (ANN) consists of neuron units that, when composed in a layered network, compute some output function from an input vector $y = h(x)$. Each neuron in the network has a specific set of input values (which may be elements of the input vector of the network, or outputs from other neurons) and a single output. The output is generally computed as $n_{w,b}(z) = f(w \cdot z + b)$ for some *activation function* f , weight vector w , and bias parameter b . The sigmoid function is often used as the activation function, i.e. $f(l) = \frac{1}{1+e^{-l}}$, because it mimics the hard threshold activation pattern of a biological neuron.

Neurons are connected to form a neural network. Typically, the network is composed of layers of neu-

rons, where neurons in the first layer accept inputs from the input vector x , and neurons in each following layer take inputs from the outputs of the neurons in the preceding layer. Then, the network output vector y consists of the outputs from neurons in the last layer of the network. In fully connected neural networks, a neuron takes inputs from every neuron in the previous layer.

Forward propagation refers to the process of propagating some input vector x through each layer of the neural network to compute $y = h(x)$. In a fully connected neural network, this can be done using efficient matrix operations (which can take advantage of fast matrix libraries such as `numpy`). Let Z_l be the output vector of the l th neural network layer (where $Z_0 = x$) and n_{li} be the i th neuron in layer l ; then, $Z_{l+1} = f(W^T Z_l + B)$ where W_{ij} is the weight from n_{li} to $n_{l+1,j}$ and B_j is the bias parameter for neuron $n_{l+1,j}$.

Neural networks can be trained using back propagation. At a high level, we compute a cost function on the outputs from the neural network given some input and desired output, and propagate the error (in the form of partial derivatives of the cost) starting at the last layer to the first layer. These error terms are then used to compute the derivative with respect to specific weight and bias parameters, which can then be updated via gradient descent.

2.1 ANN for multi-label classification

Artificial neural networks are often used for multi-label classification. However, the sigmoid activation function is not well suited for this purpose, where we want to assign exactly one label c for each input vector x . Instead, we use *softmax activation function*, defined as

$$f(L, i) = \frac{e^{L_i}}{\sum_j e^{L_j}}$$

Here, L is a vector containing inputs to the activation function for each neuron in the softmax layer. For back propagation, the cost function given a desired output vector o is the cross-entropy error function,

$$E = - \sum_i o_i \log(y_i)$$

2.2 Stochastic gradient descent

In normal gradient descent neural network training, we iteratively update parameters (weights and

bias terms) after averaging derivatives from back propagation across all training samples. However, when the training set is large, each iteration of gradient descent may take a significant amount of time to complete. Stochastic gradient descent instead randomly selects mini-batches of a predetermined size from the training samples on each iteration and updates parameters by averaging derivatives across only the selected samples (the batch size is generally selected to yield optimal performance with matrix libraries, although in our implementation we perform back propagation separately for each sample). This increases solution sparsity as well as convergence speed.

We implement one variation of stochastic gradient descent that further reduces training time in many cases. Rather than updating parameters directly from the computed gradient ∇ , we apply a momentum that retains gradients from previous iterations. Let $v_0 = 0$ be the initial velocity. For a training rate α and momentum m , we update parameters θ_i on the i th iteration as

$$v_i = mv_{i-1} + \alpha \nabla_i$$

$$\theta_i = \theta_{i-1} - v_i$$

Note that the training rate α is generally smaller in stochastic gradient descent than in conventional gradient descent because the random mini-batch selection introduces greater variance on the training process.

3 Convolutional neural networks

Images, along with many other data types such as audio signals, exhibit strong local patterns that need to be identified for classification. In some cases, fully connected neural networks may ignore these patterns, perhaps overfitting instead; in other cases, training fully connected networks to identify local patterns and achieve high classification accuracy takes a significant number of training iterations. Convolutional neural networks take an alternate approach, where the localized pattern properties are directly encoded into the structure of the neural network. In this section, we discuss the functionality of convolution and pooling layers, and strategies for incorporating them into neural networks.

3.1 Convolution

Images can often be hierarchically broken down into features and sub-features that support image recognition. For example, a flower may contain a stem and a petal, each of which consist of edges at various positions and angles. Additionally, these features may exist at various locations in the image: if an image is shifted in one direction, an image recognition algorithm should still be able to classify it in the same way.

