

Problem 1

Compare the average loss of the two models. Provide an explanation for what you observe.

Average training loss of One layer NN: 0.5431659753792194

Average testing loss One layer NN: 0.657667151617061

Average training loss of Two layer NN: 0.4734565497489776

Average testing loss of Two layer NN: 0.5930840866920725

We can observe that the average of loss of the two layer NN is lower compare to one layer NN. Therefore, the performance of the two layer NN is better than that of the one layer NN. The reason is that the hidden layer in two layer NN is able to learn more complex representations of the input data than one layer NN.

Problem 2

Comment on your parameter choices. These include the learning rate, the hidden layer size and the number of epochs for training.

The learning rate is 0.001, which is the default value. A learning rate of 0.001 is relatively small, which means the model will take smaller steps during training. At same time, this prevents the risk of over shooting and will have a higher chance of better performance.

The hidden layer size is by default, 10. A hidden size of 10 means that the neural network has 10 neurons in its hidden layer. 10 is relatively small for hidden size, but it is enough to work well on simple problems with a small number of input features.

The number of epochs for training is 25, the default. This means that the model will go over the entire training dataset 25 times. This is a reasonable number of epochs, and increasing in may improve performance, but may also cause overfitting problems.

Problem 3

a) If a ‘black box’ model gives an answer that disagrees with a human expert, which answer should be believed? Are there circumstances where we should believe one party more often than the other?

It is not always clear whose answer to be believed. We may trust the human expert more if they have a proven track record of expertise in the relevant field. Also, since the model is a 'black box' with limited transparency and interpretability, we may be more inclined to trust the human expert's opinion, which can be explained and understood more easily. However, in some cases, we may prefer to trust the model's answer over the human expert's opinion if we suspect that the expert's judgment may be biased or influenced by personal factors.

b) Companies often hide the logic behind their products by making their software closed-source. Are there differences between companies selling closed source software, where the logic is known but hidden, versus companies selling 'black box' artificial intelligence software, where the logic might be altogether unknown? Is using one type of software more justifiable than using the other?

One major difference between the two is the level of transparency and accountability. In closed-source software, the company retains control over the software and can be held accountable for any issues or vulnerabilities. In contrast, 'black box' AI software can be even more opaque and difficult to audit, as the internal workings of the software are not always clear, even to the developers. This lack of transparency can raise concerns about accountability, fairness, and bias in the decisions made by the software.

Both can be justifiable in certain circumstances. Closed-source software can be justifiable when it is necessary to protect intellectual property, trade secrets, or confidential information. 'Black box' AI software can be justifiable when it is designed and tested with rigorous standards for accuracy, fairness, and interoperability.