$FMAN45 \underset{\tiny ML~Assignment-3}{Machine} \ Learning$

Praveenkumar HIREMATH

August 17, 2023

Common layers and backpropagation

Exercise 1: Derive expressions for $\frac{\partial L}{\partial \mathbf{x}}$, $\frac{\partial L}{\partial \mathbf{W}}$ and $\frac{\partial L}{\partial \mathbf{b}}$ in terms of $\frac{\partial L}{\partial \mathbf{y}}$, W and \mathbf{x} .

A neural network layer can be presented as $f = \sigma \circ l : \mathbb{R}^m \to \mathbb{R}^n$. The layer performs two tasks, namely

• Linearization: A datapoint $\mathbf{x} \in \mathbb{R}^m$ enters the layer and is modified as $\mathbf{y} = l(\mathbf{x}) \in \mathbb{R}^n$ i.e.

$$y_i = \sum_{i=1}^m W_{ij} x_j + b_i \tag{1}$$

Equation (1) can be written in matrix form as $\mathbf{y} = \mathbf{W}\mathbf{x} + \mathbf{b}$ where we need to train the model for optimal \mathbf{W} and \mathbf{b} .

• Activation of neurons (also called nodes) in a layer: The output of linearization goes into an activation function that leads to a neuron in a node having an active or inactive state.

Therefore, the training of a network requires the calculation of different gradients for back propagation in the neural network.

(i) $\frac{\partial L}{\partial x_i}$:

$$\frac{\partial L}{\partial x_i} = \sum_{l=1}^n \frac{\partial L}{\partial y_l} \frac{\partial y_l}{\partial x_i}$$

$$= \sum_{i=1}^n \frac{\partial L}{\partial y_l} \frac{\partial}{\partial x_i} \left(\sum_{j=1}^m W_{lj} x_j + b_j \right)$$

$$= \sum_{i=1}^n \frac{\partial L}{\partial y_l} W_{li}$$

$$\implies \frac{\partial L}{\partial x_i} = \sum_{l=1}^n W_{il} \frac{\partial L}{\partial y_l}$$
(2)

$$\Rightarrow \begin{pmatrix} W_{1,1} & W_{2,1} & W_{3,1} & \dots & W_{m,1} \\ W_{1,2} & W_{2,2} & W_{3,2} & \dots & W_{m,2} \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ \vdots & \vdots & \ddots & \dots & \vdots \\ \vdots & \vdots & \ddots & \dots & \vdots \\ W_{1,n} & W_{2,n} & W_{3,n} & \dots & W_{m,n} \end{pmatrix} \cdot \begin{pmatrix} \partial L/\partial y_1 \\ \partial L/\partial y_2 \\ \vdots \\ \vdots \\ \partial L/\partial y_m \end{pmatrix} = \mathbf{W} \frac{\partial L}{\partial \mathbf{y}}$$
(3)

(ii) Now $\frac{\partial L}{\partial W_{ij}}$:

$$\frac{\partial L}{\partial W_{ij}} = \sum_{l=1}^{n} \frac{\partial L}{\partial y_l} \frac{\partial y_l}{\partial W_{ij}}$$
$$= \sum_{l=1}^{n} \frac{\partial L}{\partial y_l} \frac{\partial}{\partial W_{ij}} \left(\sum_{o=1}^{m} W_{lo} x_j + b_o \right)$$

the partial derivative w.r.t. W_{ij} is non-zero and equal to x_j only for i = l and o = j

$$\implies \frac{\partial L}{\partial W_{ij}} = \frac{\partial L}{\partial y_i} x_j \tag{4}$$

$$\implies \begin{pmatrix} \frac{\partial L}{\partial y_1} \\ \frac{\partial L}{\partial y_2} \\ \vdots \\ \frac{\partial L}{\partial y_m} \end{pmatrix} \cdot (x_1 \ x_2 \x_m) = \frac{\partial L}{\partial \mathbf{y}} \mathbf{x}^T$$

$$(5)$$

(iii) Similarly for $\frac{\partial L}{\partial b_i}$,

$$\frac{\partial L}{\partial b_i} = \sum_{l=1}^n \frac{\partial L}{\partial y_l} \frac{\partial y_l}{\partial b_i}$$
$$= \sum_{i=1}^n \frac{\partial L}{\partial y_l} \frac{\partial}{\partial b_i} \left(\sum_{o=1}^m W_{lo} x_o + b_o \right)$$

the partial derivative w.r.t. b_i is non-zero and equal to 1 only for i = o

$$\implies \frac{\partial L}{\partial b_i} = \frac{\partial L}{\partial y_i} \tag{6}$$

$$\implies \frac{\partial L}{\partial \mathbf{b}} = \frac{\partial L}{\partial \mathbf{y}} \tag{7}$$

Exercise 2: Computing the gradients of batches.