The idea behind convolutional layers for image recognition is that a feature can be represented as an n by n *filter*, and then convolved two-dimensionally with the m by m input (which in this case would be an image). If regions of the input match up with the filter, then elements of the convolution output corresponding to those regions will generally take higher values. The output from the convolution is added with a bias term and passed through an activation function. Notably, each component of the convolution can be modeled as a neuron: each neuron takes inputs from a sub-region, multiplies the input by a weight matrix (the filter), and then applies the activation function; besides the sparsely connected input, the only other difference from conventional neural networks is that we require the weight matrix to be the same across multiple neurons (since convolution applies a single filter repeatedly across the image). This enables the detection of local patterns that we desire, since the filter is restricted to only consider sub-regions of the input, while still incorporating the weights and bias components that define neural networks.

In each convolutional layer, we have k filters, each an n by n matrix. Then, for an m by m input, we get a k by $(m - n + 1)$ by $(m - n + 1)$ output from the two-dimensional convolution.

3.2 Pooling

Pooling layers apply an aggregate function (typically either max or mean) on non-overlapping regions of the output from convolutional layers (this is done separately for each filter). These regions are often equal in size; so if the output from the convolutional layer is 30 by 30, the pooling layer may pool across each of the four 15 by 15 regions, yielding four output values.

Pooling accomplishes two purposes. First, we reduce the amount of data that later layers need to consider, speeding up training and reducing overfitting. Second, we get a degree of translation invariance. If the input is shifted slightly, the result after pooling will still be similar. This is desirable

since generally image recognition classes should remain the same under basic transforms.

3.3 Network

Convolution and pooling can be used in isolation, without incorporation in a convolutional neural network. In this case, an autoencoder is typically used to train the filters, where the training goal is to have the output layer match the input layer despite a smaller number of neurons in intermediate layers. The trained filters can then be used to extract features from both training and testing data, and then fed into any classifier. This also supports unsupervised learning of features.

Convolutional neural networks present a more interesting case, where the convolution and pooling operations are combined with classification into a single structure that can be trained in one process. Typical convolutional neural networks consist of one to three convolutional layers followed by fully connected hidden layers; back propagation is carried out across the entire network. When there are several convolutional layers, the first convolutional layer often is used by the network as an edge detector (this determination happens from training alone, without any manual specification other than the layer sizes), while later convolutional layers in the network detect more and more complex features; for simple datasets, a single convolutional layer can be applied to directly identify features. The hidden layers use final pooling outputs to eventually classify the image.

4 CNN evaluation

We implement a CPU-based convolutional neural network library [1] in Python using the `numpy` package, which provides fast scientific computing operations. We evaluate its performance on the MNIST dataset of handwritten digits in terms of overall training algorithm, network structure, number of filters, size of filters, number of pooling regions, and output layer activation function.

4.1 MNIST dataset

The Mixed National Institute of Standards and Technology (MNIST) dataset contains sixty thousand training images and ten thousand testing images. Its name comes from the NIST dataset that it is an adaptation of. In the NIST dataset, training and testing images were taken from two different sources, while in MNIST, the sources are merged.

Hidden Layer Configuration	Test Error	Time of One Iteration / Sec
No hidden layer	0.0269	30.48
10-neuron hidden layer	0.0173	30.80
16-neuron hidden layer	0.0174	30.66
32-neuron hidden layer	0.0181	30.56
32-neuron followed by 16-neuron hidden layers	0.0193	30.43

Table 1: Performance of Our Neural Nets Using Different Configurations After Pooling Layer

Each MNIST image contains a single handwritten digit (from zero to nine). The images are all 28 pixels by 28 pixels and grayscale.

There are numerous ways to implement the neural net. In our actual implementation, we use a basic default setting of the neural net, and then adjust parameters of it to look at the change to its performances, such as test error rate and average time taken to run an iteration. In our implementation, the default setting is using 64 filters of size 13 by 13, a pooling layer of size 2 by 2. The layer after the pooling stage consists of 256 neurons, which will then be directly and completely connected to the final output layer consisting of 10 neurons, i.e. no more layers between the post-pooling layer and final output layer.

4.2 Performance of Our Neural Nets Using Different Configurations After Pooling Layer

To start, we explore how different configurations of the neural nets after the pooling layer affects the performance of our neural net. We can see that generally they all have the same average iteration time. As we go down the table, the model gets more complex, and the test error first goes down and then goes up, suggesting overfitting for the last model.

