TECHNISCHE UNIVERSITÄT MÜNCHEN
Zentrum Mathematik

PROF. DR. M. WOLF **Mathematical Foundations of Machine Learning** Summer 2016
Blatt 2
http://www-m5.ma.tum.de/Allgemeines/MA4801_2016S (20.04.2016)

The following homework will be discussed on April 27th to 29th:

I. Simple start

In the framework of the lecture, what is the relation between the average empirical risk $\mathbb{E}_S\left[\hat{R}(h)\right]$ and the risk $R(h)$?

II. PAC learning

Let $\mathcal{X}$ and $\mathcal{Y}$ be finite sets, choose the error probability as risk function and consider a deterministic scenario, where there is a function $f : \mathcal{X} \to \mathcal{Y}$ that determines the 'true' label $f(x) \in \mathcal{Y}$ for every $x \in \mathcal{X}$. Hence, in particular, the training data is of the form $S = \big(x_i, f(x_i)\big)_{i=1}^n$ and the underlying joint distribution has the form $P(x, y) = \delta_{y,f(x)}p(x)$ with some (unknown) distribution p on $\mathcal{X}$.

1. Prove that $\forall \epsilon > 0, h \in \mathcal{F} : \quad R(h) > \epsilon \quad \Rightarrow \quad \mathbb{P}_S\left[\hat{R}(h) = 0\right] \leq e^{-\epsilon n}$.
2. Suppose that $\forall S\ \exists h_S \in \mathcal{F} : \hat{R}(h_S) = 0$, i.e., there is a function in $\mathcal{F}$ that matches the training data (which is for instance the case if $f \in \mathcal{F}$). Show (using 1.) that under this assumption:
$$\mathbb{P}_S\left[R(h_S) > \epsilon\right] \leq |\mathcal{F}|e^{-\epsilon n}$$
3. Use 2. to derive a bound on n that suffices for an (ϵ, δ)-PAC bound. Compare this with the bound derived in the lecture.
4. Look at the proofs of PAC bounds here and in the lecture. Where do you see room for improvements?
5. Apply the bound on n derived in 3. to the following cases under the assumption that $f \in \mathcal{F}$. If necessary, look up the meaning of the mentioned classes.
   (a) $\mathcal{F}$ is the set of all Boolean function on N bits.
   (b) $\mathcal{F}$ is the set of all conjunctions of at most N Boolean literals.
   (c) $\mathcal{F}$ is the set of k-term disjunctive normal form formulas of N Boolean literals.