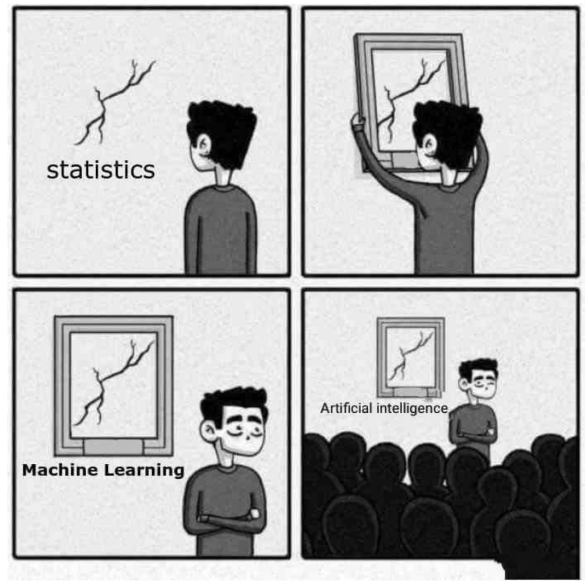
Chapter 1: The Learning Problem (II)



1 Section 1.1.3: Learning vs Design

Problem 1. You should complete Exercise 1.5 to get practice identifying when to use a learning approach to a problem, and when to use a "design" approach to a problem.

2 Section 1.3: Is Learning Feasible? and Section 1.4: Error and Noise

Problem 2. Draw Figure 1.11, highlighting the differences between Figure 1.9 and Figure 1.2.

Problem 3. In this problem we will explore the train/test split protocol for training machine learning algorithms.

1. Define the in-sample error and out-of-sample errors (page 21).

2. A fundamental goal of the machine learning discipline is to understand the out-of-sample error of different algorithms. One of the most powerful tools for doing this is Hoeffding's inequality. It is introduced informally in the textbook on page 19, Eq (1.4) in the context of a toy example involving marbles. The following formally stated theorem is a bit more versatile, and it's what we'll rely on in this class.

   Theorem 1 (Hoeffding Inequality)**.** Let $a_1, ..., a_N$ be N independent and identically distributed random variables satisfying $0 \leq a_i \leq 1$. Let $\nu = \frac{1}{n} \sum_{i=1}^{N} a_i$ be the empirical average and $\mu = \mathbb{E}\nu$ be the true mean of the underlying distribution. Then, for all $\epsilon > 0$,

   $$\mathbb{P}\left(|\nu - \mu| \geq \epsilon\right) \leq 2\exp(-2\epsilon^2 N). \tag{1}$$

   Describe the shape of the distribution defined by inequality 1 above.

3. Let g be the output of running the PLA on the training data. What does Hoefding's inequality say about the out-of-sample error?

Problem 4. How large of a test set do you need to guarantee with probability at least 0.99 that $|E_{\text{test}} - E_{\text{out}}| \leq 0.01$?

Problem 5. This problem explores the optimal way to size your test sets.

1. If you have a test set with 1000 samples, what bound does the Hoeffding inequality give on the probability that $|E_{\text{test}} - E_{\text{out}}| \leq 0.01$?

2. Why is this bound "trivial"?

3. What if you change the accuracy to $|E_{\text{test}} - E_{\text{out}}| \leq 0.05$?

4. What if you use the original accuracy $|E_{\text{test}} - E_{\text{out}}| \leq 0.01$ but use 10000 samples in your test set?

5. If we expect the accuracy of our learning algorithm to be close to 1 (i.e. we expect $|E_{\text{test}} - E_{\text{out}}|$ to be close to 0), should we use a larger or a smaller test set than when we expect the accuracy to be close to 0.8 (i.e. we expect $E_{\text{test}} - E_{\text{out}}|$ to be close to 0.2)?