4.3 Performance of Our Neural Nets Using Different Filter Size (Default Setting)

Firstly we investigate how filter size affects the performance of our neural net. We tried out various different filter sizes ranging from “5 by 5” to “15 by 15”. For each of the filter size, we tested in our neural nets, using the 60,000 training data, and then tested on the 10,000 testing data, with both

training and testing data from MNIST. Our neural net is run with the each filter size for 10 hours on the training data.

The results are shown in figure 1 and 2. The horizontal axis of both figures show the filter size. For instance, when the filter size is “7 by 7”, it achieves an test error rate at about 3.5% and average iteration time takes about 20 seconds.

From the results, we can see that as filter size increases, the average iteration time generally increases. This is probably because low filter size model has fewer number of features, and the update of the features is faster. On the other hand, high filter size model has much more number of features. For instance, the “15 by 15” filter size model has 25 times many features than the “5 by 5” filter size model, and thus the update is much slower, which contributes to slower running time per iteration. From our experiment, the filter size that achieves the fastest running time is “5 by 5”, the smallest of all filter sizes.

The test error rate generally decreases and then increases. This is probably because a very low filter size has too few features, and thus cannot capture all the information from the image; while a very high filter size tends to have too many features, and thus tends to overfit the training data and, as a consequence, performs badly in test data. Another problem with high filter size model is that the training time takes longer due to more features, and thus when terminated at a fixed time (as in our experiment), it will have run much fewer iterations than the low filter size model, i.e. the number of iteration completed is not sufficient. From our experiment, the optimal filter size range is from “9 by 9” to “13 by 13”.

4.4 Performance of Our Neural Nets Using Different Number of Filters (Default Setting)

Secondly we investigate how changing the number of filters affects the performance of our neural net. Note that for all experiments in this subsection, we use the default setting of filter size “13 by 13”. The number of filters we explored ranges from 8 to 256. Again, our neural net is run with the each filter size for 10 hours on the training data from MNIST.

The results are shown in figure 3 and 4. The horizontal axis of both figures show the the number of filters used, and is plotted in log scales. For instance, when the number of filters is 16, it achieves an test error rate at about 3% and average iteration time takes about 10 seconds.

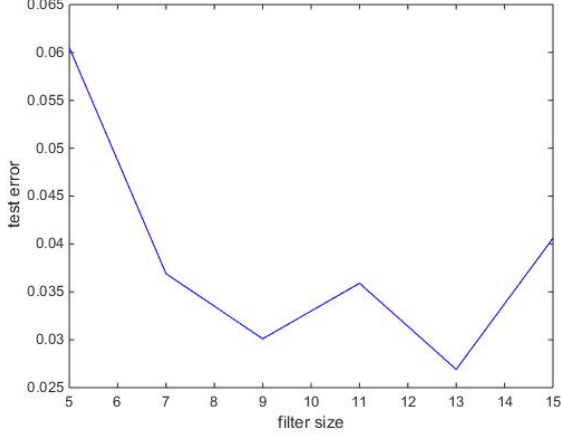


Figure 1: Test Error Against Filter Size (Default Setting)

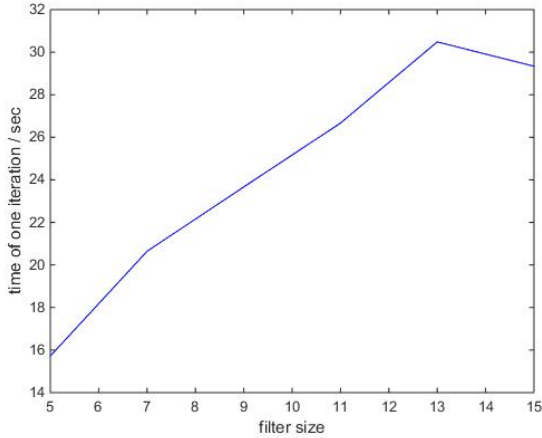


Figure 2: Time Per Iteration Against Filter Size (Default Setting)

