705.641.81: Natural Language Processing Self-Supervised Models

Homework 3: Building Your Neural Network!

For homework deadline and collaboration policy, please see our Canvas page.
Name: ______Muhammad Ashar Khan________
Collaborators, if any: ____
Sources used for your homework, if any: ____

This assignment is focusing on understanding the fundamental properties of neural networks and their training.

Homework goals: After completing this homework, you should be comfortable with:

- thinking about neural networks
- key implementation details of NNs, particularly in PyTorch,
- explaining and deriving Backpropagation,
- debugging your neural network in case it faces any failures.

Concepts, intuitions and big picture

1. Suppose you have built a neural network. You decide to initialize the weights and biases to be zero. Which of the following statements are True? (Check all that apply)
   ▫ Each neuron in the first hidden layer will perform the same computation. So even after multiple iterations of gradient descent each neuron will be computing the same thing as other neurons in the same layer.
   ▫ Each neuron in the first hidden layer will perform the same computation in the first iteration. But after one iteration of gradient descent they will learn to compute different things because we have "broken symmetry".
   ▫ Each neuron in the first hidden layer will compute the same thing, but neurons in different layers will compute different things, thus we have accomplished "symmetry breaking" as described in lecture.
   ▫ The first hidden layer's neurons will perform different computations from each other even in the first iteration; their parameters will thus keep evolving in their own way.

2. Vectorization allows you to compute forward propagation in an L-layer neural network without an explicit for-loop (or any other explicit iterative loop) over the layers $l = 1,2,\times, L$. True/False?
   ▫ True
   ▫ False

3. The `tanh` activation usually works better than sigmoid activation function for hidden units because the mean of its output is closer to zero, and so it centers the data better for the next layer. True/False?
   ▫ True
   ▫ False

4. Which of the following techniques does NOT prevent a model from overfitting?
   ▫ Data augmentation ▫ Dropout ▫ Early stopping ▫ None of the above

5. Why should dropout be applied during training? Why should dropout NOT be applied during evaluation?

   a. Dropout should be applied during training to prevent overfitting. This sets the activation of nodes to 0 and therefore teaches the model to find different connections and patterns. Dropout should not be applied during evaluation because we need the entire predictive power of the model, which is not possible if some nodes are not activated.

6. Explain why initializing the parameters of a neural net with a constant is a bad idea.
    a. This is a bad idea because the model will not perform well and training will be difficult. The layers in will produce the same linear combination and therefore the gradients will stay the same. Since all layers are the same, the model is also unable to learn different and new information.

7. You design a fully connected neural network architecture where all activations are sigmoids. You initialize the weights with large positive numbers. Is this a good idea? Explain your answer.
    a. This is not a good idea because each neuron will be activated with a value of 1 or near 1. This will cause vanishing gradients and the model will not be able to learn.

8. Explain what is the importance of “residual connections”.
    a. Residual connections allow us to create a deeper networks without the vanishing gradient problem. The connection connects an earlier layer to a deeper layer and prevents the gradient from disappearing.

9. What is cached (“memoized”) in the implementation of forward propagation and backward propagation?
    ▫ Variables computed during forward propagation are cached and passed on to the corresponding backward propagation step to compute derivatives.
    ▫ Caching is used to keep track of the hyperparameters that we are searching over, to speed up computation.
    ▫ Caching is used to pass variables computed during backward propagation to the corresponding forward propagation step. It contains useful values for forward propagation to compute activations.

10. Which of the following statements is true?
    ▫ The deeper layers of a neural network are typically computing more complex features of the input than the earlier layers.
    ▫ The earlier layers of a neural network are typically computing more complex features of the input than the deeper layers.

Revisiting Jacobians

Recall that Jacobians are generalizations of multi-variate derivatives and are extremely useful in denoting the gradient computations in computation graph and Backpropagation. A potentially confusing aspect of using Jacobains is their dimensions and so, here we're going focus on understanding Jacobian dimensions.

Recap:

Let's first recap the formal definition of Jacobian. Suppose $\mathbf{f}: \mathbb{R}^n \to \mathbb{R}^m$ is a function takes a point $\mathbf{x} \in \mathbb{R}^n$ as input and produces the vector $\mathbf{f}(\mathbf{x}) \in \mathbb{R}^m$ as output. Then the Jacobian matrix of $\mathbf{f}$ is defined to be an $m \times n$ matrix, denoted by $\mathbf{J_f}(\mathbf{x})$, whose (i, j)th entry is $\mathbf{J}_{ij} = \frac{\partial f_i}{\partial x_j}$, or:

$$\mathbf{J} = \begin{bmatrix} \frac{\partial \mathbf{f}}{\partial x_1} & \cdots & \frac{\partial \mathbf{f}}{\partial x_n} \end{bmatrix} = \begin{bmatrix} \nabla^\top f_1 \\ \vdots \\ \nabla^\top f_m \end{bmatrix} = \begin{bmatrix} \frac{\partial f_1}{\partial x_1} & \cdots & \frac{\partial f_1}{\partial x_n} \\ \vdots & \ddots & \vdots \\ \frac{\partial f_m}{\partial x_1} & \cdots & \frac{\partial f_m}{\partial x_n} \end{bmatrix}$$

Examples:

The shape of a Jacobian is an important notion to note. A Jacobian can be a vector, a matrix, or a tensor of arbitrary ranks. Consider the following special cases:

- If f is a scalar and w is a $d \times 1$ column vector, the Jacobian of f with respect to **w** is a row vector with $1 \times d$ dimensions.
- If y is a $n \times 1$ column vector and z is a $d \times 1$ column vector, the Jacobian of $\mathbf{z}$ with respect to y, or $J_z(y)$ is a $d \times n$ matrix.
- Suppose A $\in \mathbb{R}^{m \times n}$ and $\mathbf{B} \in \mathbb{R}^{l \times p \times q}$. Then the Jacobian $J_A(B)$ is a tensor of shape $(m \times n) \times (l \times p \times q)$. More broadly, the shape of the Jacobian is determined as (shape of the output)×(shape of the input).

