University of Salzburg | Lecturer: Roland Kwitt

Machine Learning (911.236)

Exercise sheet **A**

Exercise 1. 2 P.

Lets consider the class $\mathcal{H}$ of Boolean conjunctions over (at most) d Boolean literals.

Our domain set here is $\mathcal{X} = \{0,1\}^d$ and the label set is $\mathcal{Y} = \{0,1\}$. A Boolean literal $x_i, i \in [d]$ is either one, zero or not included in the conjunction. We say the empty conjunction *always* returns 1. For instance, with $d = 3$, we could have a conjunction of the form $x_1 \wedge \overline{x_3}$ as one possible hypothesis (reading: x_1 *and* not x_3 – here, x_2 does not appear at all).

Example: Take $d = 3$ and let, for the sake of argument, the *true labeling function* be $x_1 \wedge \overline{x_3}$. In that case, a training set (of size $m = 3$) could look like this:

$$S = (((1,0,1),0),((0,0,1),0),((1,0,0),1))$$

Show that $\mathcal{H}$ is PAC learnable via ERM. That is, show that for any labeling function, f, and any distribution $\mathcal{D}$ over $\mathcal{X}$, if realizability holds, then with probability $1-\delta$ over the choice of

$$m \geq \ldots$$

samples (drawn i.i.d. according to $\mathcal{D}$ and labeled by f), we have that $L_{\mathcal{D},f}(h_S) \leq \epsilon$.

Hint: Look at the hypothesis class $\mathcal{H}$ carefully (does this fall into the already discussed setting of the lecture?)

Exercise 2. 2 P.

Lets consider the hypothesis class of *monotone* conjunctions over (at most) d Boolean literals (monotone means we do not have negated Boolean literals). Our domain set is $\mathcal{X} = \{0,1\}^d$, the label set is $\mathcal{Y} = \{0,1\}$. One example, for $d = 3$, would be $h(\mathbf{x}) = x_1 \wedge x_3$, but $x_1 \wedge \overline{x}_3$ would not be in that class). Assume realizability and specify an ERM algorithm.

Exercise 3. 3 P.

Let $\mathcal{X}$ be a discrete domain set, $\mathcal{Y} = \{0,1\}$ our label set and let

$$\mathcal{H} = \{h_z : z \in \mathcal{X}\} \cup h^-$$

where

$$h_z(x) = \begin{cases} 1, & \text{if } x = z \\ 0, & \text{otherwise} \end{cases}.$$

Here, h^- denotes the hypothesis that is constant 0, i.e., $\forall x \in \mathcal{X} : h(x) = 0$.

Consider the following ERM algorithm (returning the ERM hypothesis h_S): if there is a positive instance, x^+, in the training set S, return h_{x^+}. If no positve instance exists in S, return h^-.

Proof that $\mathcal{H}$ is PAC learnable via this ERM algorithm. That is, show that for any labeling function, f, and any distribution $\mathcal{D}$ over $\mathcal{X}$, if realizability holds, then with probability $1-\delta$ over the choice of

$$m \geq \ldots$$

samples (drawn i.i.d. according to $\mathcal{D}$ and labeled by f), we have that $L_{\mathcal{D},f}(h_S) \leq \epsilon$.

Hint: Make a case distinction for the case where (1) h^- is the true labeling function and (2) there actually is a unique positive instance in S, i.e., the true labeling function , f was some h_z. What are the cases where $L_{\mathcal{D},f}(h_S) > \epsilon$?

Total #points: 7 P.