HOMEWORK 5: NEURAL NETWORKS

10-301/10-601 Introduction to Machine Learning (Spring 2022)
https://www.cs.cmu.edu/~mgormley/courses/10601/
OUT: 2022-02-27
DUE: 2022-03-18
TAs: Abbey, Abhi, Alex, Neural, Shelly, Udai

Summary In this assignment, you will build an image recognition system using a neural network. In the Written component, you will walk through an on-paper example of how to implement a neural network. Then, in the Programming component, you will implement an end-to-end system that learns to perform image classification.

START HERE: Instructions

- **Collaboration Policy**: Please read the collaboration policy here: http://www.cs.cmu.edu/~mgormley/courses/10601/syllabus.html
- **Late Submission Policy:** See the late submission policy here: http://www.cs.cmu.edu/~mgormley/courses/10601/syllabus.html
- **Submitting your work:** You will use Gradescope to submit answers to all questions and code. Please follow instructions at the end of this PDF to correctly submit all your code to Gradescope.
  - **Written:** For written problems such as short answer, multiple choice, derivations, proofs, or plots, please use the provided template. Submissions can be handwritten onto the template, but should be labeled and clearly legible. If your writing is not legible, you will not be awarded marks. Alternatively, submissions can be written in LaTeX. Each derivation/proof should be completed in the boxes provided. You are responsible for ensuring that your submission contains exactly the same number of pages and the same alignment as our PDF template. If you do not follow the template, your assignment may not be graded correctly by our AI assisted grader.
  - **Programming:** You will submit your code for programming questions on the homework to Gradescope (https://gradescope.com). After uploading your code, our grading scripts will autograde your assignment by running your program on a virtual machine (VM). When you are developing, check that the version number of the programming language environment (e.g. Python 3.9.6) and versions of permitted libraries (e.g. `numpy` 1.21.2 and `scipy` 1.7.1) match those used on Gradescope. You have 10 free Gradescope programming submissions. After 10 submissions, you will begin to lose points from your total programming score. We recommend debugging your implementation on your local machine (or the Linux servers) and making sure your code is running correctly first before submitting your code to Gradescope.
- **Materials:** The data that you will need in order to complete this assignment is posted along with the writeup and template on the course website.

Instructions for Specific Problem Types

For “Select One” questions, please fill in the appropriate bubble completely:

Select One: Who taught this course?

- ● Matt Gormley
- ○ Marie Curie
- ○ Noam Chomsky

If you need to change your answer, you may cross out the previous answer and bubble in the new answer:

Select One: Who taught this course?

- ● Matt Gormley
- ○ Marie Curie
- ~~●~~ Noam Chomsky

For “Select all that apply” questions, please fill in all appropriate squares completely:

Select all that apply: Which are scientists?

- ■ Stephen Hawking
- ■ Albert Einstein
- ■ Isaac Newton
- □ I don’t know

Again, if you need to change your answer, you may cross out the previous answer(s) and bubble in the new answer(s):

Select all that apply: Which are scientists?

- ■ Stephen Hawking
- ■ Albert Einstein
- ■ Isaac Newton
- ~~■~~ I don’t know

For questions where you must fill in a blank, please make sure your final answer is fully included in the given space. You may cross out answers or parts of answers, but the final answer must still be within the given space.

Fill in the blank: What is the course number?

$\boxed{10\text{-}601}$ $\boxed{10\text{-}\cancel{6}301}$

Written Questions (47 points)

1 Example Feed Forward and Backpropagation (29 points)

$$\begin{tikzcd}
\boxed{\mathbf{x}} \arrow[r] & \boxed{\mathbf{a} = Linear(\boldsymbol{\alpha}^*, \boldsymbol{\alpha}_b, \mathbf{x})} \arrow[r] & \boxed{\mathbf{z} = Sigmoid(\mathbf{a})} \arrow[r] & \boxed{\mathbf{b} = Linear(\boldsymbol{\beta}^*, \boldsymbol{\beta}_b, \mathbf{z})} \arrow[r] & \boxed{\hat{\mathbf{y}} = Softmax(\mathbf{b})} \arrow[r] & \boxed{l(\hat{\mathbf{y}}, \mathbf{y}) = CELoss(\hat{\mathbf{y}}, \mathbf{y})} \\
& \boxed{\boldsymbol{\alpha}^*} \arrow[u] & \boxed{\boldsymbol{\alpha}_b} \arrow[ul] & \boxed{\boldsymbol{\beta}^*} \arrow[u] & \boxed{\boldsymbol{\beta}_b} \arrow[ul] & \boxed{\mathbf{y}} \arrow[u]
\end{tikzcd}$$

Figure 1: Computational Graph for a One Hidden Layer Neural Network

Network Overview Consider the neural network with one hidden layer shown in Figure 1. The input layer consists of 6 features $\mathbf{x} = [x_1, ..., x_6]^T$, the hidden layer has 4 nodes $\mathbf{z} = [z_1, ..., z_4]^T$, and the output layer is a probability distribution $\mathbf{y} = [y_1, y_2, y_3]^T$ over 3 classes (**1-indexed** such that y_i is the probability of label i).

$\boldsymbol{\alpha}^*$ is the matrix of weights from the inputs to the hidden layer and $\boldsymbol{\beta}^*$ is the matrix of weights from the hidden layer to the output layer.

$\alpha^*_{j,i}$ represents the weight going *to* the node z_j in the hidden layer *from* the node x_i in the input layer (e.g. $\alpha^*_{1,2}$ is the weight from x_2 to z_1), and $\boldsymbol{\beta}^*$ is defined similarly. We will use a sigmoid activation function for the hidden layer and a softmax for the output layer.

The bias vectors $\boldsymbol{\alpha}_b, \boldsymbol{\beta}_b$ are defined such that the jth value of $\boldsymbol{\alpha}_b$ (which we denote $\alpha_{j,b}$) is the bias value for a_j and the kth value of $\boldsymbol{\beta}_b$ is the bias value for b_k.

Network Details Equivalently, we define each of the following.