Problem setup:

Suppose we have:

- X, an $n \times d$ matrix, $x_i \in \mathbb{R}^{d \times 1}$ correspond to the rows of $X = [x_1, \dots, x_n]^\top$
- Y, a $n \times k$ matrix
- W, a $k \times d$ matrix and w, a $d \times 1$ vector

For the following items, compute <u>(1) the shape of each Jacobian, and (2) an expression for each Jacobian</u>:

1. $f(w) = c$ (constant)
    a. Shape = 1xd
    b. $\nabla f(w) = 0$

2. $f(w) = \| w \|^2$ (squared L2-norm)
    a. 1xd
    b. $\nabla f(w) = 2w^T$

3. $f(w) = w^\top x_i$ (vector dot product)
    a. 1xd
    b. $\nabla f(w) = x_i^T$

4. $f(w) = Xw$ (matrix-vector product)
    a. n x d
    b. $\nabla f(w) = X$

5. $f(w) = w$ (vector identity function)
    a. d x d
    b. $\nabla f(w) = I_d$

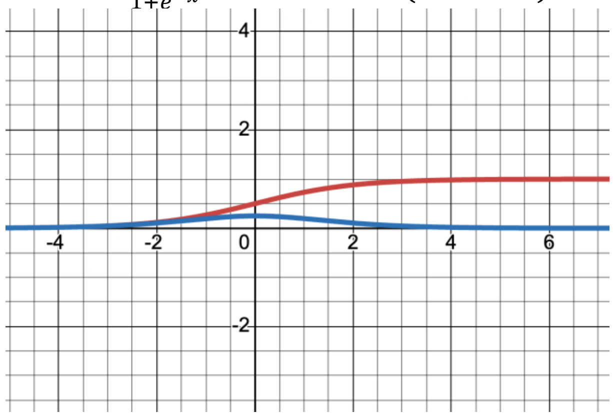
6. $f(w) = w^2$ (element-wise power)
    a. d x d
    b. $\nabla f(w) = diag(2w)$

7. **Extra Credit:** $f(W) = XW^\top$ (matrix multiplication)

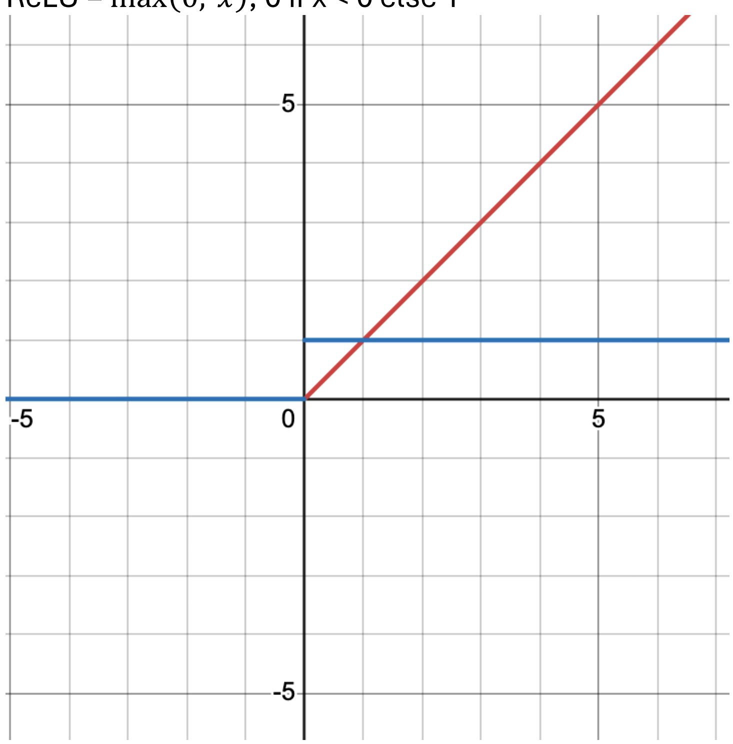
Activations Per Layer, Keeps Linearity Away!