With N elements in a batch, multiple inputs $\mathbf{x}^{(1)}, \mathbf{x}^{(2)}, ... \mathbf{x}^{(N)}$ form the columns of matrix \mathbf{X} , and \mathbf{X} is given by

$$\mathbf{X} = \left(\mathbf{x}^{(1)} \ \mathbf{x}^{(2)} \dots \ \mathbf{x}^{(N)}\right). \tag{8}$$

Then, y = Wx + b becomes,

$$\mathbf{Y} = (\mathbf{y}^{(1)} \ \mathbf{y}^{(2)} \ \dots \ \mathbf{y}^{(N)}) = (\mathbf{W}\mathbf{x}^{(1)} + \mathbf{b} \ \mathbf{W}\mathbf{x}^{(2)} + \mathbf{b} \ \dots \ \mathbf{W}\mathbf{x}^{(N)} + \mathbf{b})$$
(9)

because a datapoint $\mathbf{x} \in \mathbb{R}^m$ and the size of a batch is $N, \mathbf{Y} \in \mathbb{R}^{mXN}$. The equation (9) is implemented in the file "layers/fully_connected_forward.m" as follows.

```
1 %implementing for forward propagation
2 b = repmat(b,1,batch); % replicating bias vector
3 Y = W*X + b;
```

From exercise 1,

$$\frac{\partial L}{\partial b_i} = \sum_{l=1}^{n} \frac{\partial L}{\partial y_l} \frac{\partial y_l}{\partial b_i}$$

and from equation (9),

$$\Rightarrow \frac{\partial L}{\partial b_{i}} = \sum_{k=1}^{N} \sum_{l=1}^{n} \frac{\partial L}{\partial y_{l}^{(k)}} \frac{\partial y_{j}^{(k)}}{\partial b_{i}}$$

$$= \sum_{k=1}^{N} \sum_{l=1}^{n} \frac{\partial L}{\partial y_{l}^{(k)}} \frac{\partial}{\partial b_{i}} \left(\sum_{j=1}^{m} W_{lj} x_{j}^{(k)} + b_{j} \right)$$

$$= \sum_{k=1}^{N} \frac{\partial L}{\partial y_{i}^{(k)}} \quad \text{when } i = j$$

$$\Rightarrow \frac{\partial L}{\partial \mathbf{b}} = \frac{\partial L}{\partial \mathbf{Y}} \mathbf{I}$$
(10)

where **I** is a row vector and has dimensions NX1, and $\frac{\partial L}{\partial \mathbf{Y}}$ has dimension mXN.

Thus, $\frac{\partial L}{\partial \mathbf{b}}$ has dimension mX1.

Similarly,

$$\frac{\partial L}{\partial W_{ij}} = \sum_{k=1}^{N} \sum_{l=1}^{n} \frac{\partial L}{\partial y_{j}^{(k)}} \frac{\partial y_{j}^{(k)}}{\partial W_{ij}}$$

$$= \sum_{k=1}^{N} \sum_{l=1}^{n} \frac{\partial L}{\partial y_{j}^{(k)}} \frac{\partial}{\partial W_{ij}} \left(\sum_{j=1}^{m} W_{lj} x_{j}^{(k)} + b_{j} \right)$$

$$= \sum_{k=1}^{N} \frac{\partial L}{\partial y_{i}^{(k)}} x_{j}^{(k)} \quad \text{when } i = l$$

$$\implies \frac{\partial L}{\partial \mathbf{W}} = \frac{\partial L}{\partial \mathbf{Y}} \mathbf{X}^{T}$$
with $\frac{\partial L}{\partial \mathbf{W}}$ having dimension $m \times n$. (11)