The input:

$$\mathbf{x} = [x_1, x_2, x_3, x_4, x_5, x_6]^T \tag{1}$$

Linear combination at the first (hidden) layer:

$$a_j = \alpha_{j,b} + \sum_{i=1}^{6} \alpha^*_{j,i} \cdot x_i, \ \forall j \in \{1, \ldots, 4\} \tag{2}$$

Activation at the first (hidden) layer:

$$z_j = \sigma(a_j) = \frac{1}{1 + \exp(-a_j)}, \ \forall j \in \{1, \ldots, 4\} \tag{3}$$

Equivalently, we can write this as vector operation where the sigmoid activation is applied individually to each element of the vector $\mathbf{a}$:

$$\mathbf{z} = \sigma(\mathbf{a}) \tag{4}$$

Linear combination at the second (output) layer:

$$b_k = \beta_{k,b} + \sum_{j=1}^{4} \beta^*_{k,j} \cdot z_j, \ \forall k \in \{1, \ldots, 3\} \tag{5}$$

Activation at the second (output) layer:

$$\hat{y}_k = \frac{\exp(b_k)}{\sum_{l=1}^{3} \exp(b_l)}, \ \forall k \in \{1, \ldots, 3\} \tag{6}$$

Loss We will use cross entropy loss, $\ell(\hat{\mathbf{y}}, \mathbf{y})$. If $\mathbf{y}$ represents our target output, which will be a one-hot vector representing the correct class, and $\hat{\mathbf{y}}$ represents the output of the network, the loss is calculated by:

$$\ell(\hat{\mathbf{y}}, \mathbf{y}) = -\sum_{i=1}^{3} y_i \log(\hat{y}_i) \tag{7}$$

For the below questions use natural log in the equation.

Prediction When doing prediction, we will predict the argmax of the output layer. For example, if $\hat{y}_1 = 0.3, \hat{y}_2 = 0.2, \hat{y}_3 = 0.5$ we would predict class 3. If the true class from the training data was 2 we would have a one-hot vector $\mathbf{y}$ with values $y_1 = 0$, $y_2 = 1$, $y_3 = 0$.

1. In the following questions you will derive the matrix and vector forms of the previous equations which define our neural network. These are what you should hope to program in order to keep your program under the Gradescope time-out.
   When working these out it is important to keep a note of the vector and matrix dimensions in order for you to easily identify what is and isn't a valid multiplication. Suppose you are given an training example: $\mathbf{x}^{(1)} = [x_1, x_2, x_3, x_4, x_5, x_6]^T$ with **label class 2**, so $\mathbf{y}^{(1)} = [0, 1, 0]^T$. We initialize the network weights as:

$$\boldsymbol{\alpha}^* = \begin{bmatrix} \alpha_{1,1} & \alpha_{1,2} & \alpha_{1,3} & \alpha_{1,4} & \alpha_{1,5} & \alpha_{1,6} \\ \alpha_{2,1} & \alpha_{2,2} & \alpha_{2,3} & \alpha_{2,4} & \alpha_{2,5} & \alpha_{2,6} \\ \alpha_{3,1} & \alpha_{3,2} & \alpha_{3,3} & \alpha_{3,4} & \alpha_{3,5} & \alpha_{3,6} \\ \alpha_{4,1} & \alpha_{4,2} & \alpha_{4,3} & \alpha_{4,4} & \alpha_{4,5} & \alpha_{4,6} \end{bmatrix}$$

$$\boldsymbol{\beta}^* = \begin{bmatrix} \beta_{1,1} & \beta_{1,2} & \beta_{1,3} & \beta_{1,4} \\ \beta_{2,1} & \beta_{2,2} & \beta_{2,3} & \beta_{2,4} \\ \beta_{3,1} & \beta_{3,2} & \beta_{3,3} & \beta_{3,4} \end{bmatrix}$$

We want to also consider the bias term and the weights on the bias terms ($\alpha_{j,b}$ and $\beta_{k,b}$). To account for these we can add them as a new column to the beginning of our initial weight matrices to represent biases, (e.g. $\alpha_{1,0} = \alpha_{1,b}$).

$$\boldsymbol{\alpha} = \begin{bmatrix} \alpha_{1,0} & \alpha_{1,1} & \alpha_{1,2} & \alpha_{1,3} & \alpha_{1,4} & \alpha_{1,5} & \alpha_{1,6} \\ \alpha_{2,0} & \alpha_{2,1} & \alpha_{2,2} & \alpha_{2,3} & \alpha_{2,4} & \alpha_{2,5} & \alpha_{2,6} \\ \alpha_{3,0} & \alpha_{3,1} & \alpha_{3,2} & \alpha_{3,3} & \alpha_{3,4} & \alpha_{3,5} & \alpha_{3,6} \\ \alpha_{4,0} & \alpha_{4,1} & \alpha_{4,2} & \alpha_{4,0} & \alpha_{4,4} & \alpha_{4,5} & \alpha_{4,6} \end{bmatrix}$$

$$\boldsymbol{\beta} = \begin{bmatrix} \beta_{1,0} & \beta_{1,1} & \beta_{1,2} & \beta_{1,3} & \beta_{1,4} \\ \beta_{2,0} & \beta_{2,1} & \beta_{2,2} & \beta_{2,3} & \beta_{2,4} \\ \beta_{3,0} & \beta_{3,1} & \beta_{3,2} & \beta_{3,3} & \beta_{3,4} \end{bmatrix}$$

We then add a corresponding new first dimension to our input vectors, always set to 1 ($x_0^{(i)} = 1$), so our input becomes:

$$\mathbf{x}^{(1)} = [1, x_1, x_2, x_3, x_4, x_5, x_6]^T$$

(a) (1 point) By examining the shapes of the initial weight matrices, how many neurons do we have in the first hidden layer of the neural network? Do not include the bias in your count.

Answer

(b) (1 point) How many output neurons will our neural network have?

Answer

(c) (1 point) What is the vector $\mathbf{a}$ whose elements are made up of the entries a_j in Equation 2 (using $x_i^{(1)}$ in place of x_i). Write your answer in terms of $\boldsymbol{\alpha}$ and $\mathbf{x}^{(1)}$.