Based on the content we saw at the class lectures, answer the following:

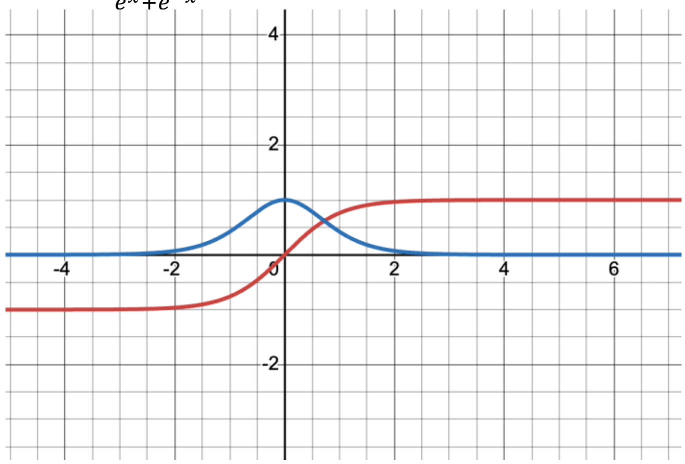
1. Why are activation functions used in neural networks?
    a. Activation functions are used to introduce non-linearity in the model. They also make it easier to approximate any continuous function.
2. Write down the formula for three common action functions (sigmoid, ReLU, Tanh) and their derivatives (assume scalar input/output). Plot these activation functions and their derivatives on $(-\infty, +\infty)$.
    a. $\sigma(x) = \frac{1}{1+e^{-x}}, \sigma'(x) = \sigma(x)\big(1-\sigma(x)\big)$



    b. ReLU = $\max(0,\ x)$, 0 if x < 0 else 1



c. $tanh = \frac{e^x - e^{-x}}{e^x + e^{-x}}$, $tanh' = 1 - \tanh^2(x)$



3. What is the "vanishing gradient" problem? (respond in no more than 3 sentences) Which activation functions are subject to this issue and why? (respond in no more than 3 sentences).

    a. Gradients shrink exponentially as they backpropagate through the layers which may prevent the model from learning. The sigmoid and tanh are most prone to this problem because they are near 0.

4. Why zero-centered activation functions impact the results of Backprop?

    a. Zero-centered activation functions impact the results of backpropagation because of the vanishing gradient problem. The values which are extremely small eventually cause all values to become zero.

5. Remember the Softmax function $\sigma(\mathrm{z})$ and how it extends sigmoid to multiple dimensions? Let's compute the derivative of Softmax for each dimension. Prove that:

$$\frac{d\sigma(\mathbf{z})_i}{dz_j} = \sigma(\mathbf{z})_i\left(\delta_{ij} - \sigma(\mathbf{z})_j\right)$$

where δ_{ij} is the Kronecker delta function.[1]

    a. If we differentiate the softmax function, then we get:

[1] https://en.wikipedia.org/wiki/Kronecker_delta

$$\frac{\partial \sigma(z)_i}{\partial z_j} = \frac{\partial}{\partial z_j}\left(\frac{e^{z_i}}{S}\right)$$

And if we try the two cases of Kronecker delta function, we have two derivates:

$\frac{\partial \sigma(z)_i}{\partial z_i} = \frac{e^{z_i}}{S}\left(1 - \frac{e^{z_i}}{S}\right) = \sigma(z)_i(1 - \sigma(z)_i)$, if i == j and,

$$\frac{\partial \sigma(z)_i}{\partial z_i} = \frac{e^{z_i}}{S}\left(-\frac{e^{z_i}}{S}\right) = \sigma(z)_i(-\sigma(z)_i)$$

When combining, we have the final form:

$$\frac{\partial \sigma(z)_i}{\partial z_i} = \sigma(z)_i\left(\delta_{ij} - \sigma(z)_i\right)$$

6. Use the above point to prove that the Jacobian of the Softmax function is the following:

$$\mathbf{J}_\sigma(\mathbf{z}) = \mathrm{diag}\big(\sigma(\mathbf{z})\big) - \sigma(\mathbf{z})\sigma(\mathbf{z})^\top$$

where $\mathrm{diag}(.)$ turns a vector into a diagonal matrix. Also, note that $\mathbf{J}_\sigma(\mathbf{z}) \in \mathbb{R}^{K\times K}$..

a. Given the formula in the last problem, the two cases we get are:

$J_{ii} = \sigma(z)_i(1 - \sigma(z)_i)$ and $J_{ij} = \sigma(z)_i\big(-\sigma(z)_j\big)$

We can structure this as:

$J_{\sigma(z)} = diag\big(\sigma(z)\big) - \sigma(z)\sigma(z)^T$

Because $diag\big(\sigma(z)\big)$ is a diagonal matrix of $\sigma(z)$ and the outer product of $\sigma(z)\sigma(z)^T$ is $\sigma(z)_i\sigma(z)_j$ and subtracting the two gives the two cases above.

Simulating XOR

1. Can a single-layer network simulate (represent) an XOR function on $\mathbf{x} = [x_1, x_2]$?

$$y = \mathrm{XOR}(\mathbf{x}) = \begin{cases} 1, & \text{if } \mathbf{x} = (0,1) \text{ or } \mathbf{x} = (1,0) \\ 0, & \text{if } \mathbf{x} = (1,1) \text{ or } \mathbf{x} = (0,0). \end{cases}$$

Explain your reasoning using the following single-layer network definition: $\hat{y} = \mathrm{ReLU}(W \cdot \mathbf{x} + b)$

It is not possible with a single layer because the layer above is just a linear function with a max of 0.

2. Repeat (1) with a two-layer network:

$$\mathbf{h} = \text{ReLU}(W_1 \cdot \mathbf{x} + \mathbf{b}_1)$$
$$\hat{y} = W_2 \cdot \mathbf{h} + b_2$$

   Note that this model has an additional layer compared to the earlier question: an input layer x ∈ $\mathbb{R}^2$, a hidden layer h with ReLU activation functions that are applied component-wise, and a linear output layer, resulting in scalar prediction $\hat{y}$. Provide a set of weights W_1 and W_2 and biases b_1 and b_2 such that this model can accurately model the XOR problem.

