Foundations of Deep Learning – Homework Assignment #4
Adi Album & Tomer Epshtein

Part 1:

Experiment:

Demonstrate the four empirical postulates we relied on in class when rationalizing about generalization in deep learning.

Results:

We chose to work with the CIFAR10 dataset with the common MobileNetV2 architecture.

Here are our results:

1. Standard NNs (=MobileNetV2) trained by a standard optimization algorithm (=Adam) on a standard dataset (=CIFAR10) generalize well without any explicit regularization. Even though # of learned parameters >> # of training examples.
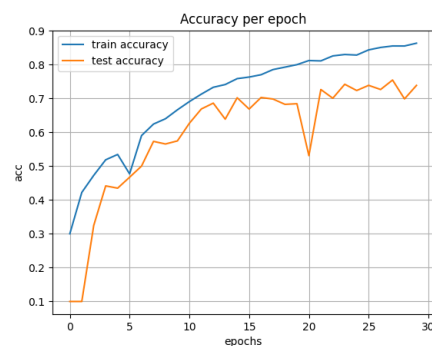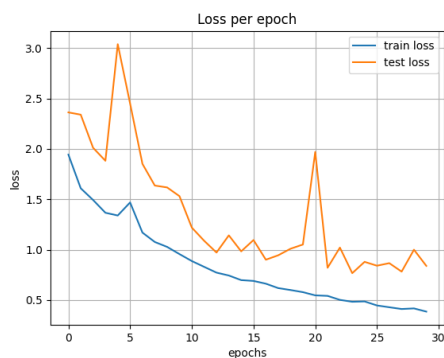
2. In the regime of (1.), the training error of learned hypothesis ≈ 0. This remains the case even if we replace the training examples by <u>any</u> training set of the same size. We demonstrated this by replacing CIFAR10 dataset with random images (with every pixel randomly samples from a uniform 0,1 distribution) and every image is uniformly at random labeled 0-9.
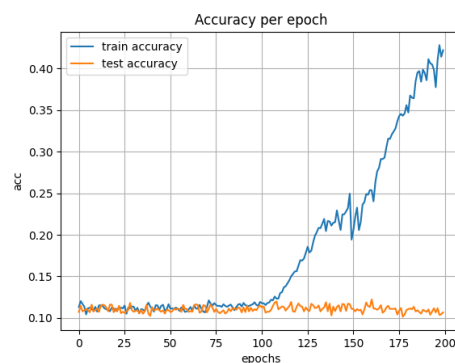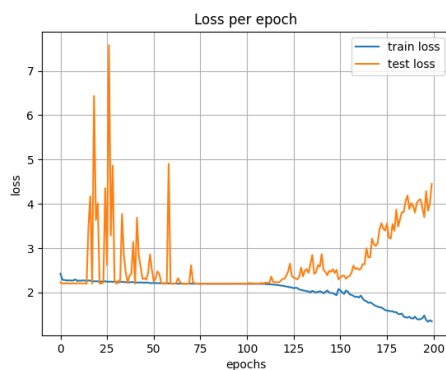
3. In the regime of (1.), with half the training set being CIFAR10 and the second half is replaced by random data, the test error of the learned hypothesis (whose training error is of course ≈ 0) is far better than trivial.

Loss per epoch / Accuracy per epoch
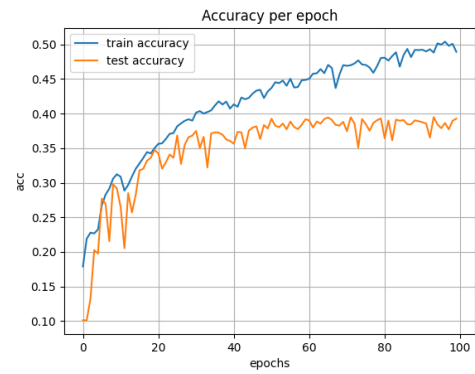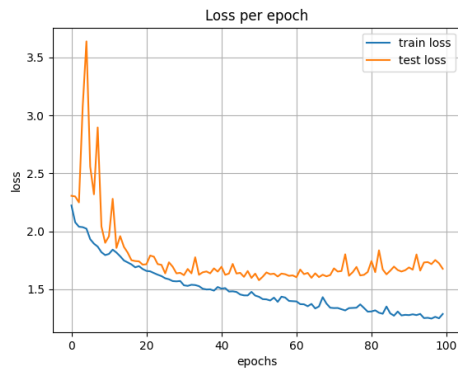
4. In the regime of (1.), with half of the training being CIFAR10 and the second half replaced by adversarially labeled CIFAR10, test error significantly deteriorates

Loss per epoch / Accuracy per epoch