Finally,

$$\frac{\partial L}{\partial \mathbf{X}} = \left(\frac{\partial L}{\partial \mathbf{x}^{(1)}} \quad \frac{\partial L}{\partial \mathbf{x}^{(2)}} \quad \dots \frac{\partial L}{\partial \mathbf{x}^{(N)}}\right)
= \left(\mathbf{W}^{T} \frac{\partial L}{\partial \mathbf{y}^{(1)}} \quad \mathbf{W}^{T} \frac{\partial L}{\partial \mathbf{y}^{(2)}} \quad \dots \mathbf{W}^{T} \frac{\partial L}{\partial \mathbf{y}^{(N)}}\right)
\implies \frac{\partial L}{\partial \mathbf{X}} = \mathbf{W}^{T} \frac{\partial L}{\partial \mathbf{Y}}
\text{with } \frac{\partial L}{\partial \mathbf{X}} \text{ having dimension } nXN.$$
(12)

Equations (10, 11 and 12) are implemented in the file "layers/fully_connected_backward.m" as follows.

```
1 % For Backward propagation implementation
2 dldb = sum(dldY, 2);
3 dldX = W'*dldY;
4 dldX = reshape(dldX, sz);
5 dldW = dldY*X';
```

Exercise 3: Regularized Linear Unit (ReLU).

The ReLU function is given by

$$ReLU: \mathbb{R} \to \mathbb{R}; \qquad x_i \to y_i := max(x_i, 0)$$
 (13)

Equation (13) is implemented in the file "layers/relu_forward.m" as follows.

```
1 % ReLU implementation
2 Y = max(X,0);
```

differentiation of this ReLU function w.r.t. x_i yields,

$$\frac{\partial L}{\partial x_i} = \sum_{l=1}^n \frac{\partial L}{\partial y_j} \frac{\partial y_l}{\partial x_i} = \sum_{l=1}^n \frac{\partial L}{\partial y_j} \frac{\partial}{\partial x_i} (max(x_l, 0)) = \begin{cases} \frac{\partial L}{\partial y_i}, & \text{for } l = i \text{ and } x_i > 0\\ 0, & \text{for } l \neq i \text{ and } x_i \leq 0. \end{cases}$$
(14)

The equation (14) is implemented in the file "layers/relu_backward.m" as follows.

```
1 %ReLU backprop
2 function dldX = relu_backward(X, dldY)
3     dldX = dldY.*heaviside(X);
4 end
```

Exercise 4: Softmax loss

It is given that for a vector $\mathbf{x} = [x_1,...,x_m]^T \in \mathbb{R}^m$, the probability of class i can be expressed as

$$y_i = \frac{e^{x_i}}{\sum_{j=1}^m e^{x_j}}. (15)$$

Supposing that the ground truth class is c, the loss L that needs to be minimized is given by

$$L(\mathbf{x},c) = -\log(y_c) = -\log\left(\frac{e^{x_c}}{\sum_{j=1}^m e^{x_j}}\right) = -x_c + \log\left(\sum_{j=1}^m e^{x_j}\right)$$
(16)

Equation (16) is implemented in the file "layers/softmaxloss_forward.m" as follows.

```
1 %Softmaxloss forward
2 x_lin_ids = sub2ind(sz,labels',1:batch); % converting to linear indices
3 L = mean(log(sum(exp(x)))-x(x_lin_ids));
```

Computing $\frac{\partial L}{\partial x_i}$: Differentiating the loss $L(\mathbf{x},c)$, i.e. equation (16), gives

$$\frac{\partial L}{\partial x_i} = \frac{\partial}{\partial x_i} \left(-x_c + \log \left(\sum_{j=1}^m e^{x_j} \right) \right) = \begin{cases} -\left(1 - \frac{e^{x_i}}{\sum_{j=1}^n e^{x_j}}\right) = y_i - 1, & \text{for } i = c \\ \frac{e^{x_i}}{\sum_{j=1}^n e^{x_j}} = y_i, & \text{for } i \neq c. \end{cases}$$
(17)

Equation (17) is implemented in the file "layers/softmaxloss_backward.m" as follows.

```
1 %Softmaxloss backprop
2 x_lin_ids = sub2ind(sz,labels',1:batch); % Linear indices
3 dldx = exp(x)./sum(exp(x)); % when i different from c
4 dldx(x_lin_ids) = dldx(x_lin_ids) - 1; % when i same as c
5 dldx = dldx./batch; % because of averaging over batch during forward prop
```

Training a Neural Network

Exercise 5: Gradient descent with momentum

Training a neural network involves minimizing the loss (one example loss)

$$L(\mathbf{w}) = \frac{1}{2} \sum_{i=1}^{N} L(\mathbf{x}^{(i)}, z^{(i)}; \mathbf{w}).$$
(18)