   $W_1 =$ [[1, -1], [-1, 1]], $b_1 =$ [[0], [0]], $W_2 =$ [1, 1], $b_2 =$ 0

3. Consider the same network as above (with ReLU activations for the hidden layer), with an arbitrary differentiable loss function $\ell: \{0,1\} \times \{0,1\} \to \mathbb{R}$ which takes as input $\hat{y}$ and y, our prediction and ground truth labels, respectively. Suppose all weights and biases are initialized to zero. Show that a model trained using standard gradient descent will not learn the XOR function given this initialization.

   a. Since the weights and biases are initialized to zero, the gradients will not update and therefore the model will not be able to represent the XOR function.

4. **Extra Credit:** Now let's consider a more general case than the previous question: we have the same network with an arbitrary hidden layer activation function:

$$\mathbf{h} = f(W_1 \cdot \mathbf{x} + \mathbf{b}_1)$$
$$\hat{y} = W_2 \cdot \mathbf{h} + b_2$$

   Show that if the initial weights are any uniform constant, then gradient descent will not learn the XOR function from this initialization.

A computation graph, so elegantly designed
With nodes and edges, so easily combined
It starts with inputs, a simple array
And ends with outputs, in a computationally fair way

Each node performs, an operation with care
And passes its results, to those waiting to share
The edges connect, each node with its peers
And flow of information, they smoothly steer

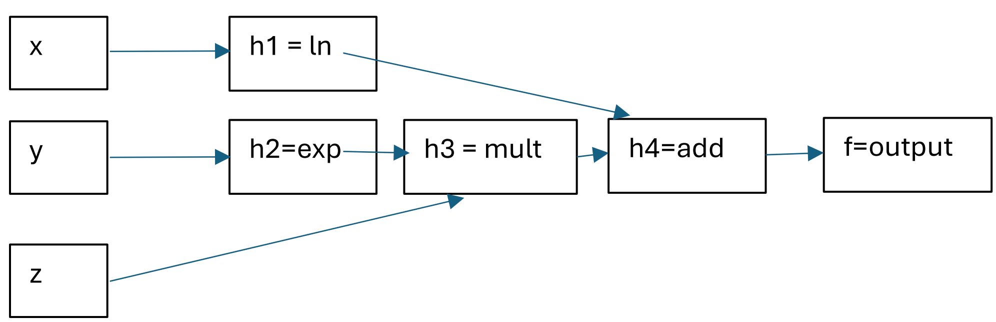
It's used to calculate, complex models so grand
And trains neural networks, with ease at hand
Backpropagation, it enables with grace
Making deep learning, a beautiful race

–ChatGPT Feb 3 2023

Neural Nets and Backpropagation

Draw the computation graph for $f(x, y, z) = \ln x + \exp(y) \cdot z$. Each node in the graph should correspond to only one simple operation (addition, multiplication, exponentiation, etc.). Then we will follow the forward and backward propagation described in class to estimate the value of f and partial derivatives $\frac{\partial f}{\partial x}, \frac{\partial f}{\partial y}, \frac{\partial f}{\partial z}$ at $[x, y, z] = [1,3,2]$. For each step, show you work.

1. Draw the computation graph for $f(x, y, z) = \ln x + \exp(y) \cdot z$. The graph should have three input nodes for x, y, z and one output node f. Label each intermediate node h_i.



2. Run the forward propagation and evaluate f and h_i $(i = 1,2, \ldots)$ at $[x, y, z] = [1,3,2]$.
    a. F(1, 3, 2) = ln(1) + exp(3) * 2 = 40.17

3. Run the backward propagation and give partial derivatives for each intermediate operation, i.e., $\frac{\partial h_i}{\partial x}$, $\frac{\partial h_j}{\partial h_i}$, and $\frac{\partial f}{\partial h_i}$. Evaluate the partial derivatives at $[x, y, z] = [1,3,2]$.

$$f' = \frac{\partial f}{\partial f}$$

$$h_4' = \frac{\partial f}{\partial h_1} = 1$$

$$h_3' = \frac{\partial f}{\partial h_3} = 1$$

$$h_2' = \frac{\partial h_2}{\partial y} = \exp(y)$$

$$h_1' = \frac{\partial h_1}{\partial x} = \frac{1}{x}$$

4. Aggregate the results in (c) and evaluate the partial derivatives with chain rule. Show your work.

$f = h_1 + h_3$ and $h_1 = \ln(x)$ so $\frac{\partial f}{\partial x} = \frac{\partial f}{\partial h_1} \cdot \frac{\partial h_1}{\partial x} = \frac{1}{x}$

$$\frac{\partial f}{\partial y} = \frac{\partial f}{\partial h_3} \cdot \frac{\partial h_3}{\partial y} = 1 \cdot \exp(y)$$

$\frac{\partial h_3}{\partial h_2} = z$ and $\frac{\partial h_3}{\partial z} = h_2$ so $\frac{\partial f}{\partial z} = \frac{\partial f}{\partial h_3} \cdot \frac{\partial h_3}{\partial z} = \exp(y)$

Programming

In this programming homework, we will

- implement MLP-based classifiers for the sentiment classification task of homework 1.

