



Why

With a probabilistic data-generation model, it is natural to select a hypothesis which performs well on the training set.

Definition

Let $((\Omega, \mathcal{A}, \mathbf{P}), \{x_i : \Omega \rightarrow \mathcal{X}\}_{i=1}^n, f : \mathcal{X} \rightarrow \mathcal{Y})$ be *probabilistic data-generation model* with training set $S : \Omega \rightarrow (\mathcal{X} \times \mathcal{Y})^n$.

For a dataset $D = ((\xi_1, \gamma_1), \dots, (\xi_n, \gamma_n)) \in (\mathcal{X} \times \mathcal{Y})^n$, the *empirical error* of a predictor $h : \mathcal{X} \rightarrow \mathcal{Y}$ is

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

and so an *empirical error minimizer* for the dataset is a hypothesis $h : \mathcal{X} \rightarrow \mathcal{Y}$ whose empirical error is minimal.

An *empirical risk minimization inductor* or *empirical risk minimization algorithm* is $A : (\mathcal{X} \times \mathcal{Y})^n \rightarrow (\mathcal{X} \rightarrow \mathcal{Y})$ for which $A((\xi_1, \gamma_1), \dots, (\xi_n, \gamma_n))$ is an empirical risk minimizer.

For the random variable training set S , the *training error* of a classifier $h : \mathcal{X} \rightarrow \mathcal{Y}$ is a random variable $\text{err}_h : \Omega \rightarrow \mathbf{R}$ defined by

$$\text{err}_h(\omega) = (1/n) |\{i \in \{1, 2, \dots, m\} \mid h(x_i(\omega)) \neq y_i(\omega)\}|,$$

and the *empirical error minimizer set* is the random variable $\text{EEM} : \Omega \rightarrow (\mathcal{X} \rightarrow \mathcal{Y})$ defined by $\text{EEM}(\omega)$ is

$$\{h : \mathcal{X} \rightarrow \mathcal{Y} \mid \text{err}_h(\omega) \leq \text{err}_g(\omega) \text{ for all } g : \mathcal{X} \rightarrow \mathcal{Y}\}.$$

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 $A \subset \mathcal{X} \subset \mathbf{R}^2$ and $\mathcal{Y} = \{0, 1\}$. 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 $(\mathcal{X}, \mathcal{A}, \mathbf{P})$ we have $A \in \mathcal{A}$ and $\mathbf{P}(A) = 1/2$.

For the training set S in $\mathcal{X} \times \mathcal{Y}$, the hypothesis $h : \mathcal{X} \rightarrow \mathcal{Y}$ defined by

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

achieves zero empirical risk but has error (w.r.t. \mathbf{P}) 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.”