Here, \mathbf{w} , $\mathbf{x}^{(i)}$ and $z^{(i)}$ stand for network parameters, network input, and corresponding ground truth, respectively. Because N is usually very large, the gradient is evaluated over a batch of $n \ll N$ elements. Then using the gradient descent algorithm, the parameters are updated as follows.

$$\mathbf{w}_{n+1} = \mathbf{w}_n - \alpha \frac{\partial L}{\partial \mathbf{w}} \tag{19}$$

with the hyperparameter α being the network learning rate

In gradient descent with momentum, the parameters are updated by modifying the equation (19), as follows.

$$\mathbf{m}_{n} = \mu \mathbf{m}_{n-1} + (1 - \mu) \frac{\partial L}{\partial \mathbf{w}}$$
 (20)

and

$$\mathbf{w}_{n+1} = \mathbf{w}_n - \alpha \mathbf{m}_n \tag{21}$$

Here, \mathbf{m}_n is a moving average of the gradient estimations while the hyperparameter $0 < \mu < 1$ controls the smoothness of the gradient used to update parameters. This gradient descent with momentum is implemented as follows. This implementation can be found in the file "training.m".

Classifying handwritten digits (MNIST dataset)

Exercise 6

Using the baseline model provided in the file "mnist_starter.m", an accuracy of 0.9773 (97.73%) was achieved for training options: $\alpha = 1e^{-1}$, 'iterations' = 3000, 'batch size' = 16, 'momentum' = 0.9 and 'weight decay' = 0.005. For this model, kernels learned by the first convolution layer are provided in Figure 1. From these kernels, though it is hard to precisely say what features are identified, it looks like features like edges, slanted lines (/), and curved lines are recognized.

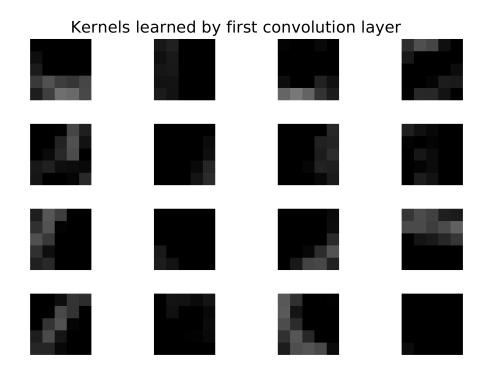


Figure 1: Kernels learned by first convolution layer (MNIST dataset).

With 0.9773 accuracy, this baseline model for MNIST predicts some digits wrongly. The images of such wrongly predicted digits are presented in Figure 2. Some of these images look hard to predict even for humans. So the model missclassifying such images was expected. However, '6' predicted as '5' and '0' predicted as '8' were surprising. This shows that the model is not perfect (97.73% accuracy). Further, the confusion matrix is plotted in Figure 3. Using the confusion matrix, precision and recall are computed for each class (each digit $\in 0,1..9$) and provided in Table 1. For all the digits, precision and recall values are close to one which means the model performance is very good. The average precision and recall of the model are 0.9737 and 0.9735, respectively. The number of parameters in the network (baseline) is provided in Table 2.

Additionally, an attempt was made to further improve the baseline model for MNIST dataset by reducing the learning rate α from $1e^{-1}$ to $1e^{-3}$ and increasing iterations to 7000. The accuracy of the model on testset reduced to 91%. This is because of the slow progress towards optimum due to 100 times smaller α . This meant that a larger number of iterations are needed. Therefore, this was not ventured any further.

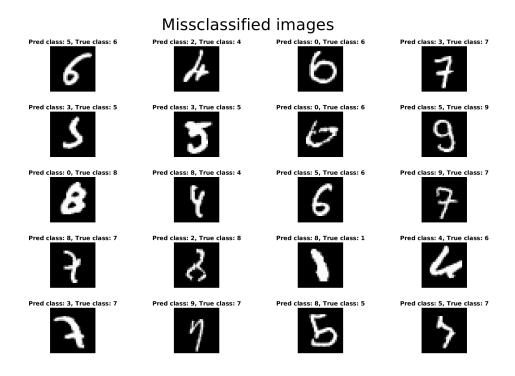


Figure 2: Images of wrongly predicted digits.

Confusion matrix chart using Matlab's confusionmat() and confusionchart() **Predicted Class**

Figure 3: MNIST confusion matrix chart.