Skeleton Code and Structure:

The code base for this homework can be found at this GitHub repo under the `hw3` directory. Your task is to fill in the missing parts in the skeleton code, following the requirements, guidance, and tips provided in this pdf and the comments in the corresponding .py files. The code base has the following structure:

- `mlp.py` reuse the sentiment classifier on movie reviews you implemented in homework 1, with additional requirements to implement MLP-based classifier architectures and forward pass .

- `main.py` provides the entry point to run your implementations `mlp.py`

- `hw3.md` provides instructions on how to setup the environment and run each part of the homework in `main.py`

TODOs — Your tasks include 1) generate plots and/or write short answers based on the results of running the code; 2) fill in the blanks in the skeleton to complete the code. We will explicitly mark these plotting, written answer, and filling-in-the-blank tasks as **TODOs** in the following descriptions, as well as a **`# TODO`** at the corresponding blank in the code. **TODOs** (Copy from your HW1). We are reusing most of the `model.py` from homework 1 as the starting point for the `mlp.py` - you will see in the skeleton that they look very similar. Moreover, in order to make the skeleton complete, for all the **`# TODO (Copy from your HW1)`**, please fill in the blank below them by copying and pasting the corresponding implementations you wrote for homework 1 (i.e. the corresponding **`# TODO`** in homework 1.)

Submission:

Your submission should contain two parts: 1) plots and short answers under the corresponding questions below; and 2) your completion of the skeleton code base, in a `.zip` file

MLP-based Sentiment Classifier

In both homework 1 & 2, our implementation of the `SentimentClassifer` is essentially a single-layer feedforward neural network that maps input features directly to 2-dimensional output logits. In this part of the programming homework, we will expand the architecture of our classifier to multi-layer perceptron (MLP).

Reuse Your HW1 Implementation

TODOs (Copy from your HW1): for all the **`# TODO (Copy from your HW1)`** in `mlp.py`, please fill in the blank below them by copying and pasting the corresponding implementations you wrote for homework 1 (i.e. the corresponding **`# TODO`** in the `model.py` in homework 1).

Build MLPs

Remember from the lecture that MLP is a multi-layer feedforward network with perceptrons as its nodes. A perceptron consists of non-linear activation of the affine (linear) transformation of inputs.

TODOs: Complete the `__init__` and `forward` function of the `SentimentClassifier` class in `mlp.py` to build MLP classifiers that supports custom specification of architecture (i.e. number and dimension of hidden layers)

Hint: check the comments in the code for specific requirements about input, output, and implementation. Also, check out the document of nn.ModuleList about how to define and implement forward pass of MLPs as a stack of layers.

Train and Evaluate MLPs

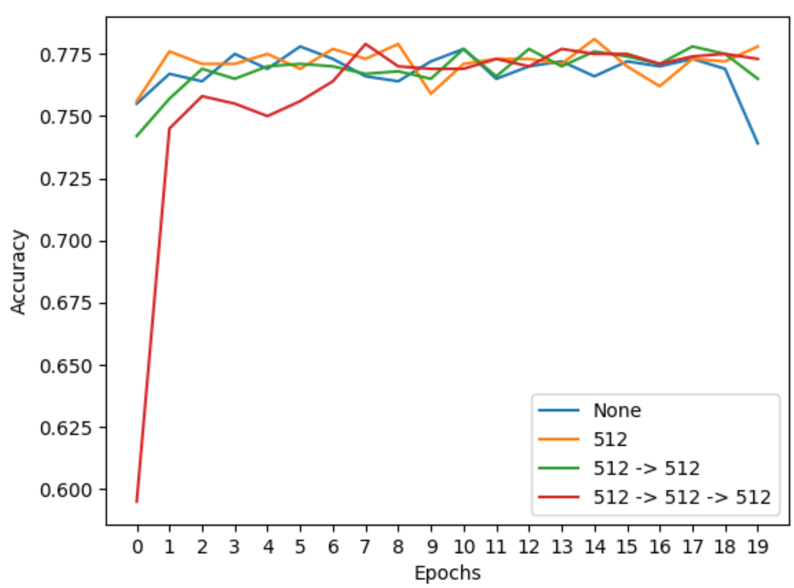
We provide in `main.py` several MLP configurations and corresponding recipes for training them.

TODOs Once you finished 6.1.2, you can run `load_data_mlp` and `explore_mlp_structures` to train and evaluate these MLPs and paste two sets of plots here:

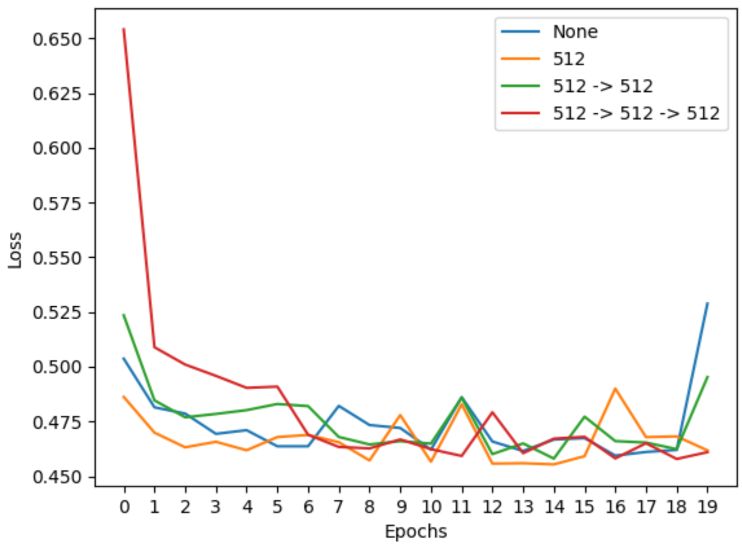
- 4 plots of train & dev loss for each MLP configuration
- 2 plots of dev losses and accuracies across MLP configurations

and describe in 2-3 sentences your findings.
Hint: what are the trends of train & dev loss and are they consistent across different configurations? Are deeper models always better? Why?

