輪講資料 Understanding Machine Learning: From Theory to Algorithms Part I

Masanari Kimura

June 12, 2019

Abstract

本資料は書籍”Understanding Machine Learning: From Theory to Algorithms”[1] の輪講資料です．本資料は該当書籍の Chapter2 〜 Chapter4 の内容を含みます．

1 Empirical Risk Minimization

学習アルゴリズムは，未知の分布 D からサンプリングされた学習データセット S を入力として，予測器 $h_S : \mathcal{X} \mapsto \mathcal{Y}$ を出力する．ここでこの学習アルゴリズムは，未知の D について損失を最小化するような h_S を見つけることが目的となる．

学習アルゴリズムは分布 D 全体について観測することはできないため，真の損失を直接得ることはできない．そこで一つの解決策として，以下の経験損失を最小化することが挙げられる：

$$L_s(h) := \frac{|\{i \in [m] : h(x_i) \neq y_i\}|}{m} \tag{1}$$

ここで $[m] = \{1,\ldots,\mathrm{m}\}$．このように現実的に得られる学習サンプルについて経験損失 $L_s(h)$ を最小化することで h の学習を行うようなフレームワークを Empirical Risk Minimization（ERM）という．

1.1 Empirical Risk Minimization with Inductive Bias

ERM は強力なフレームワークである一方，過適合（Overfitting）の問題が存在する．そこで，ERM が学習データだけでなく未知のデータに対しても良好な性能を保証できるような方法を探す必要がある．

一つの一般的な解決方法として，ERM の探索空間を制限することが挙げられる．形式的には，学習アルゴリズムは学習データを観測する前に，ある予測器集合を選択しておくことになる．この予測器集合を仮説集合（hypothesis class）と呼び，$\mathcal{H}$ で表現する．与えられた仮説集合 $\mathcal{H}$ と学習データセット S について，学習アルゴリズム $\mathrm{ERM}_{\mathcal{H}}$ は ERM のフレームワークを用いて予測器 $h : \mathcal{X} \mapsto \mathcal{Y} \in \mathcal{H}$ を選択する．

$$ERM_{\mathcal{H}} \in argmin_{h \in \mathcal{H}} L_S(h) \tag{2}$$

このような学習アルゴリズムに予測器を $\mathcal{H}$ から選択するような制限を inductive bias という．こうした $\mathrm{ERM}_{\mathcal{H}}$ は過適合しないことが保証されている．

1.2 有限仮説集合

仮説集合に対するもっとも単純な制限は，仮説集合のサイズに上界（upper bound）を設けることが考えられる．本章では，仮説集合 $\mathcal{H}$ が有限である場合，学習サンプルが十分に与えられた $\mathrm{ERM}_{\mathcal{H}}$ が過適合しないことを示す．

学習サンプル S について h_S を $\mathrm{ERM}_{\mathcal{H}}$ を適用した結果とすると，

$$h_S \in argmin_{h \in \mathcal{H}} L_S(h) \tag{3}$$

とする．以降，簡単のため以下に示す仮定を用いる．

定義 **1.**（*The Realizability Assumption*）$L_D(h^*) = 0$ となるような $h^* \in \mathcal{H}$ が存在する．

References

[1] Shai Shalev-Shwartz and Shai Ben-David. *Understanding machine learning: From theory to algorithms*. Cambridge university press, 2014.