Answer

(d) (1 point) **Select all that apply:** We cannot take the matrix multiplication of our weights $\boldsymbol{\beta}$ and the vector $\mathbf{z} = [z_1, z_2, z_3, z_4]^T$ since they are not compatible shapes. Which of the following would allow us to take the matrix multiplication of $\boldsymbol{\beta}$ and $\mathbf{z}$ such that the entries of the vector $\mathbf{b} = \boldsymbol{\beta}\mathbf{z}$ are equivalent to the values of b_k in Equation 5?

- ☐ A) Remove the last column of $\boldsymbol{\beta}$
- ☐ B) Remove the first row of $\mathbf{z}$
- ☐ C) Append a value of 1 to be the first entry of $\mathbf{z}$.
- ☐ D) Append an additional column of 1's to be the first column of $\boldsymbol{\beta}$
- ☐ E) Append a row of 1's to be the first row of $\boldsymbol{\beta}$
- ☐ F) Take the transpose of $\boldsymbol{\beta}$

(e) (1 point) What are the entries of the output vector $\hat{\mathbf{y}}$? Your answer should be written in terms of b_1, b_2, b_3.

$\hat{\mathbf{y}}$

2. We will now derive the matrix and vector forms for the backpropagation algorithm, for example

$$\frac{\partial \ell}{\partial \boldsymbol{\alpha}} = \begin{bmatrix} \frac{\partial \ell}{\partial \alpha_{10}} & \frac{\partial \ell}{\partial \alpha_{11}} & \cdots & \frac{\partial \ell}{\partial \alpha_{16}} \\ \frac{\partial \ell}{\partial \alpha_{20}} & \frac{\partial \ell}{\partial \alpha_{21}} & \cdots & \frac{\partial \ell}{\partial \alpha_{26}} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{\partial \ell}{\partial \alpha_{40}} & \frac{\partial \ell}{\partial \alpha_{41}} & \cdots & \frac{\partial \ell}{\partial \alpha_{46}} \end{bmatrix}$$

The mathematics which you have to derive in this section jump significantly in difficulty, you should always be examining the shape of the matrices and vectors and making sure that you are comparing your matrix elements with calculations of individual derivatives to make sure they match (e.g., the element of the matrix $(\frac{\partial \ell}{\partial \boldsymbol{\alpha}})_{2,1}$ should be equal to $\frac{\partial \ell}{\partial \alpha_{2,1}}$). Recall that ℓ is our loss function defined in Equation 7:

Note: all vectors are column vectors (i.e. an n dimensional vector $v \in \mathbb{R}^{n \times 1}$). **Assume that all input vectors to linear layers have a bias term folded in, unless otherwise specified**. All partial derivatives should be written in denominator layout notation. An example of denominator notation is that $\frac{\partial \ell}{\partial \beta} \in \mathbb{R}^{3 \times 5}$ because $\beta \in \mathbb{R}^{3 \times 5}$.

(a) (1 point) What is the derivative $\frac{\partial \ell}{\partial \hat{y}_i}$, where $1 \leq i \leq 3$? Your answer should be in terms of y_i and $\hat{y}_i$. Recall that we define the loss $\ell(\hat{y}, y)$ as follows (*note: log is a natural log*):

$$\ell(\hat{\mathbf{y}}, \mathbf{y}) = -\sum_{i=1}^{3} y_i \log(\hat{y}_i) \tag{7}$$

$\partial \ell / \partial \hat{y}_i$

(b) (1 point) Suppose we have $\hat{y} = [0.2, 0.7, 0.1]^T$ and $y = [0, 1, 0]^T$. Compute the value of $\frac{\partial \ell}{\partial b_2}$. Use your answer from part (a), as well as the fact that the derivative of the softmax function with respect to b_k is as follows:

$$\frac{\partial \hat{y}_l}{\partial b_k} = \hat{y}_l(\mathbb{I}[k = l] - \hat{y}_k) \tag{8}$$

where $\mathbb{I}[k = l]$ is an indicator function such that if $k = l$ then it returns value 1 and 0 otherwise. Show your work below.

HINT: Recall that $\frac{\partial \ell}{\partial b_k} = \sum_l \frac{\partial \ell}{\partial \hat{y}_l} \frac{\partial \hat{y}_l}{\partial b_k}$.

$\partial\ell/\partial b_2$

(c) (3 points) Now, write the derivative $\frac{\partial \ell}{\partial b_k}$ in a smart way such that you do not need the indicator function in Equation 8. Write your solutions in terms of $\hat{y}_k, y_k$. Show your work below.

$\partial\ell/\partial b_k$

(d) (1 point) What are the elements of the vector $\frac{\partial \ell}{\partial \mathbf{b}}$? (Recall that $\mathbf{y}^{(1)} = [0, 1, 0]^T$)

$\partial \ell / \partial \mathbf{b}$

(e) (2 points) What is the derivative $\frac{\partial \ell}{\partial \boldsymbol{\beta}}$? Your answer should be in terms of $\frac{\partial \ell}{\partial \mathbf{b}}$ and $\mathbf{z}$.

You should first consider a single entry in this matrix: $\frac{\partial \ell}{\partial \beta_{kj}}$.

$\partial \ell / \partial \boldsymbol{\beta}$

(f) (1 point) Explain in one short sentence why we use the matrix $\boldsymbol{\beta}^*$ (the matrix $\boldsymbol{\beta}$ without the first column of ones) when calculating the derivative matrix $\frac{\partial \ell}{\partial \alpha}$?

Answer

(g) (1 point) What is the derivative $\frac{\partial \ell}{\partial \mathbf{z}}$ (**not including the bias term**)? Your answer should be in terms of $\frac{\partial \ell}{\partial \mathbf{b}}$ and $\boldsymbol{\beta}^*$.

$\partial \ell / \partial \mathbf{z}$

(h) (1 point) What is the derivative $\frac{\partial \ell}{\partial a_j}$ in terms of $\frac{\partial \ell}{\partial z_j}$ and z_j?