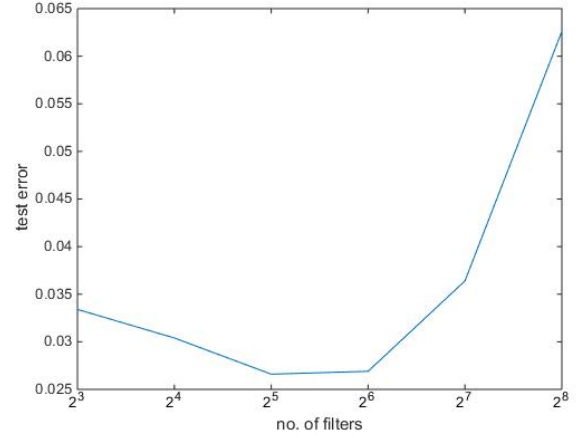


Figure 3: Test Error Against Number of Filters (Default Setting)

From the results, we can see that as the number of filters increases, the average iteration time generally increases, with almost the same speed. This is as expected, because the fewer number of filters in the model, the less complex the model is, and hence the fewer parameters the model needs to update. For instance, the model that with 256 filters have approximately 16 times more parameters (weights, features, etc.) to update compared to the model with 16 filters, and this shows in figure 4 as the running time per iteration for the former model is about 16 times of that of the latter model.

The test error rate generally decreases and then increases. This is probably due to the same reason that we mention previously: models with low number of filters underfit the training data, while models with high number of filters tends to overfit. From our experiment, the optimal number of filters to use ranges approximately from 16 to 64.

4.5 Performance of Our Neural Nets Using Different Pooling Sizes (Default Setting)

Next we investigate how different pooling sizes used affects the performance of our neural net. Again that for all experiments in this subsection, we use the default setting of 64 filters of size “13 by 13”. The number of filters we explored ranges from the extreme case “1 by 1” (pool all things into one) to “6 by 6”.

The results are shown in figure 5 and 6. The horizontal axis of both figures show the the dimension of the pooling size used. For instance, when the pooling size is 4 by 4, it achieves an test error

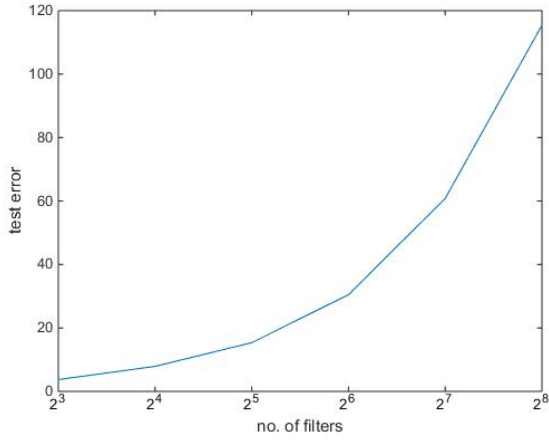


Figure 4: Time Per Iteration Against Number of Filters (Default Setting)

rate at about 4.2% and average iteration time takes about 34 seconds.

From the results, we can see that as the number of pooling size increases, the average iteration time general increases, and the relationship is almost linear. This is as expected, because the fewer number of filters in the model, the less complex the model is, and hence the fewer parameters the model needs to update. For instance, the model that with pooling sizes of “6 by 6” have many more parameters (weights, features, etc.) to update compared to the model with pooling size “1 by 1”, and this shows up in figure 6.

Again, The test error rate shows a “U-shape” trend, and the reason is the same as that in the previous subsection: models with low number of filters underfit the training data, while models with high number of filters tends to overfit. From our experiment, the optimal pooling size is “2 by 2”.

4.6 Heatmap

5 Comparison with HOG-feature recognition

Before deep learning technique is widely used in image recognition, various other methods were used to extract the features from the image and models were trained on these features. Examples include HOG (Histogram of Oriented Gradients) Feature Extraction and SIFT (Scale Invariant Feature Transform) Feature Extraction. In this section, we will compare the results by our neural nets model and by HOG Feature Extraction technique + SVM,

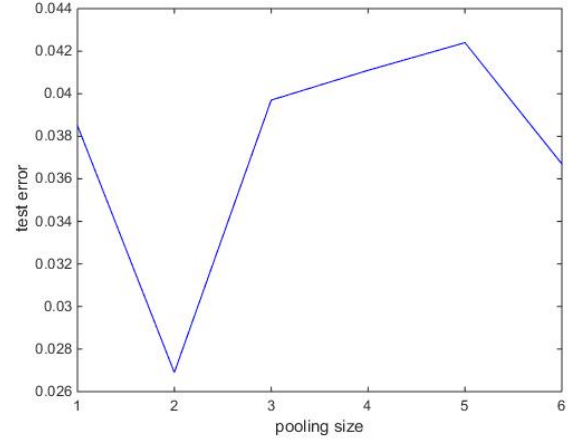


Figure 5: Test Error Against Pooling Size (Default Setting)

