



Why

A natural and simple approach is to select a predictor which performs best on the (correctly) labeled training dataset.

Definition

Let $((X, \mathcal{X}, \mu), f : X \rightarrow Y)$ be a probabilistic data-generation model. For a dataset $(x_1, y_1), \dots, (x_n, y_n)$ in $X \times Y$, the *empirical error* of a predictor $h : X \rightarrow Y$ is

$$\frac{1}{n} |\{i \in \{1, 2, \dots, n\} \mid h(\xi_i) \neq \gamma_i\}|,$$

and so an *empirical error minimizer* for the dataset is a hypothesis whose empirical error is minimal.

Let $\mathcal{M}_{X \rightarrow Y}$ denote the set of measurable functions from X to Y . An *empirical risk minimization inductor* or *empirical risk minimization algorithm* is an inductor $A : (X \times Y)^n \rightarrow \mathcal{M}_{X \rightarrow Y}$ for which $A(D)$ is an empirical risk minimizer of D , for all datasets $D \in (X \times Y)^n$,

Other terminology for the empirical error includes *empirical risk*. For these reasons, the learning paradigm of selecting a predictor h to minimize the empirical risk is called *empirical risk minimization* or *ERM*.

Overfitting

Although selecting a classifier to minimize the empirical risk seems natural, it can be foolish. Let $A \subset X \subset \mathbf{R}^2$, and $Y =$

$\{0, 1\}$. Suppose that the true classifier $f : \mathcal{X} \rightarrow \mathcal{Y}$ is $f(x) = 1$ if $x \in A$ and $f(x) = 0$ otherwise. Suppose that for the underlying distribution (X, \mathcal{X}, μ) we have $A \in \mathcal{X}$ and $\mu(A) = 1/2$.

For any training set $(x_1, y_1), \dots, (x_n, y_n)$ in $X \times Y$, the hypothesis $h : X \rightarrow Y$ defined by

$$h(x) = \begin{cases} y_i & \text{if } x_i = x \\ 0 & \text{otherwise.} \end{cases}$$

achieves zero empirical risk but has error (w.r.t. μ) of $1/2$. Such a classifier is said to be *overfit* or to exhibit *overfitting*. It is said to fit the training dataset “too well.”

Inductive bias

One way to mitigate overfitting for empirical error minimization is to constrain the set of predictors considered to a particular hypothesis class. As mentioned in Hypothesis Classes, we call the hypothesis class an *inductive bias*.