$\partial \ell / \partial a_j$

(i) (1 point) What is the matrix $\frac{\partial \ell}{\partial \boldsymbol{\alpha}}$? Your answer should be in terms of $\frac{\partial \ell}{\partial \mathbf{a}}$ and $\mathbf{x}^{(1)}$.

$\partial \ell / \partial \boldsymbol{\alpha}$

3. Now you will put these equations to use in an example with numerical values. **You should use the answers you get here to debug your code.**
You are given a training example $\mathbf{x}^{(1)} = [1, 0, 1, 1, 0, 1]^T$ with **label class 2**, so $\mathbf{y}^{(1)} = [0, 1, 0]^T$. We initialize the network weights as:

$$\boldsymbol{\alpha}^* = \begin{bmatrix} 1 & 2 & 0 & -1 & 3 & 2 \\ 2 & 3 & 1 & 0 & 1 & 1 \\ 1 & 3 & 1 & 2 & -1 & 2 \\ 0 & 1 & 2 & 0 & 0 & 3 \end{bmatrix}$$

$$\boldsymbol{\beta}^* = \begin{bmatrix} 1 & 2 & 0 & 1 \\ 1 & -1 & 3 & 2 \\ 3 & 0 & -1 & 1 \end{bmatrix}$$

We want to also consider the bias term and the weights on the bias terms ($\alpha_{j,b}$ and $\beta_{j,b}$). Lets say they are all initialized to 1. To account for this we can add a column of 1's to the beginning of our initial weight matrices.

$$\boldsymbol{\alpha} = \begin{bmatrix} 1 & 1 & 2 & 0 & -1 & 3 & 2 \\ 1 & 2 & 3 & 1 & 0 & 1 & 1 \\ 1 & 1 & 3 & 1 & 2 & -1 & 2 \\ 1 & 0 & 1 & 2 & 0 & 0 & 3 \end{bmatrix}$$

$$\boldsymbol{\beta} = \begin{bmatrix} 1 & 1 & 2 & 0 & 1 \\ 1 & 1 & -1 & 3 & 2 \\ 1 & 3 & 0 & -1 & 1 \end{bmatrix}$$

And we can set our first value of our input vectors to always be 1 ($x_0^{(i)} = 1$), so our input becomes:

$$\mathbf{x}^{(1)} = [1, 1, 0, 1, 1, 0, 1]^T$$

Using the initial weights, run the feed forward of the network over this example (rounding to 4 decimal places during the calculation) and then answer the following questions.

(a) (1 point) What is a_1?

a_1

Work

(b) (1 point) What is z_1?

z_1

Work

(c) (1 point) What is b_2? We have computed z_2 = 0.9933, z_3 = 0.9991, z_4 = 0.9975 for you.

b_2

Work

(d) (1 point) What is $\hat{y}_2$? We have computed $b_1 = 4.9367, b_3 = 3.8562$ for you.

$\hat{y}_2$	Work

(e) (1 point) Which class would we predict on this example? Your answer should just be an integer $\in \{1, 2, 3\}$.

Class	Work

(f) (1 point) What is the total loss on this example?

Loss	Work

4. Now use the results of the previous question to run backpropagation over the network and update the weights with **Stochastic Gradient Descent**. Use learning rate $\eta = 1$.

   Do your backpropagation calculations rounding to 4 decimal places then answer the following questions:

   (a) (1 point) What is the value of $\frac{\partial \ell}{\partial \beta_{1,0}}$?

$\partial \ell / \partial \beta_{1,0}$	Work

   (b) (1 point) What is the updated value of the weight $\beta_{1,0}$?

$\beta_{1,0}$	Work

   (c) (1 point) What is the value of $\frac{\partial \ell}{\partial \alpha_{3,2}}$?

$\partial \ell / \partial \alpha_{3,2}$	Work

(d) (1 point) What is the updated value of the weight $\alpha_{3,2}$?

$\alpha_{3,2}$

Work

(e) (2 points) What is the updated weight of the input layer bias term applied to z_2 (i.e. $\alpha_{2,0}$)?

$\alpha_{2,0}$

Work

2 Empirical Questions (18 points)

The following questions should be completed after you work through the programming portion of this assignment. **For any plotting questions, you must title your graph, label your axes and provide units, and provide a legend in order to receive full credit.**

For these questions, **use the small dataset**. Use the following values for the hyperparameters unless otherwise specified:

Parameter	**Value**
Number of Hidden Units	50
Weight Initialization	RANDOM
Learning Rate	0.01

Please submit computer-generated plots for all parts. To get full credit, your plots must have a label for both axes with the value plotted on that axis, provide a legend labeling every line, and have a title.

1. Hidden Units

   (a) (2 points) Train a single hidden layer neural network using the hyperparameters mentioned in the table above, except for the number of hidden units which should vary among 5, 20, 50, 100, and 200. Run the optimization for 100 epochs each time.

   Plot the average training cross-entropy (sum of the cross-entropy terms over the training dataset divided by the total number of training examples) on the y-axis vs number of hidden units on the x-axis. In the **same figure**, plot the average validation cross-entropy.

Avg. Train and Validation Cross-Entropy Loss

(b) (2 points) Examine and comment on the the plots of training and validation cross-entropy. What problem arises with too few hidden units, and why does it happen?

Answer

(c) (2 points) In the handout folder, we provide `metrics_sgd_small.txt`, a text file with the validation cross-entropy loss values for SGD performed using 100 epochs, 50 hidden units, random init, and 0.01 learning rate. In the **same figure**, plot them against your validation results for SGD **with** Adagrad using the same set of parameters and the small dataset.

Avg. Validation Cross-Entropy Loss of SGD with and without AdaGrad

(d) (2 points) Examine and compare the two results. What do you observe?

Answer

2. Learning Rate

   (a) (6 points) Train a single hidden layer neural network using the hyperparameters mentioned in the table above, except for the learning rate which should vary among 0.1, 0.01, and 0.001. Run the optimization for 100 epochs each time.