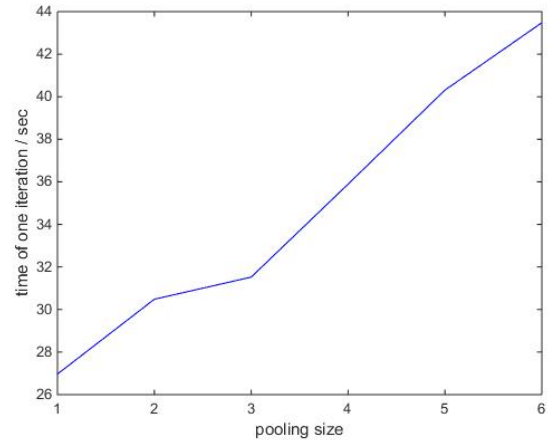


Figure 6: Time Per Iteration Against Pooling Size (Default Setting)

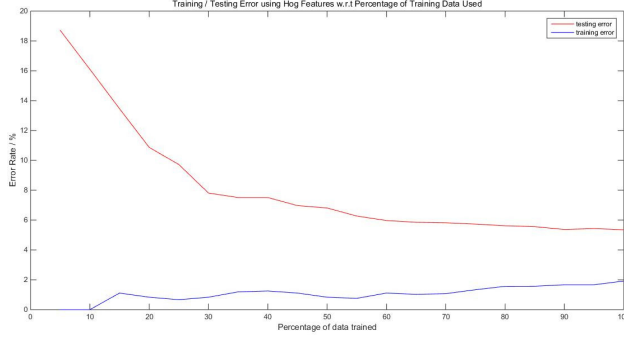


Figure 7: Training / Testing Error Using Hog Features Against Percentage of Training Data Used

using different percentage of the 60,000 training data.

Note that we have completely implemented the neural net model ourselves, but we used Matlab packages for the Hog Classification Method.

The results are shown in figure 7 and 8. From the figures, we can see that the training error rate is generally lower than the testing error rate, and this is expected because our model is based on the training set. Moreover, as we used more training data, we generally got a higher training error, but a lower testing error. This is because with less training data, it is much easier to fit a model that does very well on the training set, but the same model does not generalize well to the overall data, and thus performs badly on the testing set. As the training set data increases, although we get a higher training error as it becomes increasingly harder to fit a perfect model on the training set, the testing error generally decreases. This agrees with our intuition.

Moreover, we can see that our neural net model performs much better than the HOG feature-extraction technique. At any percentage of training data, our model achieves a test error strictly less than the HOG feature-extraction technique. When all training data is used, our neural net model achieves an error rate of about 2.25 percent test error, while the HOG feature-extraction technique achieves more than 6 percent. This perhaps explains why the old feature-extraction techniques, such as HOG and SIFT, are becoming increasingly obsolete today, due to the advent of deep learning..

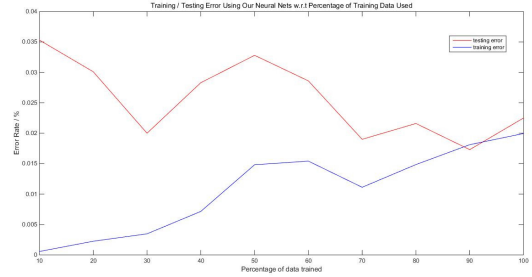


Figure 8: Training / Testing Error Using Our Neural Net Against Percentage of Training Data Used

6 Conclusion

References

- [1] Favyen Bastani and Zhengli Wang. CNN git repository, December 2014. <https://github.com/uakfdotb/cnn>.
- [2] Andrea Frome, German Cheung, Ahmad Abdulkader, Marco Zennaro, Bo Wu, Alessandro Bissacco, Hartwig Adam, Hartmut Neven, and Luc Vincent. Large-scale privacy protection in google street view. In *IEEE International Conference on Computer Vision*, 2009.
- [3] LISA Lab. DeepLearning documentation: Convolutional neural networks (LeNet), December 2014. <http://deeplearning.net/tutorial/lenet.html>.
- [4] Yann LeCun, Corinna Cortes, and Christopher J.C. Burges. MNIST database of handwritten digits. <http://yann.lecun.com/exdb/mnist/>.