Table 1: Computation of precision and recall on MNIST dataset.

$\overline{\text{Class (digit)}} =$	0	1	2	3	4	5	6	7	8	9
Precision =	0.9653	0.9955	0.9445	0.9662	0.9897	0.9689	0.9978	0.9938	0.9483	0.9675
Recall =	0.9949	0.97	0.9903	0.9891	0.9796	0.9776	0.952	0.93	0.9784	0.9732

Table 2: Details of parameters in each layer. ReLU, max-pooling, and softmaxloss layers do not have any parameters.

Layer	# Weights (Ws)	# Biases (bs)	# Total parameters
1 st Convolution layer	400	16	416
2 nd Convolution layer	6400	16	6416
Fully-connected layer	7840	10	7850
Total of all layers	14640	42	14682

Classifying tiny images (CIFAR10 dataset)

Exercise 7: Improving CIFAR model

The baseline model provided in the file "cifar10_starter.m" for CIFAR dataset, has the training options

- Number of images = 20000
- Learning rate $\alpha = 1e^{-3}$
- Iterations = 5000
- Batch size = 16
- momentum = 0.95
- Weight decay = 0.001

This baseline model has an input layer followed by a convolution layer with 16 (5X5) kernels. This convolution layer was followed by a ReLU and a maxpooling layers. Then another convolution layer with 16 (5X5) kernels. This 2nd convolution layer was followed by a ReLU, a fully connected, and a softmaxloss layers, in order. This baseline model gave an accuracy of 0.474 on the testset.

Steps taken to improve the above model

- In the case of MNIST data model, after reducing the learning rate, many more iterations were required to reach higher model/network accuracy. Therefore, despite knowing that reducing the learning rate could potentially improve the model, it was not avoided as much as possible for CIFAR data.
- While keeping the baseline model as it is, the number of training images was increased to 40000 (from 20000). This increased the accuracy to 0.4887 (from 0.474).

- With 40000 images, increasing the number of iterations to 10000 in the baseline model did not improve the model, despite the higher computational cost. In all the following attempts to improve the model, 40000 images were used.
- (Again 40000 images) Changing only momentum to 0.99 (from 0.95) and number of iterations to 15000 (from 5000), seemed promising. This improved the model accuracy to 0.535 however again at a higher computational cost.
- (Again 40000 images) Increasing only the batch size to 50 (from 16), while keeping other options the same as in the baseline model (iterations = 5000, learning rate = $1e^{-3}$..) improved the accuracy to 0.52 at slightly higher computational cost.
- Observations until this point proved that the accuracy can be increased by reducing the learning rate and changing the momentum to 0.99 but at a much higher computational cost (because a very high number of iterations was needed). Increasing the batch size yielded better accuracy at a lower cost of computation relative to other options tried.
- Now only the 1st convolution layer (with 16 (5X5) kernels) in the baseline model was replaced (in order lines 42 to 63 in the file "cifar10_optimized.m") by
 - A convolution layer with 32 (5X5) kernels.
 - A ReLU layer.
 - A maxpooling layer.
 - Another convolution layer with 16 (5X5) kernels.
 - Another ReLU layer.
 - Another maxpooling layer.

Because of the significant intraclass variations in CIFAR dataset, more (32) kernels are used in the first convolution layer to identify and select more features in the images. Then building upon these features, a bit more complex features can be identified in the subsequent convolution layers. This strategy was adopted in the hope that the intraclass variations are better identified and used to classify the images in the test dataset. As expected, this model with changed network architecture gave an accuracy of 0.552 (while all other settings remained similar to the baseline model).

- Finally, with this newly added convolution, ReLU, and maxpooling layers and with
 - -40000 images
 - learning rate $1e^{-3}$
 - momentum = 0.95
 - batch size = 50
 - iterations = 5000
 - weight decay = 0.001

an accuracy of 0.601 was achieved. Thus the baseline model was improved for the CIFAR dataset. This improved model for CIFAR is saved in

"models/cifar10_baseline40k_batch50_iters_mu95_2conv_with_32_and_16.mat".