   Plot the average training cross-entropy on the y-axis vs the number of epochs on the x-axis for the mentioned learning rates. In the **same figure**, plot the average validation cross-entropy loss. Make a separate figure for each learning rate.

Plot LR 0.1

Plot LR 0.01

Plot LR 0.001

(b) (2 points) Examine and comment on the plots of training and validation cross-entropy. Are there any learning rates for which convergence is not achieved? Are there any learning rates that exhibit other problems? If so, describe these issues and list the learning rates that cause them.

Answer

3. Weight Initialization

(a) (2 points) For this exercise, you can work on any data set. Initialize $\boldsymbol{\alpha}$ and $\boldsymbol{\beta}$ to zero and print them out after the first few updates. For example, you may use the following command to begin:

```
$ python neuralnet.py small_train.csv small_validation.csv \
small_train_out.labels small_validation_out.labels \
small_metrics_out.txt 1 4 2 0.1
```

Compare the values across rows and columns in $\boldsymbol{\alpha}$ and $\boldsymbol{\beta}$. Describe the observed behavior and how this may affect model capacity and convergence.

Answer

Programming (94 points)

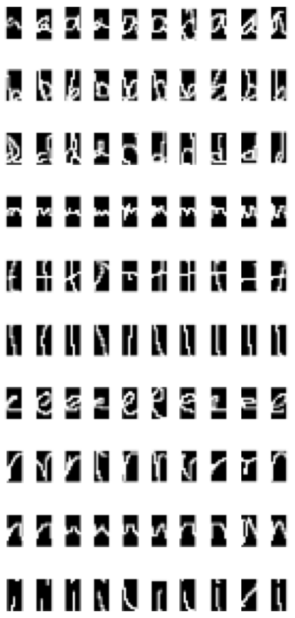
Figure 2: 10 random images of each of the 10 letters in the OCR dataset.

3 The Task

Your goal in this assignment is to implement a neural network to classify images using a single hidden layer neural network. In addition, you will implement Adagrad, a variant of stochastic gradient descent.

4 The Datasets

Datasets We will be using a subset of an Optical Character Recognition (OCR) dataset. This data includes images of all 26 handwritten letters; our subset will include only the letters "a," "e," "g," "i," "l," "n," "o," "r," "t," and "u." The handout a small dataset with 60 samples *per class* (50 for training and 10 for validation). We will also evaluate your code on a medium dataset with 600 samples per class (500 for training and 100 for validation). Figure 2 shows a random sample of 10 images of few letters from the dataset.

File Format Each dataset (small, medium, and large) consists of two csv files—train and validation. Each row contains 129 columns separated by commas. The first column contains the label and columns 2 to 129 represent the pixel values of a 16×8 image in a row major format. Label 0 corresponds to "a," 1 to "e," 2 to "g," 3 to "i," 4 to "l," 5 to "n," 6 to "o," 7 to "r," 8 to "t," and 9 to "u."

Because the original images are black-and-white (not grayscale), the pixel values are either 0 or 1. However, you should write your code to accept arbitrary pixel values in the range [0, 1]. The images in Figure 2 were produced by converting these pixel values into .png files for visualization. Observe that no feature engineering has been done here; instead the neural network you build will *learn* features appropriate for the task of character recognition.

5 Model Definition

In this assignment, you will implement a single-hidden-layer neural network with a sigmoid activation function for the hidden layer, and a softmax on the output layer. Let the input vectors $\mathbf{x}$ be of length M, and the hidden layer $\mathbf{z}$ consist of D hidden units. In addition, let the output layer $\hat{\mathbf{y}}$ be a probability distribution over K classes. That is, each element $\hat{y}_k$ of the output vector represents the probability of $\mathbf{x}$ belonging to the class k.

We can compactly express this model by assuming that $x_0 = 1$ is a bias feature on the input and that $z_0 = 1$ is also fixed. In this way, we have two parameter matrices $\boldsymbol{\alpha} \in \mathbb{R}^{D\times(M+1)}$ and $\boldsymbol{\beta} \in \mathbb{R}^{K\times(D+1)}$. The extra 0th column of each matrix (i.e. $\boldsymbol{\alpha}_{\cdot,0}$ and $\boldsymbol{\beta}_{\cdot,0}$) hold the bias parameters.

$$
\begin{aligned}
a_j &= \sum_{m=0}^{M} \alpha_{j,m} x_m \\
z_j &= \frac{1}{1+\exp(-a_j)} \\
b_k &= \sum_{j=0}^{D} \beta_{k,j} z_j \\
\hat{y}_k &= \frac{\exp(b_k)}{\sum_{l=1}^{K} \exp(b_l)}
\end{aligned}
$$

The objective function we will use for training the neural network is the average cross entropy over the training dataset $\mathcal{D} = \{(\mathbf{x}^{(i)}, \mathbf{y}^{(i)})\}$:

$$
J(\boldsymbol{\alpha}, \boldsymbol{\beta}) = -\frac{1}{N} \sum_{i=1}^{N} \sum_{k=1}^{K} y_k^{(i)} \log(\hat{y}_k^{(i)}) \tag{9}
$$

In Equation 9, J is a function of the model parameters $\boldsymbol{\alpha}$ and $\boldsymbol{\beta}$ because $\hat{y}_k^{(i)}$ is implicitly a function of $\mathbf{x}^{(i)}$, $\boldsymbol{\alpha}$, and $\boldsymbol{\beta}$ since it is the output of the neural network applied to $\mathbf{x}^{(i)}$. $\hat{y}_k^{(i)}$ and $y_k^{(i)}$ are the kth components of $\hat{\mathbf{y}}^{(i)}$ and $\mathbf{y}^{(i)}$ respectively.

