Homework 2: MNIST and Nearest Neighbor Classification

The MNIST dataset contains images of handwritten digits from 0-9, and labels $y = \{0, 1, \ldots, 9\}$. The provided script loads the MNIST dataset and displays a few images.

1. Display the 18th image in the training set. What digit is it? What is the label of the 18th image?

2. Display several images from the training set, and the corresponding labels.

3. A nearest neighbor classifier predicts the label of a new data point by finding the 'closest' data point in the training set, and using its label. If the training dataset is given by $\mathcal{D} = \{(x_i, y_i)\}_{i=1}^n$, we can specify the *nearest neighbor* of a new data point x as

$$i^* = \arg\min_i d(x, x_i)$$

and the *nearest neighbor classifier* as

$$f(x) = y_{i^*}$$

where $d(\cdot, \cdot)$ is some notion of distance. The ℓ_2 distance between two images is the square root of the sum of the squared difference between the pixel values, and can be computed in a number of ways, for example `np.linalg.norm(xtrain[i] - xtest)`.

a) Write a nearest neighbor classifier function. The function should take a single test image as input, and compute the index of the image in the training dataset that is closest to the test image (closest in an ℓ_2 sense). For this assignment, only use the first 2000 images in the training dataset. The function should then return the label of the closest training image (out of the first 2000 images in the training set).

b) Use the function to predict the class of the first image in the test dataset. What is the predicted class? Is it correct? What is the misclassification loss? What is the squared error loss?

c) Write a for loop to predict the classes of the first 1,000 images in the test set. What is empirical risk of the nearest neighbor classifier when using the misclassification (0/1) loss? What is the empirical risk when using the squared error loss function?

d) Display some of the images that were classified incorrectly alongside their nearest neighbor, and comment on why the classifier may have made a mistake.

4. A k-nearest neighbors (knn) classifier estimates the class as the *modal* class of the k nearest neighbors. In other words, the classifier finds the k labeled data points that are closest to the new data point, and finds the most commonly occurring label of those points. Write a knn classifier, and use it to predict the classes of the first 1000 images in the test set. What is empirical risk when $k = 10$?