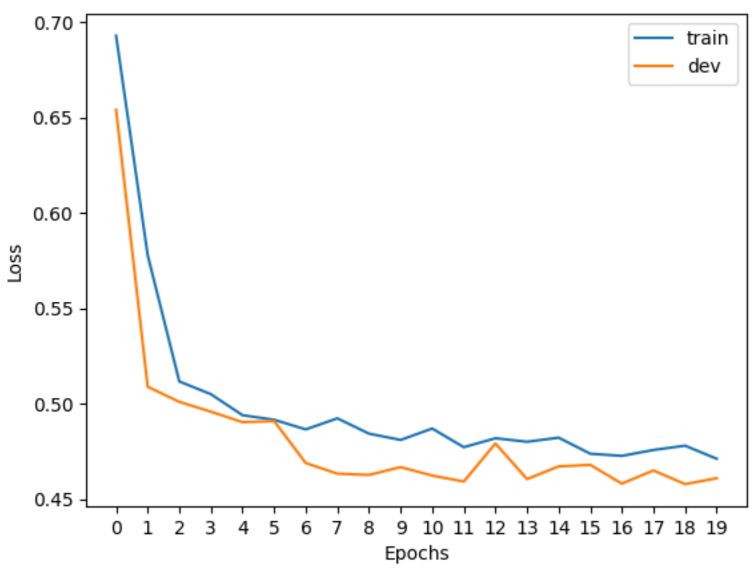
all_mlp_acc



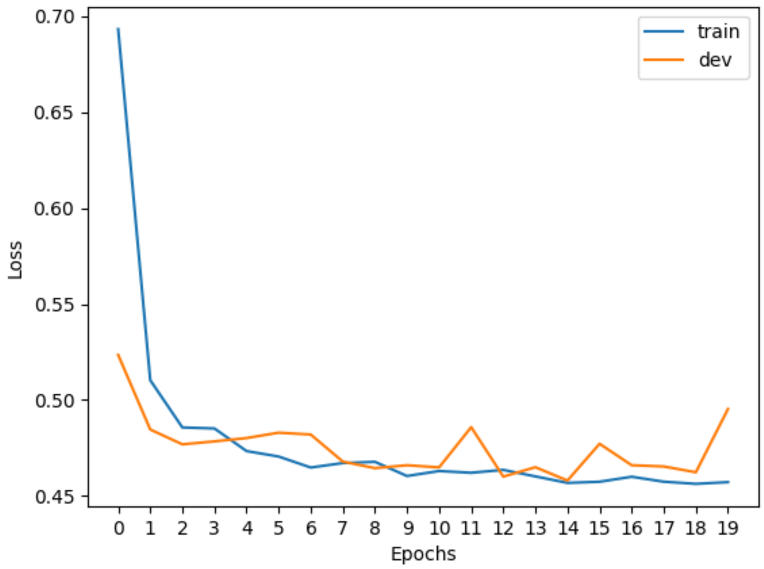
all_mlp_loss



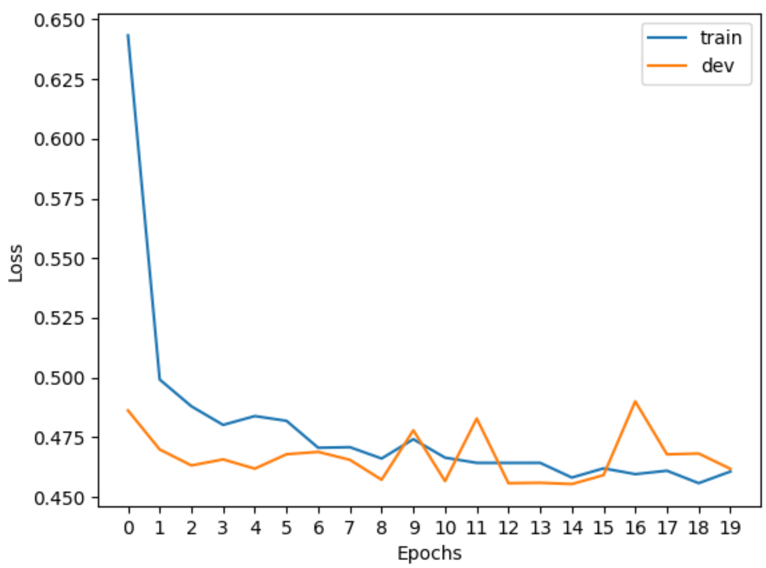
mlp_512 -> 512 -> 512_loss



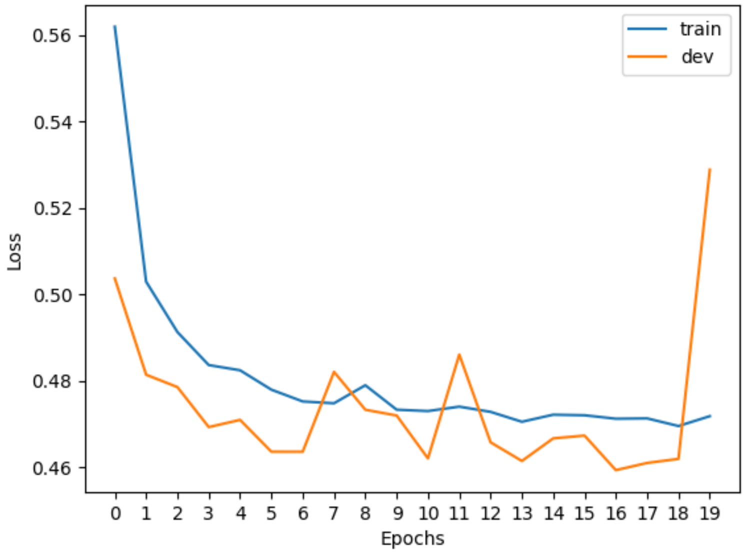
mlp_512 -> 512_loss



mlp_512_loss



mlp_None_loss



From the plots above we can see that all model configurations perform similarly in terms of accuracy and loss. When we compare the dev and train losses for each configuration, we can see that adding a hidden layer to the model slightly improves the loss over no hidden layers. However, deeper models may not always be better since they are prone to overfitting.

Embrace Non-linearity: The Activation Functions

