Experiment 3

Stress testing the MNIST image classification model

During our discussion of the MNIST images of handwritten digits, the possibility of degrading the images as a way of stress-testing the model was mentioned. Michael suggested that reducing the contrast would be one way to alter the images. Taking this idea from conceptualization to retesting the model is the goal of this section.

Block 1 is taken from the Colab notebook used during the first two weeks of the course. Run the code cell to load and scale the images.

The contrast of an image can be expressed as the difference between the largest and smallest pixel values. Reducing the contrast amounts to shrinking this difference.

3.1 Scaling (shrinking or expanding) an interval

An interval can be defined by an endpoint on the left, x_1, and an endpoint on the right, x_2. The range of the interval is defined as $x_2 - x_1$ (numbers in this interval range from x_1 to x_2). The midpoint of the interval is $(x_1 + x_2)/2$.

The first two lines of code in the first code snippet of Block 2 read input from the user to set the endpoints of the interval. Complete the last two lines of code in this code snippet to calculate the range and the midpoint of the specified interval. Enable checking the code by add a print statement that displays the range and midpoint. Run the code cell a few times to convince yourself that the code snippet is working correctly. When you have convinced yourself, add a comment below the code snippet displaying a message like "An interval with endpoints x1 = ... and x2 = ... has range ... and midpoint ... "

When considering an image, x_1 is the minimum intensity (the minimum pixel value) and x_2 is the maximum intensity (the maximum pixel value, and the interval $[x_1, x_2]$ gives the range of intensities. Reducing the range of this interval (reducing its length) reduces the contrast of the image. To do this, the interval is first centered at 0 by subtracting the midpoint, shrunk by multiplying both endpoints by a scale factor, and then recentered by adding the midpoint.

The second code snippet in Block 2 shrinks the interval created in the first code snippet. Uncomment this code snippet, add a print statement that displays the endpoints, the range, and the midpoint of the new interval. Run the code cell a few times to convince yourself that the interval is shrinking as expected. When you have convinced yourself, add a comment below the code snippet displaying a message like "The interval has endpoints x1 = ... and x2 = ..., range ..., and midpoint ... after it is shrunk."

3.2 Scaling an image in the MNIST dataset

The method of Block 2 is applied to a randomly selected image from the MNIST dataset in Block 3. Before and after images are displayed so that the decrease in contrast can be checked visually. Run the code cell of Block 3 to confirm that the contrast of the image has been reduced. After you have confirmed that the code is working as intended, add comments as indicated to explain how the code functions.

3.3 Scaling the images in the MNIST dataset

Write code in the code cell of Block 4 that applies the ideas of Block 3 to the entire MNIST dataset (all of `X_train` and all of `X_test`. Include an adapted version of the final code snippet of the code cell in Block 1 to compare three randomly selected images visually.

3.4 Testing the model of week 2 on the reduced contrast images

Copy and paste the code blocks that define and compile, train, assess, and test the model from `MNISTv2`, the Colab notebook of week 2 as Blocks 5–8.

Run the model on the reduced contrast images. Compare the test accuracy obtained for the reduced contrast images to the test accuracy obtained for the unaltered images. You may still have this value in the output of `MNISTv2`. If not, rerun the notebook.

Choosing a very small value for the scale factor will certainly cause the model to perform poorly. That is too easy. To make this step more realistic, rerun Blocks 4–8, changing the scale factor until the test accuracy is between 45 and 55 % of the test accuracy for the unaltered images.

Add a text cell as the last cell in your notebook in which you summarize the results of this experiment. The summary should include the scale factor you used to degrade the images, the test accuracy before and after degrading the images, and commentary about the model's performance that reflects on how the model performed versus how well you think a typical person would perform when classifying the nine images displayed as predictions.