To train, you should optimize this objective function using stochastic gradient descent (SGD), where the gradient of the parameters for each training example is computed via backpropagation. You should shuffle the training points when performing SGD using the provided `shuffle` function, passing in the epoch number as a random seed. Note that SGD has a slight impact on the objective function, where we are "summing" over the current point, i:

$$
J_{SGD}(\boldsymbol{\alpha}, \boldsymbol{\beta}) = -\sum_{k=1}^{K} y_k^{(i)} \log(\hat{y}_k^{(i)}) \tag{10}
$$

Lastly, let's take a look at the Adagrad update that you will be performing. For each parameter θ_t^i at round t, you will first compute an intermediate value $\mathbf{s}_t^i$, and then use this to compute the updated θ_{t+1}^i. $\mathbf{s}_t^i$ will contain the element-wise sums (denoted by $\odot$) of all the element-wise squared gradients. Therefore, $\mathbf{s}_t$ should have the same shape as $\frac{\partial J(\boldsymbol{\theta}_t)}{\partial \boldsymbol{\theta}_t^i}$. $\mathbf{s}_t$ should be initialized once, before the first epoch, to a zero vector. The update equations for $\mathbf{s}$ and θ are below.

$$\mathbf{s}_{t+1}^i = \mathbf{s}_t^i + \frac{\partial J(\boldsymbol{\theta}_t)}{\partial \boldsymbol{\theta}_t^i} \odot \frac{\partial J(\boldsymbol{\theta}_t)}{\partial \boldsymbol{\theta}_t^i}. \tag{11}$$

Then, we use $\mathbf{s}_t$ to scale the gradient for the update:

$$\boldsymbol{\theta}_{t+1}^i = \boldsymbol{\theta}_t^i - \frac{\eta}{\sqrt{\mathbf{s}_{t+1}^i + \epsilon}} \odot \frac{\partial J(\boldsymbol{\theta}_t)}{\partial \boldsymbol{\theta}_t^i}. \tag{12}$$

Here, η is the learning rate, and $\epsilon =$ `1e-5`.

5.1 Initialization

In order to use a deep network, we must first initialize the weights and biases in the network. This is typically done with a random initialization, or initializing the weights from some other training procedure. For this assignment, we will be using two possible initialization:

RANDOM The weights are initialized randomly from a uniform distribution from -0.1 to 0.1. The bias parameters are initialized to zero.

ZERO All weights are initialized to 0.

You must support both of these initialization schemes.

6 Implementation

Write a program `neuralnet.py` that implements an optical character recognizer using a one hidden layer neural network with sigmoid activations. Your program should learn the parameters of the model on the training data, report the cross-entropy at the end of each epoch on both train and validation data, and at the end of training write out its predictions and error rates on both datasets.

Your implementation must satisfy the following requirements:

- Use a **sigmoid** activation function on the hidden layer and **softmax** on the output layer to ensure it forms a proper probability distribution.
- Number of **hidden units** for the hidden layer should be determined by a command line flag.
- Support two different **initialization strategies**, as described in Section 5.1, selecting between them via a command line flag.
- Use stochastic gradient descent (SGD) to optimize the parameters for one hidden layer neural network. The number of **epochs** will be specified as a command line flag.
- Set the **learning rate** via a command line flag.
- Perform stochastic gradient descent updates on the training data on the data shuffled with the provided function. For each epoch, you must reshuffle the **original** file data, not the data from the previous epoch.
- In case there is a tie in the output layer $\hat{\mathbf{y}}$, predict the smallest index to be the label.
- You may assume that the input data will always have the same output label space (i.e. $\{0, 1, \ldots, 9\}$). Other than this, do not hard-code any aspect of the datasets into your code. We will autograde your programs on multiple data sets that include different examples.

- Do *not* use any machine learning libraries. You may use NumPy.

Implementing a neural network can be tricky: the parameters are not just a simple vector, but a collection of many parameters; computational efficiency of the model itself becomes essential; the initialization strategy dramatically impacts overall learning quality; other aspects which we will *not* change (e.g. activation function, optimization method) also have a large effect. These *tips* should help you along the way:

- Try to "vectorize" your code as much as possible—this is particularly important for Python. For example, in Python, you want to avoid for-loops and instead rely on `numpy` calls to perform operations such as matrix multiplication, transpose, subtraction, etc. over an entire `numpy` array at once. Why? Because these operations are actually implemented in fast C code, which won't get bogged down the way a high-level scripting language like Python will.
- Implement a finite difference test to check whether your implementation of backpropagation is correctly computing gradients. If you choose to do this, comment out this functionality once your backward pass starts giving correct results and before submitting to Gradescope—since it will otherwise slow down your code.

6.1 Command Line Arguments

The autograder runs and evaluates the output from the files generated, using the following command:

```
$ python3 neuralnet.py [args...]
```

Where above `[args...]` is a placeholder for nine command-line arguments: `<train_input> validation_input> <train_out> <validation_out> <metrics_out> <num_epoch> <hidden_units> <init_flag> <learning_rate>`. These arguments are described in detail below:

1. `<train_input>`: path to the training input `.csv` file (see Section 4)
2. `<validation_input>`: path to the validation input `.csv` file (see Section 4)
3. `<train_out>`: path to output `.labels` file to which the prediction on the *training* data should be written (see Section 6.2)
4. `<validation_out>`: path to output `.labels` file to which the prediction on the *validation* data should be written (see Section 6.2)
5. `<metrics_out>`: path of the output `.txt` file to which metrics such as train and validation error should be written (see Section 6.4)
6. `<num_epoch>`: integer specifying the number of times backpropogation loops through all of the training data (e.g., if `<num_epoch>` equals 5, then each training example will be used in backpropogation 5 times).
7. `<hidden_units>`: positive integer specifying the number of hidden units.
8. `<init_flag>`: integer taking value 1 or 2 that specifies whether to use RANDOM or ZERO initialization (see Section 5.1 and Section 5)—that is, if `init_flag`==1 initialize your weights randomly from a uniform distribution over the range [-0.1, 0.1] (i.e. RANDOM), if `init_flag`==2 initialize all weights to zero (i.e. ZERO). For both settings, **always initialize bias terms to zero**.
9. `<learning_rate>`: float value specifying the base learning rate for SGD with Adagrad.
10. `<--debug>`: (optional argument) set the logging level, set to DEBUG to show logging

As an example, if you implemented your program in Python, the following command line would run your program with 4 hidden units on the small data provided in the handout for 2 epochs using zero initialization and a learning rate of 0.1.

```
python neuralnet.py small_train.csv small_validation.csv \
small_train_out.labels small_validation_out.labels \
small_metrics_out.txt 2 4 2 0.1
```

6.2 Output: Labels Files

Your program should write two output `.labels` files containing the predictions of your model on training data (`<train_out>`) and validation data (`<validation_out>`). Each should contain the predicted labels for each example printed on a new line. Use `\n` to create a new line.