Remember we have learned why adding non-linearity is useful in neural nets and gotten familiar with several non-linear activation functions both in the class and 3. Now it is time to try them out in our MLPs!

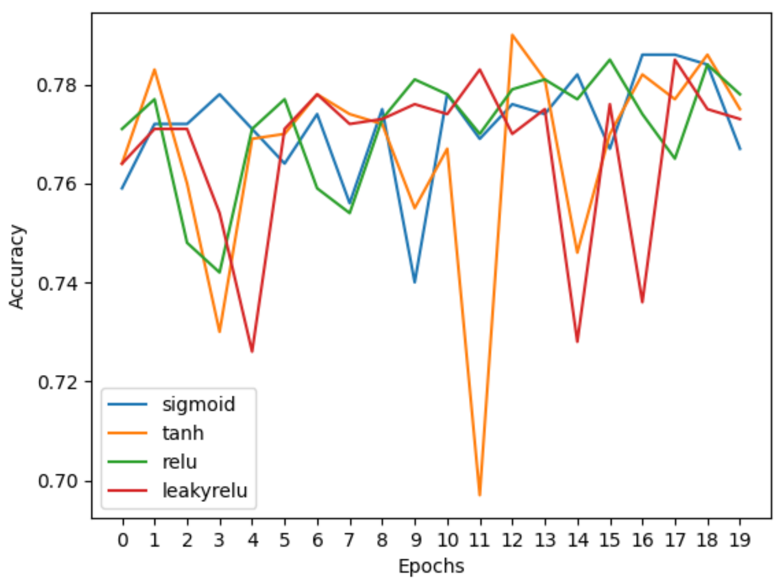
Note: for the following TODO and the TODO in 6.1.5, we fix the MLP structure to be with a single 512-dimension hidden layer, as specified in the code. You only need to run experiments on this architecture.

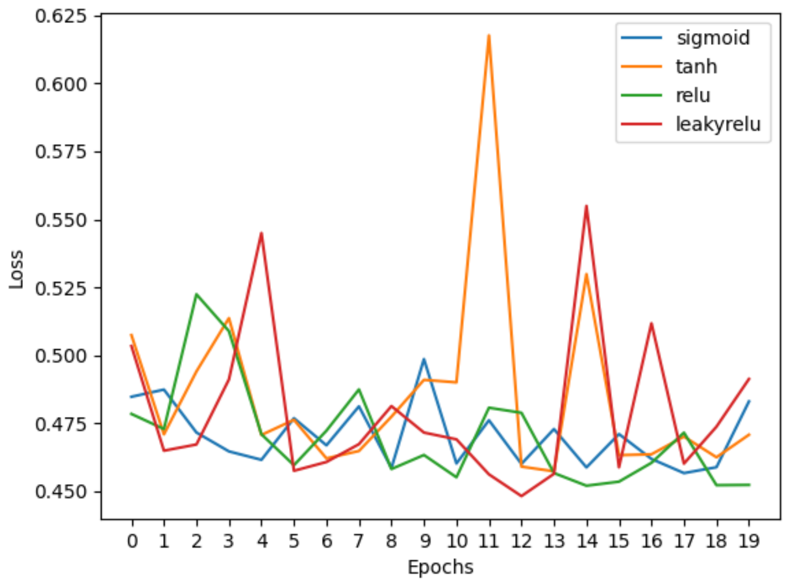
TODOs: Read and complete the missing lines of the two following functions:

- `__init__` function of the `SentimentClassifier` class: define different activation functions given the input `activation` type.
  Hint: we have provided you with a demonstration of defining the Sigmoid activation, you can search for the other `nn.<activation>` in PyTorch documentation.