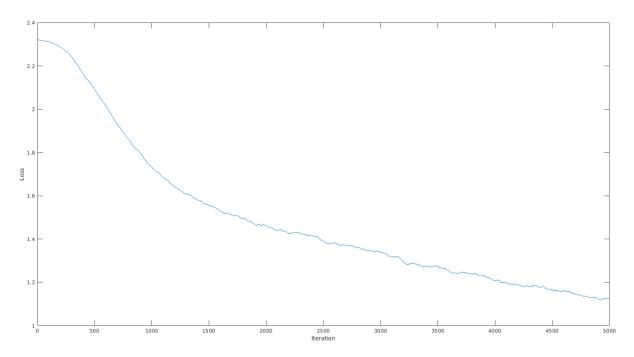


Figure 4: Loss versus number of iterations (CIFAR dataset - improved model).

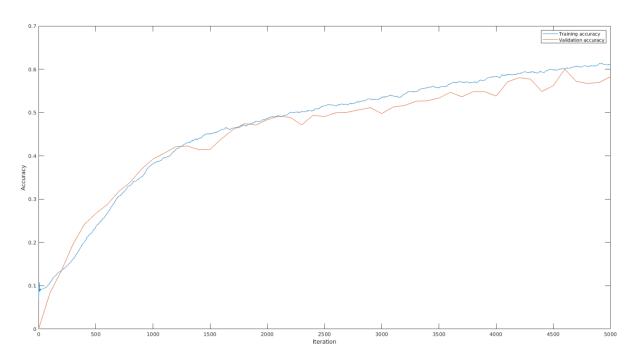


Figure 5: Accuracy versus number of iterations (CIFAR dataset - improved model). Blue curve: Training accuracy and Red curve: Validation accuracy.

Figures 4 and 5 are the plots of (i) loss vs number of iterations and (ii) Accuracy vs number of iterations using the improved CIFAR model. The 32 kernels learned by the first convolution layer in the improved model (network) are provided in Figure 6. Of the images that were wrongly and correctly predicted by this improved model, a few are presented in Figures 7 and 8, respectively.

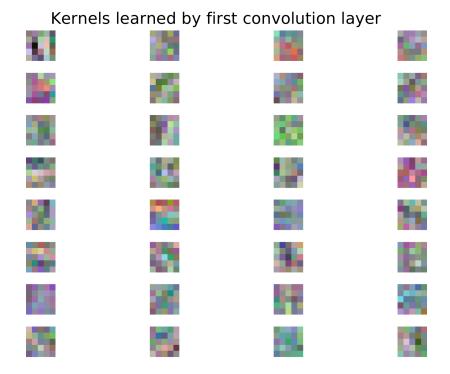


Figure 6: 32 (5X5) Kernels learned by first convolution layer (CIFAR dataset - improved model).



Figure 7: Wrongly predicted cifar images (improved model).

Correctly classified images PC:cat, TC:cat PC:ship, TC:ship PC:dog, TC:frog PC:dog, TC:dog PC:airplane, TC:airplane PC:airplane, TC:airplane PC:airplane, TC:airplane PC:horse, TC:horse PC:ship, TC:ship PC:ship, TC:ship PC:dog, TC:dog PC:airplane, TC:airplane PC:horse, TC:horse PC:horse, TC:horse PC:ship, TC:ship PC:horse, TC:horse PC:airplane, TC:airplane PC:dog, TC:dog PC:dog,

Figure 8: Correctly predicted cifar images (improved model). Here, "PC" and "TC" stand for predicted and true classes, respectively.

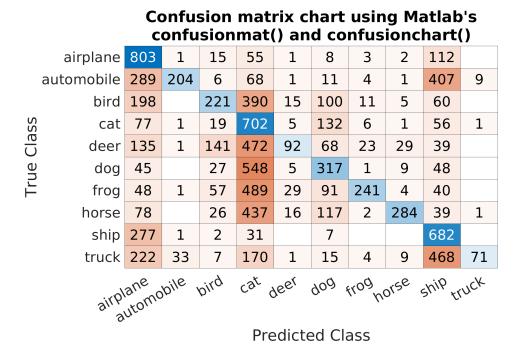


Figure 9: CIFAR dataset confusion matrix chart (improved model).

Table 3: Computation of precision and recall using the improved model on CIFAR dataset. Here, F_{1} -score = $\frac{2*Precision*Recall}{Precision+Recall}$.