Your labels should exactly match those of a reference implementation – this will be checked by the autograder by running your program and evaluating your output file against the reference solution.

Note: You should output your predicted labels using the same *integer* identifiers as the original training data. You should also insert an empty line (again using '\n') at the end of each sequence (as is done in the input data files).

6.3 Debug Output: Logging

Note that we use the debug logging level in the starter code. If we use a higher logging level, we will log things with the default logging configuration, causing potential slowdowns when executing on an autograder.

Note also that we log NumPy matrices on separate lines from strings describing them. If we do not do this (e.g., if we call `str` on them and add them to the strings), the arrays will be turned into strings even when our logging is set to ignore debug, causing potential massive slowdowns.

6.4 Output Metrics

Generate a file where you report the following metrics:

cross entropy After each epoch, report mean cross entropy on the training data `crossentropy(train)` and validation data `crossentropy(validation)` (See Equation 9). These two cross-entropy values should be reported at the end of each epoch and prefixed by the epoch number. For example, after the second pass through the training examples, these should be prefixed by `epoch=2`. The total number of train losses you print out should equal `num_epoch`—likewise for the total number of validation losses.

error After the final epoch (i.e. when training has completed fully), report the final training error `error(train)` and validation error `error(validation)`.

A sample output is given below. It contains the train and validation losses for the first 2 epochs and the final error rate when using the command given above.

```
epoch=1 crossentropy(train): 1.9946950280285547
epoch=1 crossentropy(validation): 2.010686378337308
epoch=2 crossentropy(train): 1.912184059993547
epoch=2 crossentropy(validation): 1.944326942790059
error(train): 0.782
error(validation): 0.83
```

Take care that your output has the exact same format as shown above. There is an equal sign = between the word `epoch` and the epoch number, but no spaces. There should be a single space after the epoch number (e.g. a space after `epoch=1`), and a single space after the colon preceding the metric value (e.g. a space after `epoch=1 likelihood(train):`). Each line should be terminated by a Unix line ending `\n`.

6.5 Tiny Data Set

To help you with this assignment, we have also included a tiny data set, `tiny_train.csv` and `tiny_validation.csv`, and a reference output file `tiny_output.txt` for you to use. The tiny dataset is in a format similar to the other datasets, but it only contains two samples with five features. The reference file contains outputs from each layer of one correctly implemented neural network, for both forward and back-propagation steps. We advise you to use this set to help you debug in case your implementation doesn't produce the same results as in the written part.

For your reference, `tiny_output.txt` is generated from the following command line specifications:

```
python neuralnet.py tiny_train.csv tiny_validation.csv \
tiny_train_out.labels tiny_validation_out.labels \
tiny_metrics_out.txt 1 4 2 0.1
```

The specific output file names are not important, but be sure to keep the other arguments exactly as they are shown above.

7 Gradescope Submission

You should submit your `neuralnet.py` to Gradescope. Please do not use any other file name for your implementation. This will cause problems for the autograder to correctly detect and run your code.

8 Pseudocode

Since the network structure we will use in this homework is fairly simple, we define our neural network as a single module. Note that in most deep learning libraries, there is a module corresponding to each layer type (e.g., Linear, Sigmoid, Softmax) to allow for more flexibility. We have provided more information about module-based programming in the additional readings in case you are interested.

NN Module

```
1: procedure FORWARD($\mathbf{x}$)
2:     Forward pass
3: procedure BACKWARD($\mathbf{x}$, $\mathbf{y}$, $\hat{\mathbf{y}}$)
4:     Backward pass
5: procedure TRAIN($\mathbf{x}$, $\mathbf{y}$)
6:     Train the model with SGD
7: procedure TEST($\mathbf{x}$, $\mathbf{y}$)
8:     Test the model and return the loss
```

The NN module defines a forward function $\mathbf{y} = \text{FORWARD}(\mathbf{x})$ and a backward function $\mathbf{g}_\alpha, \mathbf{g}_\beta = \text{BACKWARD}(\mathbf{x}, \mathbf{y}, \hat{\mathbf{y}})$ method. You'll want to pay close attention to the dimensions that you pass into and return from your modules.

8.1 Forward and Backward Methods

After implementing the helper functions (SIGMOID, SOFTMAX, CROSSENTROPY), we can define the methods NNFORWARD and NNBACKWARD as follows.

Algorithm 1 Forward Method

```
1: procedure NNForward(Training example $(\mathbf{x}, \mathbf{y})$)
2:     $\mathbf{a} = \text{Linear}(\mathbf{x}, \boldsymbol{\alpha})$
3:     $\mathbf{z} = \text{Sigmoid}(\mathbf{a})$
4:     $\mathbf{b} = \text{Linear}(\mathbf{z}, \boldsymbol{\beta})$
5:     $\hat{\mathbf{y}} = \text{Softmax}(\mathbf{b})$
6:     return $\hat{\mathbf{y}}$
```