- `explore_mlp_activations` in `main.py`: iterate over the activation options, define the corresponding training configurations, train and evaluate the model, and visualize the results. Note: you only need to generate the plots of dev loss and dev acc across different configurations, by calling `visualize_configs`, you **do not** need to plot the train-dev loss curves for each configuration (i.e. no need to call `visualize_epochs`). We provide you with a few choices of common activation functions, but feel free to try out the others.
  Hint: You can refer to `explore_mlp_structure` as a demonstration of how to define training configurations with fixed hyper-parameters & iterate over hyper-parameters/design choices of interests (e.g. hidden dimensions, choice of activation), and plot the evaluation results across configurations.

Once you complete the above functions, run `explore_mlp_activations` and paste the two generated plots here. Describe in 2-3 sentences your findings.





From the plots above, we can see that the loss and accuracy are extremely sporadic, more so for Tanh and LeakyReLU activation function. The ReLU and Sigmoid functions are more static. We can also notice a slight improvement for the ReLU and Sigmoid activation functions.

Hyper-parameter Tuning: Learning Rate

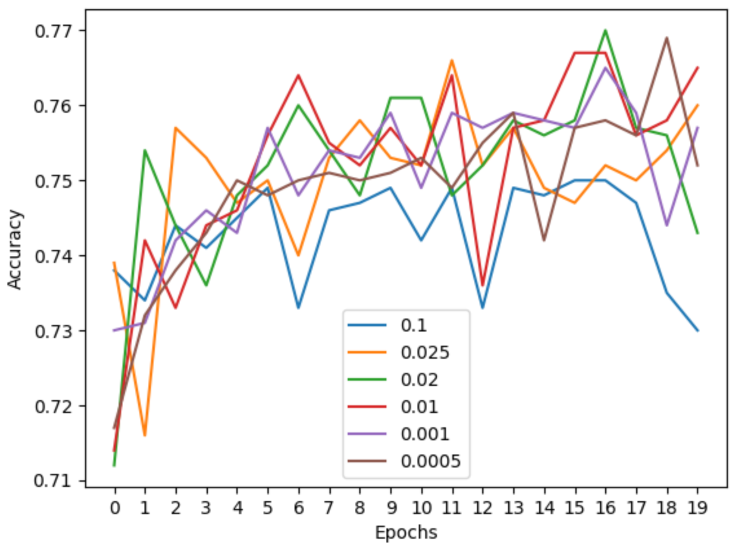
The training process mostly involves learning model parameters, which are automatically performed by gradient-based methods. However, certain parameters are "unlearnable" through gradient optimization while playing a crucial role in affecting model performance, for example, learning rate and batch size. We typically refer to these parameters as *Hyper-parameters*.

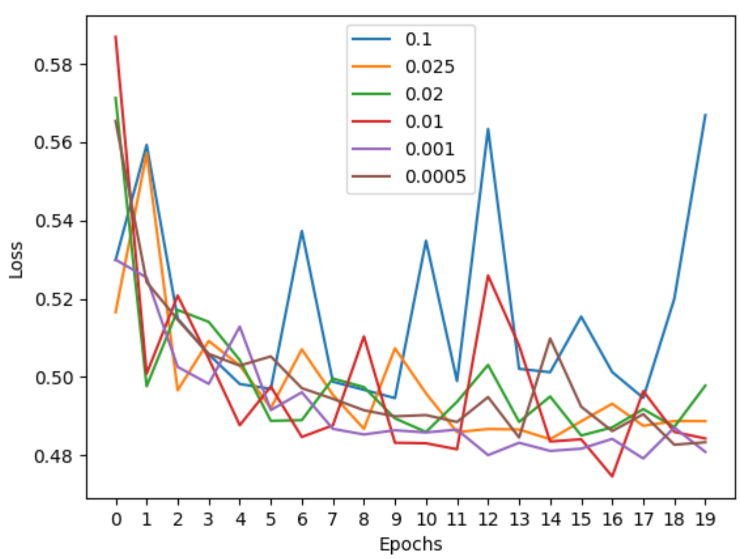
We will now take the first step to tune these hyper-parameters by exploring the choices of one of the most important one - learning rate, on our MLP. (There are lots of tutorials on how to tune the learning rate manually or automatically in practice, for example this note can serve as a starting point.)

TODOs: Read and complete the missing lines in `explore_mlp_learning_rates` in `main.py` to iterate over different learning rate values, define the training configurations, train and evaluate the model, and visualize the results. Note: same as above, you only need to generate the plots of dev loss and dev acc across different configurations, by calling `visualize_configs`, you **do not** need to plot the train-dev loss curves for each configuration (i.e. no need to call `visualize_epochs`). We provide you with the default learning rate we set to start with, and we encourage you to add more learning rate values to explore and include in your final plots curves of **at least 4 different representative learning rates.**

Hint: again, you can checkout `explore_mlp_structure` as a demonstration for how to perform hyper-parameter search.

Once you complete the above functions, run `explore_mlp_learning_rates` and paste the two generated plots here. Describe in 2-3 sentences your findings.





From the plots above, we can see that the largest learning rate of 0.1 has the most volatility which is because the weights are being updated too far in the gradient direction. The volatility decreases as the learning rate decreases. We can see that there is not much different between 0.001 and 0.0005, and increasing the learning rate past this point may make the model very slow to learn.