$\overline{\text{Class (digit)}} =$	Airplane	Automobile	Bird	Cat	Deer	Dog	Frog	Horse	Ship	Truck
Precision =	0.3697	0.843	0.4242	0.2088	0.5576	0.3661	0.8169	0.8256	0.3496	0.8659
Recall =	0.803	0.204	0.221	0.702	0.092	0.317	0.241	0.284	0.682	0.071
$\overline{F_1\text{-score}} =$	0.5063	0.3285	0.2906	0.3219	0.1579	0.3398	0.3722	0.4226	0.4623	0.1312

Table 4: Details of the network and number of parameters in each layer for the improved CIFAR model. ReLU, max-pooling, and softmaxloss layers do not have any parameters.

Layer	# Weights (Ws)	# Biases (bs)	# Total parameters	
Input layer	-	-	-	
1 st Convolution layer	2400	32	2432	
1 st ReLU layer	-	-	-	
1 st Max-pooling layer	-	-	-	
2 nd Convolution layer	12800	16	12816	
2 nd ReLU layer	-	-	-	
2 nd Max-pooling layer	-	-	-	
3 rd Convolution layer	6400	16	6416	
3 rd ReLU layer	-	-	-	
Fully-connected layer	10240	10	10250	
Softmaxloss layer	-	-	-	
Total of all layers	31840	74	31914	

Using the confusion matrix provided in Figure 9 for the improved model, precision and recall are computed for each class and tabulated in Table 3. In addition, F_1 -score is computed for each class. Based on the individual F_1 scores, it seems like the improved model can now classify "Airplanes" much better than other classes. The model has a hard time classifying "deer" and "truck" images. To improve the model further, a lower learning rate, optimally larger batch size, momentum, proper weight decay, and a larger number of iterations could have been used in the improved network. However, due to the computational limitations, an accuracy of 0.601 using the improved model is what was achievable.

Appendix

Results of CIFAR dataset baseline model.

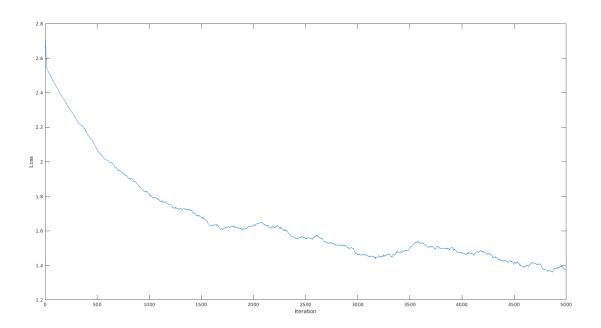


Figure 10: Loss versus number of iterations (CIFAR dataset - baseline model).

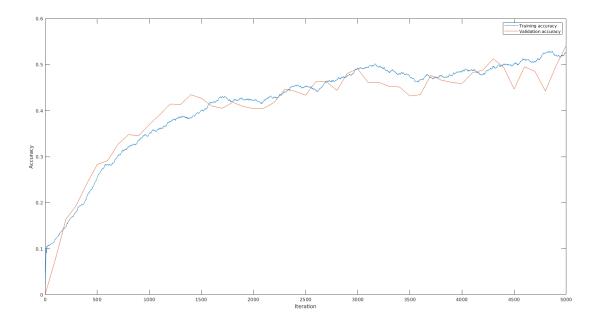


Figure 11: Accuracy versus number of iterations (CIFAR dataset - baseline model).

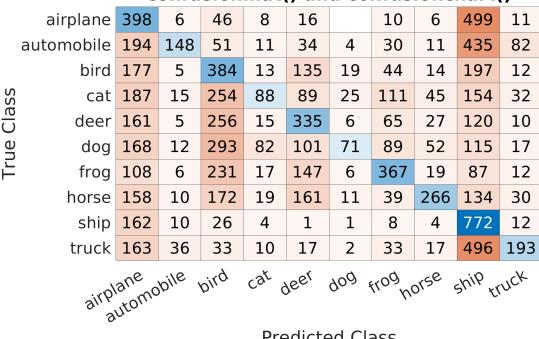


Figure 12: Wrongly predicted cifar images (baseline model).

Correctly classified images PC:airplane, TC:airplane PC:frog, TC:frog PC:horse, TC:horse PC:truck, TC:truck PC:frog, TC:frog PC:airplane, TC:airplane PC:ship TC:ship PC:ship, TC:ship PC:ship, TC:ship PC:frog, TC:frog PC:bird, TC:bird

Figure 13: Correctly predicted cifar images (baseline model).

Confusion matrix chart using Matlab's confusionmat() and confusionchart()



Predicted Class

Figure 14: CIFAR dataset confusion matrix chart (baseline model).