Algorithm 2 Backward Method

```
1: procedure NNBackward(Training example $(\mathbf{x}, \mathbf{y})$, Predicted probabilities $\hat{\mathbf{y}}$)
2:     Place intermediate quantities $\mathbf{x}, \mathbf{a}, \mathbf{z}, \mathbf{b}, \hat{\mathbf{y}}$ in scope        ▷ Hint: make use of class attributes
3:     $\mathbf{g_b} = \text{d\_CrossEntropy}(\mathbf{y}, \hat{\mathbf{y}})$
4:     $\mathbf{g}_{\boldsymbol{\beta}}, \mathbf{g_z} = \text{d\_Linear}(\mathbf{z}, \boldsymbol{\beta}, \mathbf{g_b})$
5:     $\mathbf{g_a} = \text{d\_Sigmoid}(\mathbf{a}, \mathbf{z})\mathbf{g_z}$
6:     $\mathbf{g}_{\boldsymbol{\alpha}}, \mathbf{g_x} = \text{d\_Linear}\ (\mathbf{x}, \boldsymbol{\alpha}, \mathbf{g_a})$        ▷ We discard $\mathbf{g_x}$
7:     return parameter gradients $\mathbf{g}_{\boldsymbol{\alpha}}, \mathbf{g}_{\boldsymbol{\beta}}$
```

8.2 Training Method

Consider the neural network described in Section 5 applied to the ith training example $(\mathbf{x}, \mathbf{y})$ where $\mathbf{y}$ is a one-hot encoding of the true label. Our neural network outputs $\hat{\mathbf{y}} = h_{\boldsymbol{\alpha},\boldsymbol{\beta}}(\mathbf{x})$, where $\boldsymbol{\alpha}$ and $\boldsymbol{\beta}$ are the parameters of the first and second layers respectively and $h_{\boldsymbol{\alpha},\boldsymbol{\beta}}$ is a one-hidden layer neural network with a sigmoid activation and softmax output. The loss function is negative cross-entropy $J = \ell(\hat{\mathbf{y}}, \mathbf{y}) = -\mathbf{y}^T \log(\hat{\mathbf{y}})$. $J = J_{\mathbf{x},\mathbf{y}}(\boldsymbol{\alpha}, \boldsymbol{\beta})$ is actually a function of our training example $(\mathbf{x}, \mathbf{y})$, and our model parameters $\boldsymbol{\alpha}, \boldsymbol{\beta}$ though we write just J for brevity.

In order to train our neural network, we are going to apply stochastic gradient descent. Because we want the behavior of your program to be deterministic for testing on Gradescope, we make a few simplifications: (1) you should *not* shuffle your data and (2) you will use a fixed learning rate. In the real world, you would *not* make these simplifications.

SGD proceeds as follows, where E is the number of epochs and γ is the learning rate.

Algorithm 3 Training with Stochastic Gradient Descent (SGD)

```
1:  procedure SGD(Training data $\mathcal{D}_{train}$, test data $\mathcal{D}_t$)
2:      Initialize parameters $\boldsymbol{\alpha}, \boldsymbol{\beta}$          ▷ Use either RANDOM or ZERO from Section 5.1
3:      for $e \in \{1, 2, \ldots, E\}$ do                                       ▷ For each epoch
4:          $\mathcal{D} = \text{SHUFFLE}(\mathcal{D}_{train}, e)$
5:          for $(\mathbf{x}, \mathbf{y}) \in \mathcal{D}$ do               ▷ For each training example (No shuffling)
6:              Compute neural network layers:
7:              $\mathbf{o} = \text{NNFORWARD}(\mathbf{x}, \mathbf{y}, \boldsymbol{\alpha}, \boldsymbol{\beta})$
8:              Compute gradients via backprop:
9:              $\left.\begin{aligned} \mathbf{g}_{\boldsymbol{\alpha}} &= \frac{\partial J}{\partial \boldsymbol{\alpha}} \\ \mathbf{g}_{\boldsymbol{\beta}} &= \frac{\partial J}{\partial \boldsymbol{\beta}} \end{aligned}\right\} = \text{NNBACKWARD}(\mathbf{x}, \mathbf{y}, \hat{\mathbf{y}})$
10:             Update parameters with Adagrad updates $\mathbf{g}'_{\boldsymbol{\alpha}}, \mathbf{g}'_{\boldsymbol{\beta}}$:      ▷ Refer to Eq.11
11:             $\boldsymbol{\alpha} \leftarrow \boldsymbol{\alpha} - \gamma \mathbf{g}'_{\boldsymbol{\alpha}}$
12:             $\boldsymbol{\beta} \leftarrow \boldsymbol{\beta} - \gamma \mathbf{g}'_{\boldsymbol{\beta}}$
13:         Evaluate training mean cross-entropy $J_{\mathcal{D}}(\boldsymbol{\alpha}, \boldsymbol{\beta})$
14:         Evaluate test mean cross-entropy $J_{\mathcal{D}_t}(\boldsymbol{\alpha}, \boldsymbol{\beta})$
15:     return parameters $\boldsymbol{\alpha}, \boldsymbol{\beta}$
```

8.3 Testing Method

At test time, we output the most likely prediction for each example:

Algorithm 4 Prediction at Test Time

```
1:  procedure PREDICT(Unlabeled train or test dataset $\mathcal{D}'$)
2:      for $\mathbf{x} \in \mathcal{D}'$ do
3:          Compute neural network prediction $\hat{\mathbf{y}} = h(\mathbf{x})$
4:          Predict the label with highest probability $l = \text{argmax}_k \, \hat{y}_k$
```

It's also quite common to combine the Cross-Entropy and Softmax layers into one. The reason for this is the cancelation of numerous terms that result from the zeros in the cross-entropy backward calculation. (Said trick is *not* required to obtain a sufficiently fast implementation for Gradescope.)

Some additional tips: Make sure to read the autograder output carefully. The autograder for Gradescope prints out some additional information about the tests that it ran. For this programming assignment we've specially designed some buggy implementations that you might implement and will try our best to detect those and give you some more useful feedback in Gradescope's autograder. Make wise use of autograder's output for debugging your code.

Note: For this assignment, you may make up to 10 submissions to Gradescope before the deadline, but only your last submission will be graded.

9 Collaboration Questions

After you have completed all other components of this assignment, report your answers to these questions regarding the collaboration policy. Details of the policy can be found here.

1. Did you receive any help whatsoever from anyone in solving this assignment? If so, include full details.
2. Did you give any help whatsoever to anyone in solving this assignment? If so, include full details.
3. Did you find or come across code that implements any part of this assignment? If so, include full details.

Your Answer